EZCast ProAV

How to Configure a Network for ProAV?

Scalable and flexible Audio/Video extending solutions through Ethernet or Wi-Fi environment.

2021 Dec.

Prepared by

曾聖翰 SHENG-HAN
DANIELA FORTIN PINEDA
陳志育 ALEX CHEN
羅敏 AMANDA

Approved by

HENRY CHOU, CHAIRMAN
WANWEI TEO, ASSOCIATE

EZCAST PRO

Preface

Pro AV is an advanced version of AV which encompasses all the audio or visual systems that are installed for commercial purposes. Pro AV includes various devices, for example, audio, display, whiteboards, cameras, computer and digital signage pieces. These pieces improve connectivity and communication between two separate locations. There are multiple applications for Pro AV including different sectors such as governmental, retail, education, and more.

Some market opportunities for implementing Pro AV include:
- According to research, technological advancements are expected to direct growth of the global Pro AV market in the following years
- The retail industry relies heavily on Pro AV products for customer interaction and advertisement
- The education segment is expected to create a lucrative opportunity for the global Pro AV market
- Expected in the coming years, there will be an increase in businesses adapting to their collaboration spaces with AV solutions

Advances in technology are paving the way to the growing demand of the AV industry by offering customers outstanding and innovative products.
Trends like the usage of 5G and Wi-Fi 6 and the advancement of LED displays will have an enormous impact on the increase of demand for Pro AV products.
However, the biggest revolution in this industry is the AV over IP trend. In contrast to traditional AV, it uses standard IT networking equipment to transmit and switch audiovisual signals.
In the present, the rise in demand for Internet of Things (IoT) has resulted in the growth of IP networks usage in home, entertainment, and business environments.
As the revolution of the Pro AV industry continues to move towards IP-based systems, the typical matrix switcher is now being replaced by Ethernet switches for the flexibility of higher resolutions and increased stream bandwidth.
With the growing demand for new solutions, Ethernet switching infrastructure to transmit proper high-quality multicast streams is imperative.
The EZCast ProAV solutions provide up to 200M transmission via Cat.5 Ethernet with the integrated features of HDMI loopback and passthrough.
Different from other similar devices, the design is flexible and modular in order to assemble extender, splitter, and matrix at the same time. These cost-effective solutions can be easily configured.

How to configure a network for ProAV?

There are several potential scenarios to set up a network environment for ProAV.
For example:
- Via Ethernet Network
- Combination Method of ProAVs and Computers (IGMP snooping or VLAN)
- Network across different offices

