SKU: BL-EXTP-IP-4KVW-TX ***TRANSMITTER ONLY

SKU: BL-EXTP-IP-4KVW-RX ***RECEIVER ONLY - Each source requires 1ea Transmitter and each Display requires 1ea Receiver

Brightlinks 4K HDMI over IP Matrix system is a flexible distribution system that allows you to create any size matrix configuration from 2 input to 2 outputs, all the way up to 100 inputs to 100 outputs and more, and easily switch them in any combination with our Brightlink Pro-Control APP.

Brightlinks HDMI over IP Transmitters and Receiver work with Brightlink 24 port Gigabit switch as well as most off the shelf switches as long as they support IGMP snooping and HDCP. These are POE Version which requires a POE Switch.

The Transmitters (TX) convert your HDMI signal from your source into IP signal and send via Cat6 cable into your network switch where it is then distributed to your Receivers (RX) via Cat6 cable and converted back to HDMI signal to be connected to your displays.

This IP Matrix system allows you to send 1080p, 4K@30hz, USB, IR and RS232 over long distances using IP networks with Cat5e/6 and Fiber cable (single mode- module insert not included).

The Built in Video Wall Controller, along with Brightlink's Pro-Control APP, allows you to create multiple video walls in sizes up to 8 vertical x 16 horizontal each, and easily switch your source / content to them.

Brightlink AV LTD
Brightlinkav.com

Product: BL-EXTP-IP-4KVW Doc Type:
Date: 09/28/2018 FW Rev:
>= A7.1.0

Table of Contents

Revision History

- 2018/09/28:
  - Add IGMP v2 description.
- 2018/08/03:
  - Add description for 'IGMP Header Validation' configuration in Ubiquiti Unifi switch.
- 2018/07/09:
  - Add description for parameter: Unknown Multicast Frame, Reserved Multicast Frame and Last Member Query Interval.
- 2018/07/05:
  - Add Appendix B for the configuration of specified switch.
- 2018/05/16:
  - First version.

Overview

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

The purpose of this document is to help you configure the IGMP snooping of Ethernet switch for AST1500 series product in multicast mode.

This document is only for AST1520/AST1525 firmware which version after (and include) A7.1.0.

Configuring IGMP Snooping Parameters

To manage the operation of the IGMP snooping process, you can configure the optional IGMP snooping parameters described in this section.

The parameters for each switch brand/model may be different, to refer to the instructions (user's guide / command-line reference guide) for configuration is necessary.

Please leave the other parameters not mentioned in this section at the default setting unless you have an idea of what you want.

IGMP v2 or IGMP v3

There are two major IGMP versions. IGMP v2 is more popular then v3. So, AST15xx uses IGMP v2.

IGMP Snooping

Enables IGMP snooping. For some switches, you can disable IGMP snooping either globally or for a specific VLAN.

IGMP Proxy / IGMP Report Proxy

Generates IGMP queries, collects membership reports and leaves and sends IGMP messages upstream only when needed. This is to avoid forwarding unnecessary IGMP report/leave messages to the router side.

Unknown Multicast Frame

Specified the action to perform when the switch receives an unknown multicast frame. We strongly recommend our users to drop this kind of frame because it always cause unnecessary bandwidth consumption.

Reserved Multicast Frame

Specified the action to perform when the switch receives a frame with a reserved multicast address. We suggest users to send this kind of frame to all ports.

Normal Leave

When a switch receives an IGMP Leave message from a host on a port, it forwards the message to the multicast router. The multicast router (IGMP Querier) then sends out an IGMP Group-Specific Query message to determine whether other hosts connected to the port should remain in the specific multicast group. The switch forwards the query message to all hosts connected to the port and waits for IGMP report from host to update the forwarding table. If no hosts respond before the last member query interval expires, the switch removes the group from the associated port.

Last Member Query Interval

Sets the interval that the Queryer waits after sending an IGMP query to verify that no hosts that want to receive a particular multicast group remain on a network segment.

We suggest to keep this option as default setting, 0.1 second. To extend this value to be larger than multicast_leave_force will cause that multicast never get deleted for some switches. Please reference to "**All About astparam**" document for more details about 'multicast_leave_force' .

Immediate Leave

To remove the group state when switch firmware receives an IGMP Leave report without sending an IGMP Query message.

You should only use the Immediate Leave feature on VLANs where a single host is connected to each port. If Immediate Leave is enabled in VLANs where more than one host is connected to a port, some hosts might inadvertently be dropped. So, we suggest to disable 'Immediate Leave' if you cannot enable it only for a specific port. We recommend NOT using this kind of switch for switch stacking configuration.