Basic ProAV's Configuration, via Ethernet Network

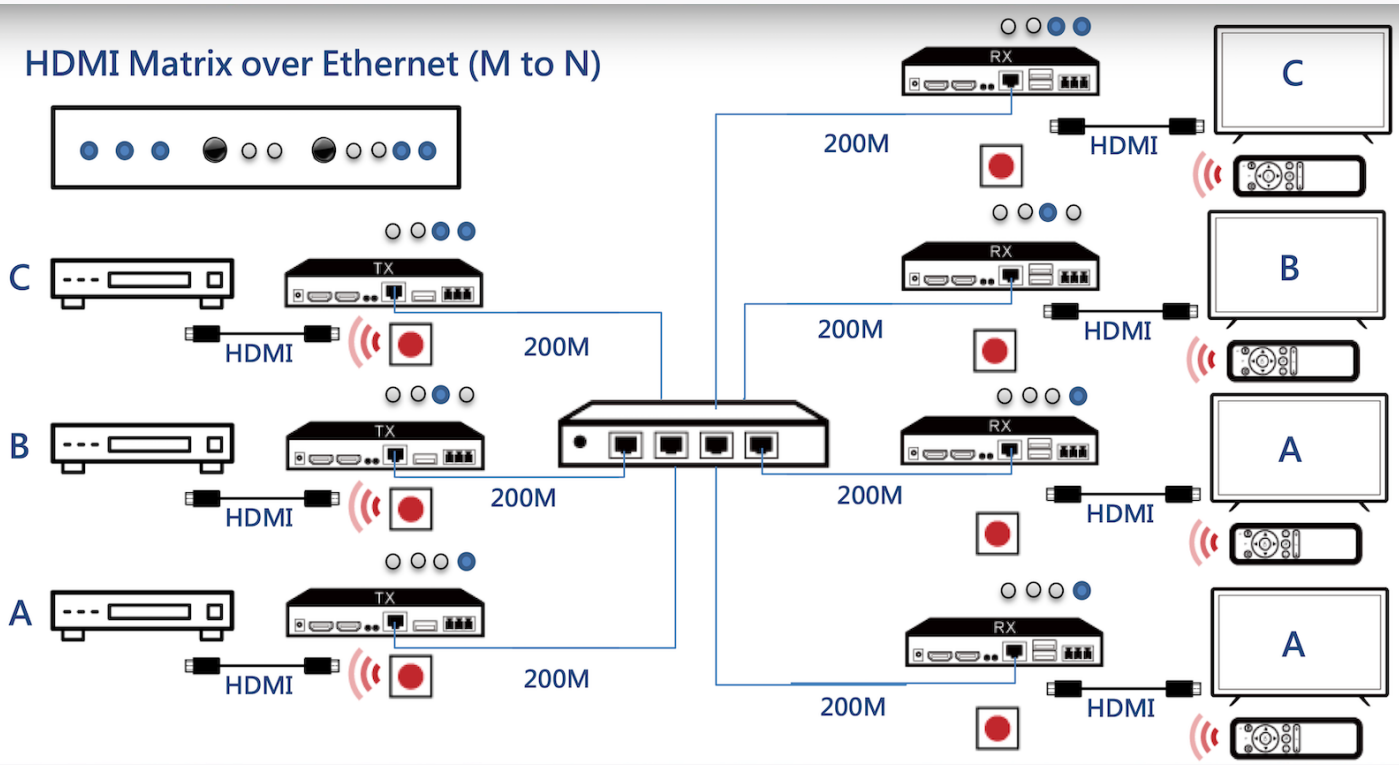
Hardware Requirement

Any Switch or Hub can both be used for a basic ProAV Configuration

Setup Step

You can connect your ProAVs to a switch, just like a computer connects to a switch. For more complexity, you can use one or more switches to extend your network topology, like a star network, tree network, or combine star network and tree network together. Be careful, don't create a loop in your network topology. It will cause your network traffic to be stuck, and you can't transmit any message anyway. Some high-level managed switches can detect the loop and prevent it, but basic switches do not have this function to avoid the loop.

EZCast ProAV Ethernet Application



Combination Method of ProAVs and Computers (VLAN or IGMP Snooping)

Hardware Requirement

Managed Switch with VLAN or IGMP Snooping

Setup Steps

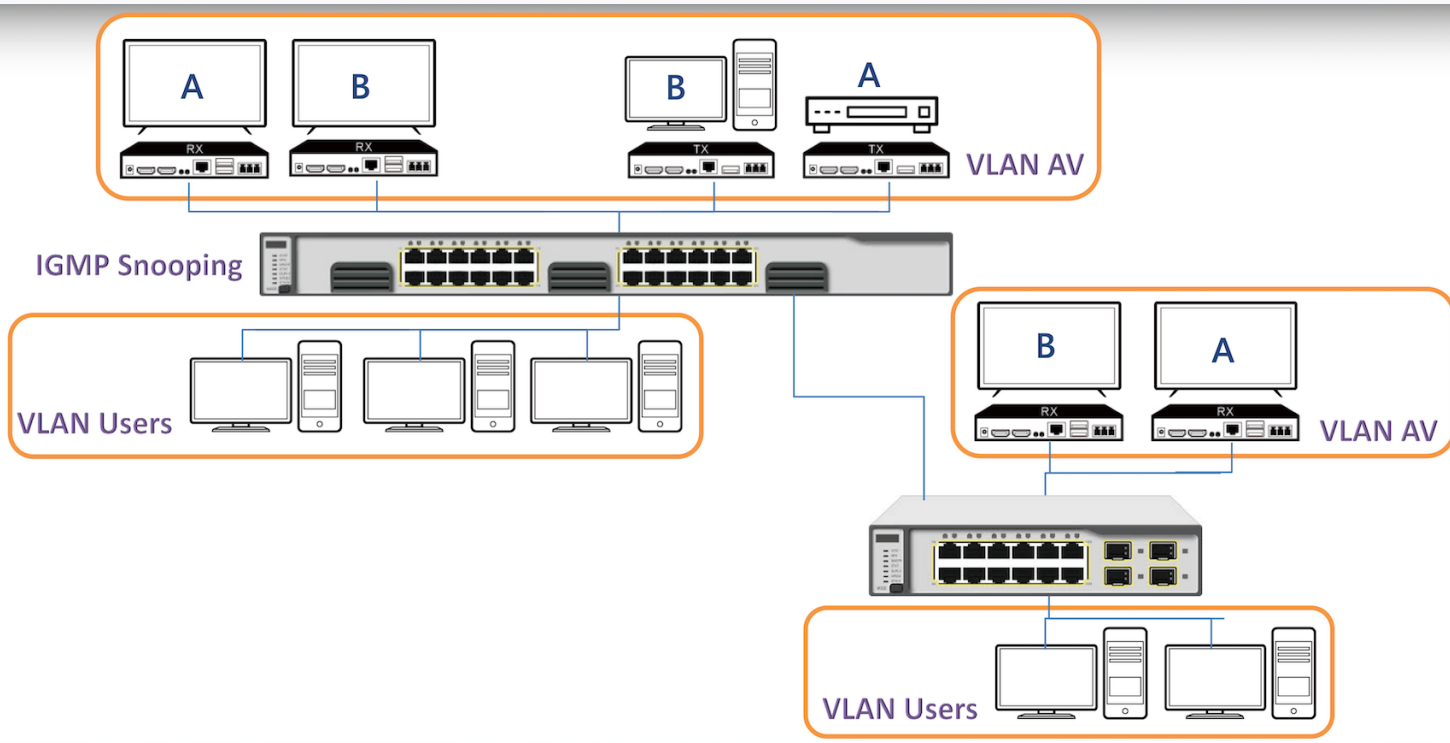
For the VLAN solution, log in to your switch. Then create a new VLAN ID for the ProAV product. For example, VLAN ID 100, and configure this VLAN ID for every port which connects to a ProAV product. So it will be separated into two or more isolated virtual networks, and will not affect your computer network speed.

For the IGMP Snooping solution, log in to your switch, and enable IGMP Snooping function. Once Switch with IGMP Snooping is enabled, it will learn message delivery pairing from IGMP operations, like join and leave, and send packages to the needed port only.

You can combine two solutions, or only use one of the above. However, if you neither set VLAN nor set IGMP Snooping, your network will be stuck by mass broadcast messages, and the system will be massively laggy or won't be able to use the internet anymore.

Please follow each switch vendor's instruction in the useful link section below to set up VLAN and IGMP Snooping.

Network Configuration for EZCast ProAV applications



Knowledge

VLAN: You can define a local area network (LAN) as a broadcast domain. A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). VLANs have a number of advantages and let you easily segment your network. VLANS are easy to manage and provide increased performance, and enhance network security.

IGMP Snooping: IGMP Snooping is a method that network switches adopt to recognize multicast groups of computers or devices that receive the same network traffic, enabling switches to forward packets to the correct devices within their network. Be careful, to complete the IGMP Snooping function, you also need to configure IGMP Querier ahead.

Useful Link

VLAN Setting for ZyXEL Switch: https://support.zyxel.eu/hc/en-us/articles/360001390814-How-to-configure-VLAN-on-Zyxel-Switch
VLAN Setting for NetGEAR Switch: https://kb.netgear.com/30818/How-to-configure-routing-VLANs-on-a-NETGEAR-managed-switch-with-shared-internet-access
VLAN Setting for DLink Switch: https://eu.dlink.com/uk/en/support/faq/switches/layer-2-gigabit/dgs-series/uk_how_to_configure_vlan_asymmetric_dgs_1210_series
VLAN Setting for Others: Just search for the keyword “vlan setting vendor” on google. :)
IGMP Snooping Setting for ZyXEL Switch: https://support.zyxel.eu/hc/en-us/articles/360003640060-How-to-configure-IGMP-Snooping-for-multicast-clients-in-the-same-LAN
IGMP Snooping Setting for ZyXEL Switch:
https://www.youtube.com/watch?v=xiGKCrquB24
IGMP Snooping Setting for NetGEAR Switch: https://kb.netgear.com/21778/How-do-I-enable-Internet-Group-Management-Protocol-IGMP-querier-using-the-web-interface-on-my-managed-switch
IGMP Snooping Setting for DLink Switch: https://eu.dlink.com/uk/en/support/faq/switches/layer-2-gigabit/dgs-series/the-basic-configuration-of-igmp-snooping-on-dgs-1510
IGMP Snooping Setting for Others: Just search keyword “igmp setting vendor” on google.

Network across different offices

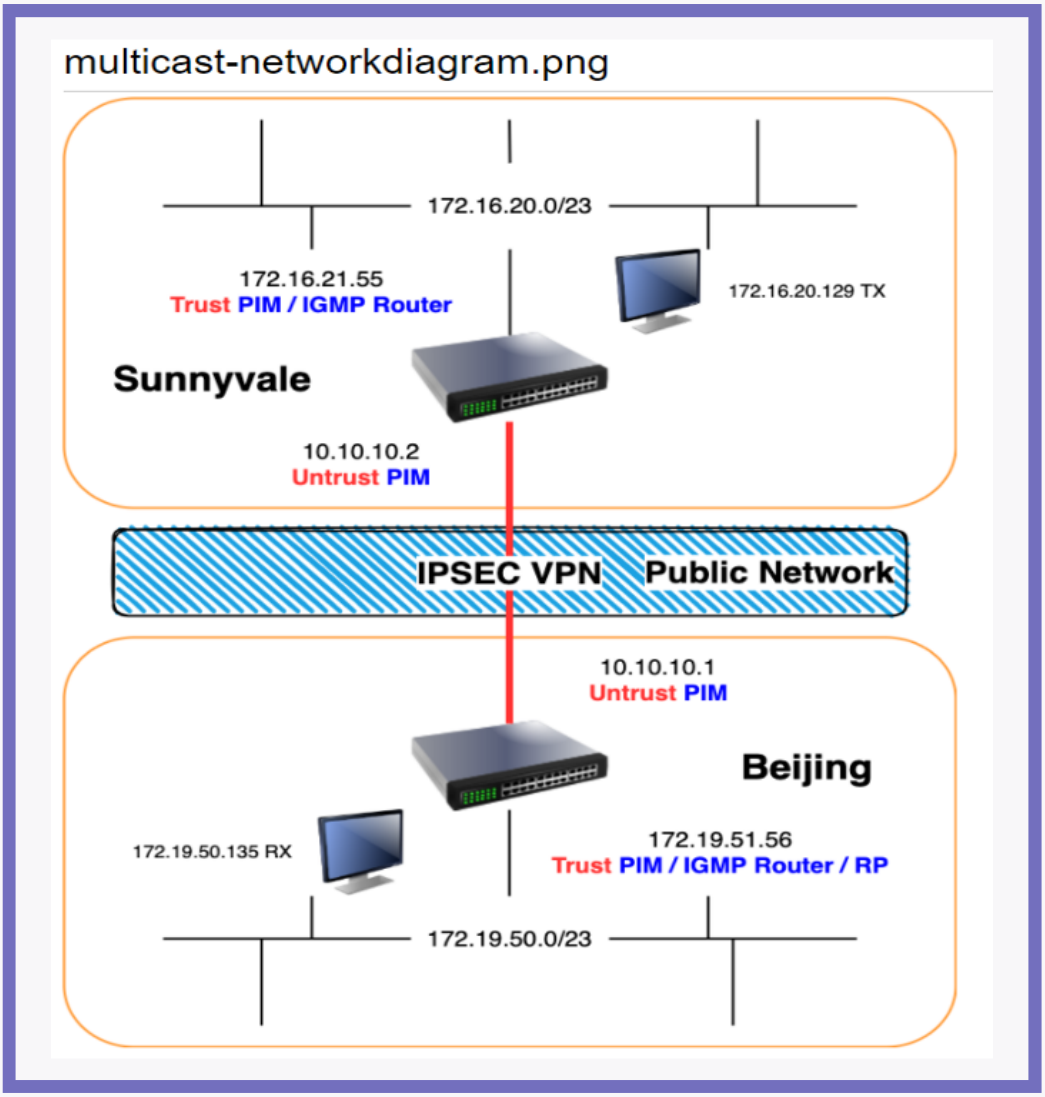
Hardware Requirement

Layer 3 Router With Multicast Routing Protocol, like PIM

Setup Step

There are various solutions, depending on your router vendor. We only illustrated one of them. You can search the keyword phrase “vendor configure multicast PIM” for further results. This solution refers to Juniper’s document and we will perform it step by step with console settings and webpage settings.

Since IGMP is the multicast routing protocol on network layer 2, it can't handle packages on network layer 3. However, PIM is the multicast routing on network layer 3, it can make up for the shortcomings of IGMP. So we combine PIM and IGMP to perform the actions.



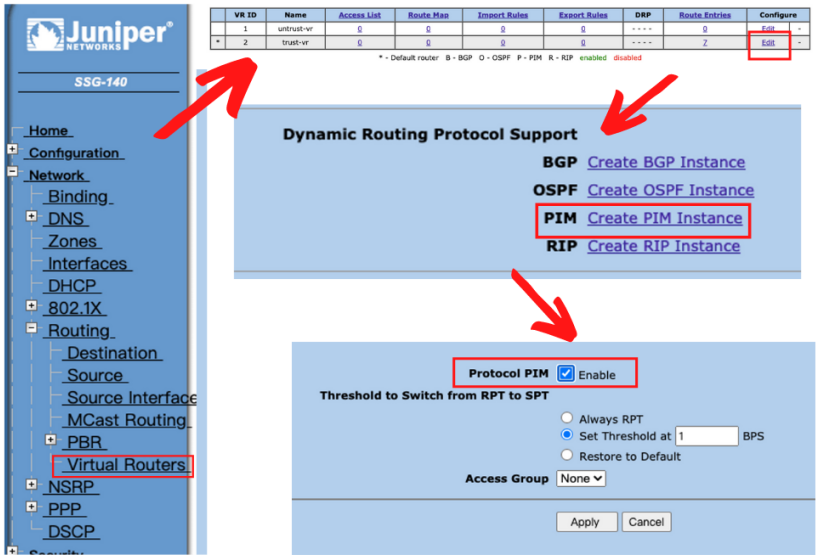
> **Assume two office's LAN networks are already connected by IPSec Site-to-Site VPN:**
>
> First, we need to add PIM for every interface which multicast packages will pass through including LAN interfaces and VPN tunnel interfaces.

PIM-Console

Sunnyvale
```
Sunnyvale-> set vr trust
Sunnyvale(trust-vr)-> set proto pim
Sunnyvale(trust-vr/pim)-> set en
Sunnyvale(trust-vr/pim)-> end
```

Beijing
```
Beijing-> set vr trust
Beijing(trust-vr)-> set proto pim
Beijing(trust-vr/pim)-> set en
Beijing(trust-vr/pim)-> end
```

PIM-WebUI

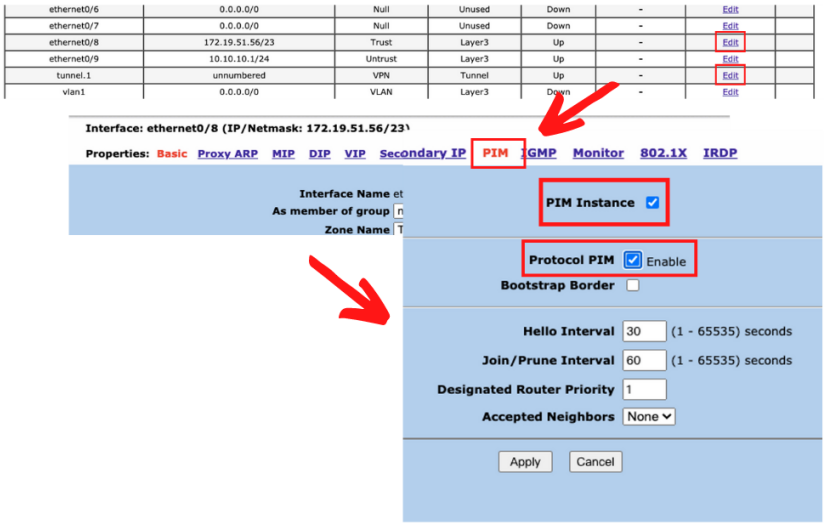


PIM-Interface-Console

Sunnyvale
```
Sunnyvale-> set interface tunnel.1 protocol pim
Sunnyvale-> set interface tunnel.1 protocol pim enable
Sunnyvale-> set interface ethernet0/8 protocol pim
Sunnyvale-> set interface ethernet0/8 protocol pim enable
```

Beijing
```
Beijing-> set interface tunnel.1 protocol pim
Beijing-> set interface tunnel.1 protocol pim enable
Beijing-> set interface ethernet0/8 protocol pim
Beijing-> set interface ethernet0/8 protocol pim enable
```

PIM-Interface-WebUI



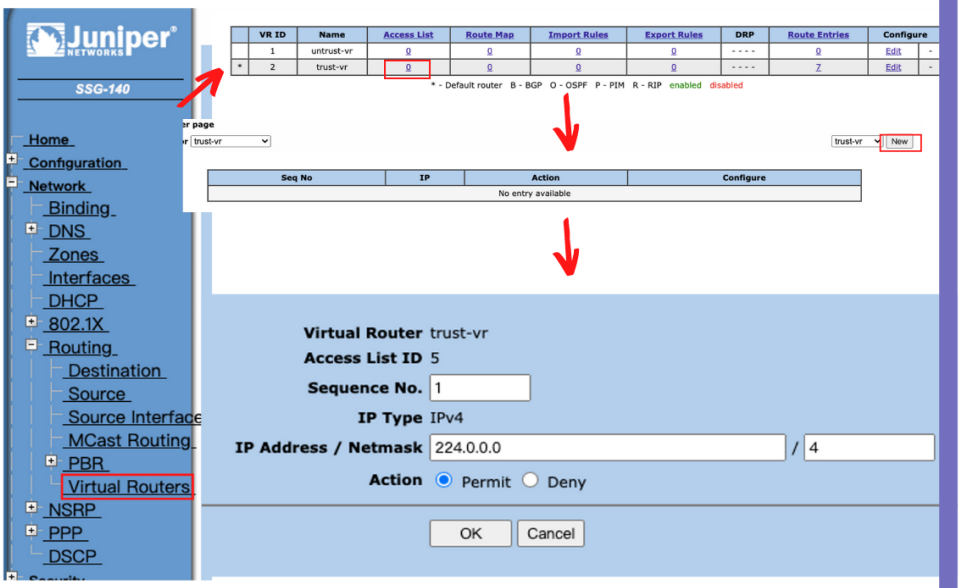
Second, add RP (Rendezvous Point) for your network, like a tree root on computer science data structure, and a PIM network like a tree growing on the root.
All multicast actions are registered to the RP node, and the RP node will construct a source-destination path on the network for every pairing IPs.
Thus, when a new RX device joins one multicast group, and the TX with the same multicast group send the packages, routers will know how to pass the packages to RX devices.

AccessList-Console

```
Sunnyvale
Sunnyvale-> set vr trust
Sunnyvale(trust-vr)-> set access-list 5
Sunnyvale(trust-vr)-> set access-list 5 permit ip 224.0.0.0/4 1
Sunnyvale(trust-vr)-> end

Beijing
Beijing-> set vr trust
Beijing(trust-vr)-> set access-list 5
Beijing(trust-vr)-> set access-list 5 permit ip 224.0.0.0/4 1
Beijing(trust-vr)-> end
```

AccessList-WebUI

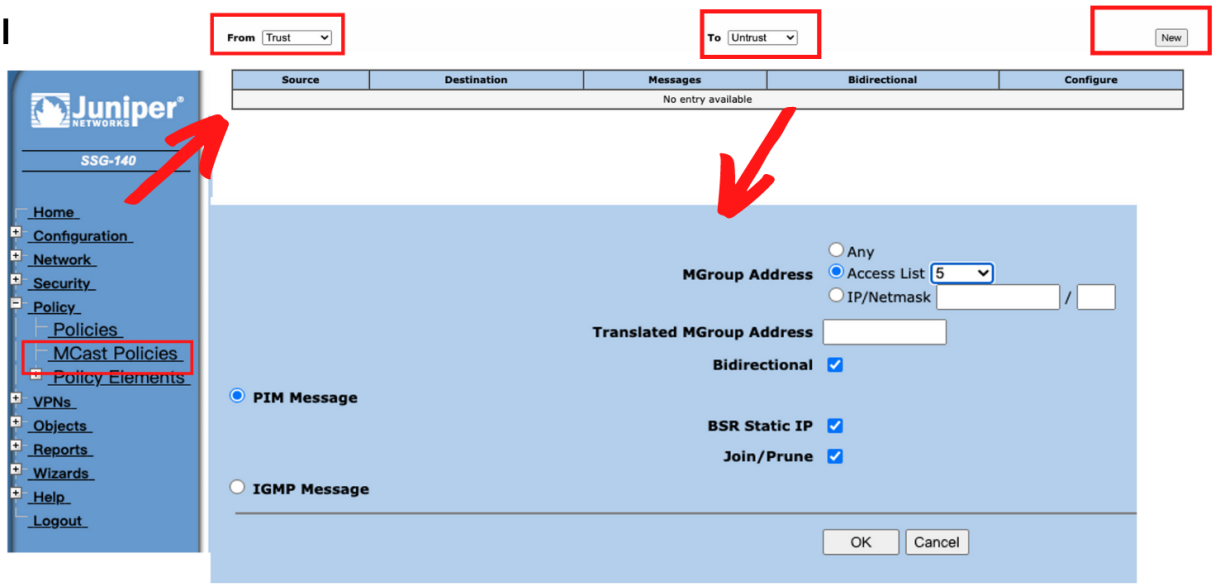


Policiy Console

Sunnyvale
Sunnyvale-> set multicast-group-policy from "Trust" mgroup-list 5 to "Untrust" pim-message bsr-static-rp join-prune bi-directional

Beijing
Beijing-> set multicast-group-policy from "Trust" mgroup-list 5 to "Untrust" pim-message bsr-static-rp join-prune bi-directional

Policy-WebUI

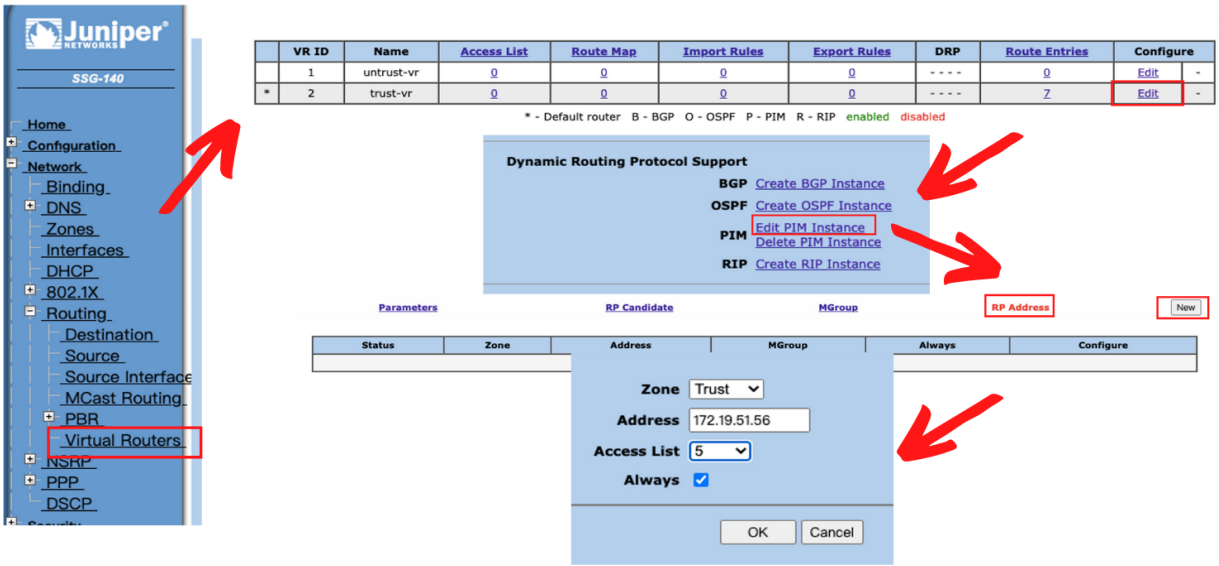


RP-Console

Sunnyvale
Sunnyvale-> set vr trust
Sunnyvale(trust-vr)-> set proto pim
Sunnyvale(trust-vr/pim)-> set zone "Trust" rp address 172.19.51.56 mgroup-list 5 always

Beijing
Beijing-> set vr trust
Beijing(trust-vr)-> set proto pim
Beijing(trust-vr/pim)-> set zone "Trust" rp address 172.19.51.56 mgroup-list 5 always

RP-WebUI



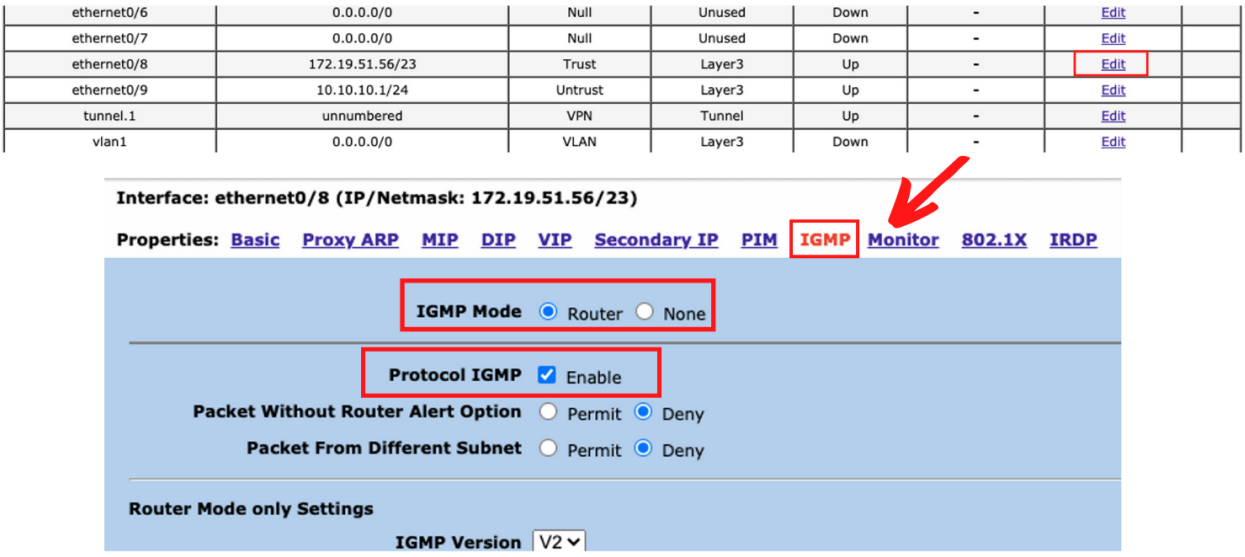
Finally, add IGMP Routers on each LAN interface. It will handle all connected switches' multicast routing. Notice that, if you only add an IGMP Router to one of the LAN interfaces but other LAN interfaces remain empty, it will not work well.

IGMP-Console

```
Sunnyvale set interface
Sunnyvale-> set interface ethernet0/8 protocol igmp router
Sunnyvale-> set interface ethernet0/8 protocol igmp enable

Beijing set interface
Beijing-> set interface ethernet0/8 protocol igmp router
Beijing-> set interface ethernet0/8 protocol igmp enable
```

IGMP-WebUI



Combined with the above steps, ProAV can extend video and audio across different offices as you wish. This setting was tested on the Juniper SSG series and proved to work smoothly.

Knowledge

IGMP: IGMP stands for Internet Group Management Protocol and is a network layer protocol allowing multiple devices to share one IP address to further receive the same data. Networked devices use IGMP to join and leave multicasting groups, and each multicasting group shares an IP address. However, most network switches see which devices have joined multicasting groups as they do not process network layer protocols. IGMP snooping is a way around this: it allows switches to "snoop" on IGMP messages, even though they technically belong to a different layer of the OSI model. IGMP snooping is not a feature of the IGMP protocol, but rather an adaptation built into some network switches.

PIM: Protocol Independent Multicast (PIM) is a collection of multicast routing protocols, each optimized for a different environment. There are two main PIM protocols, PIM Sparse Mode and PIM Dense Mode. A third PIM protocol, Bi-directional PIM, is less widely used.

Useful Links

Juniper Setting:
https://kb.juniper.net/library/CUSTOMERSERVICE/GLOBAL_JTAC/BK7691/Configuring%20Multicast%20Routing%20Over%20IPSEC%20VPN%20ns10694.pdf
PIM by Jan Ho (zh-hant): https://www.jannet.hk/protocol-independent-multicast-pim-zh-hant/
IGMP by Jan Ho (zh-hant): https://www.jannet.hk/internet-group-management-protocol-igmp-zh-hant/
Cisco Setting: https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/9356-48.html
What is IGMP? | Internet Group Management Protocol | Cloudflare:
https://www.cloudflare.com/zh-tw/learning/network-layer/what-is-igmp/

Differences Between Broadcast and Multicast

The act of forwarding a packet from one host connected in a network to another is called transmission. In a network, devices transmit the signals through unicast, broadcast, or multicast.

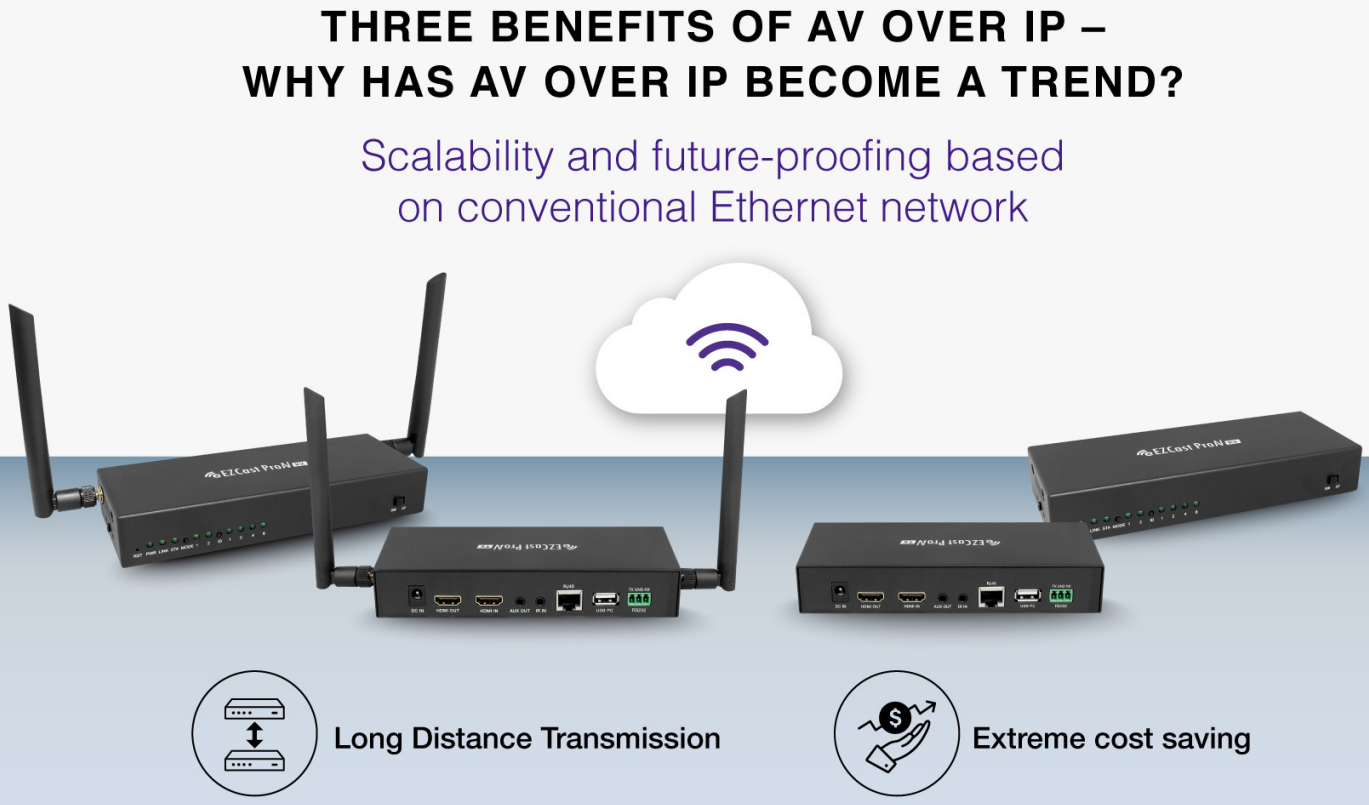
In broadcast, we send a single frame, a single packet, to many devices at once. All broadcast domain users can see this packet as it consists of a frame and a packet. Within the network, data and information are visible to the insiders. In other words, we can only broadcast in a broadcast domain, a very local subnet. This type of request or broadcast is usually sent out for management functions or to find another system. For example, an ARP request is sent to everyone within the network. You also see routers often sending router updates through methods like this, at least the older router technologies. However, some of the new routing technologies don’t use broadcast anymore. They use another method to make them way more efficient.

Multicast is a more novel and efficient method. It's a mix of a unicast and a broadcast. We’re still sending out one frame but we’re sending out this one piece of information to the systems that are interested in receiving it. Therefore, there's something that needs to be done by the stations to essentially subscribe or make themselves available to receive these types of multicast. The use is common for local multimedia delivery. The main difference between broadcast and multicast is that in multicast a request has to be sent. As a result, there is less traffic and the process is more efficient.

EZCast Pro AV vs Other Products

In short, broadcast and multicast differ in that packets in broadcast are forwarded to all the hosts connected to the network, while packets in multicast are only forwarded to the intended recipients. However, there are some problems with broadcast transmission. As time goes by, a huge amount of traffic is generated in the network. Therefore, the process becomes slow and bandwidth is wasted. In multicast the packet is transmitted only to intended recipients in the network. Consequently, the bandwidth is utilized efficiently and the traffic is under control.

Nowadays, many AV solutions are still using the broadcast method. This is not efficient if there are many devices connected to Network. In contrast, EZCast ProAV solutions adopt multicasting, a technique which only forwards the packet to the hosts that are interested in receiving it. In this way, EZCast ProAV products deliver audio and video signals with high quality.



Conclusion

Configuring the network for ProAV might seem a daunting task. The configuration usually depends on a few factors such as hardware requirements and complicated steps.

The key aspects to keep in mind are the selection of AV encoders/decoders, including the compatibility of the Ethernet switch and the amount of configuration required to implement a ProAV network. However, with EZCast ProAV solutions, the customer gets a revolutionary easy-to-use solution to a complex configuration. It reduces the inconveniences and accelerates the procedure of implementing an AV over IP solution on a complex ProAV network topology.

Other benefits of EZCast ProAV include:
- No more complex and expensive matrix switch equipment
- Greater flexibility and scalability in system design and functions
- No necessity to install and maintain specific AV networks
- Highly integrated SoC with HDMI receiver and Gigabit PHY embedded
- Unified transmitter and receiver
- Economic LAN backbone of Fast Ethernet
- Easy deployment configuration
- The low bandwidth requirement makes it become the world's first wired and wireless combination solution which has the greatest compatibility with numerous applications

For more information on EZCast ProAV offered solutions, please visit:
https://www.ezcast.com/product/proAV