Fast Leave

For most of switches, 'Immediate Leave' is also called 'Fast Leave'.

But the 'Fast Leave' options on some switches (e.g. Zyxel switch) is different, right after receiving an IGMP leave message, the switch itself sends out an IGMP Group-Specific Query message to determine whether other hosts should remain in the specific multicast group with another configurable 'Last Membership Query Interval'.

Multicast Router / MRouter / Router Port / IGMP Querier Mode

Configures a static connection to a multicast router. The port(s) which 'Multicast Router' is enabled is called multicast router port(mrouter port or router port).

Two critical things occur when the switches know about an multicast router port:

- The switch "relays" the IGMP reports from the receivers to the multicast router port, which means that the IGMP reports go toward the multicast router.
- The switch sends the multicast stream out its multicast router port

IGMP Snooping Querier / Auto Querier / Querier

Configures a snooping querier on an interface when there is no multicast router in the VLAN to generate queries.

We strongly recommend our users to disable this feature because most of switches can detect router ports by IGMP Queries (or Multicast Router Solicitation messages).

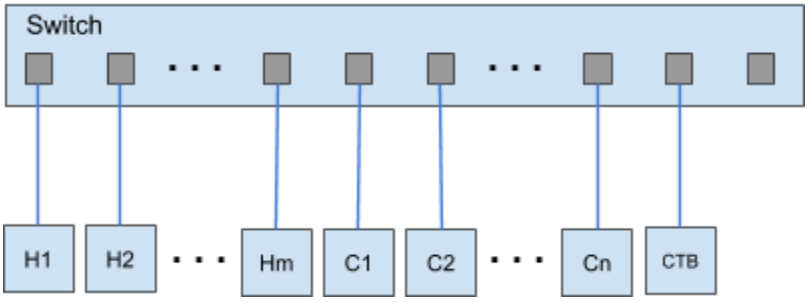
IGMP Snooping VLAN Configuration

Some switches defined additional 'IGMP Snooping' and/or 'Querier' configuration for a specific VLAN. Users may need to create a VLAN entry if no VLAN configuration exist for IGMP snooping.

Sample Configuration

We listed several common network deployment samples for user's reference.

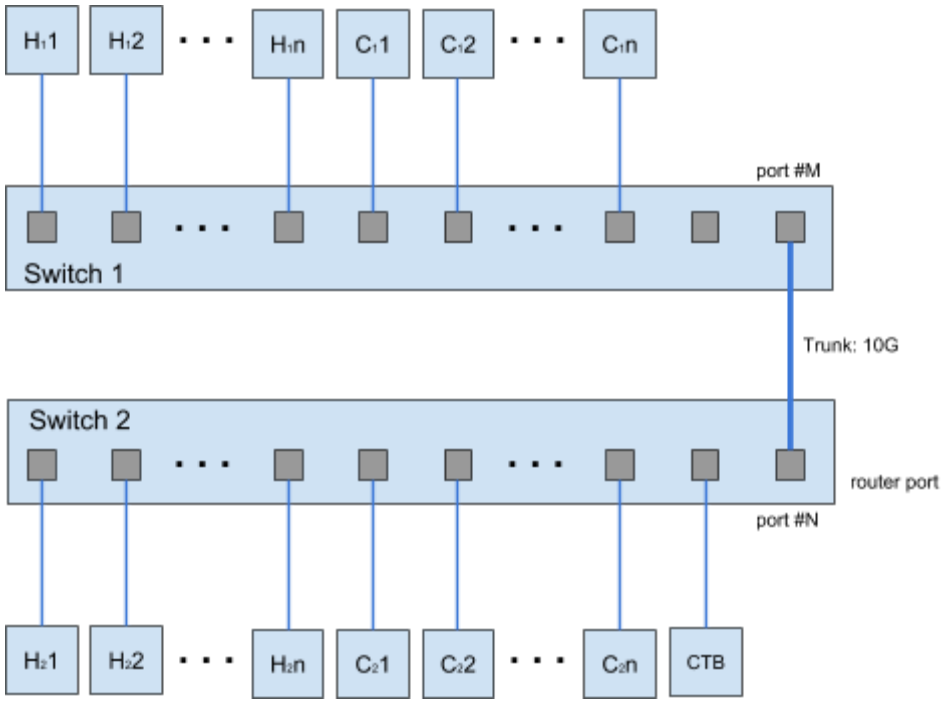
Single One Switch



Host: Hn is the Host #n connected to switch (Tx)
Client: Cn is the Client #n connected to switch (Rx)
CTB: control box

IGMP v2 Snooping: Enable
Immediate Leave: Enable, on each port
Querier: Disable
IGMP Proxy: Disable
Router Port: Disabled

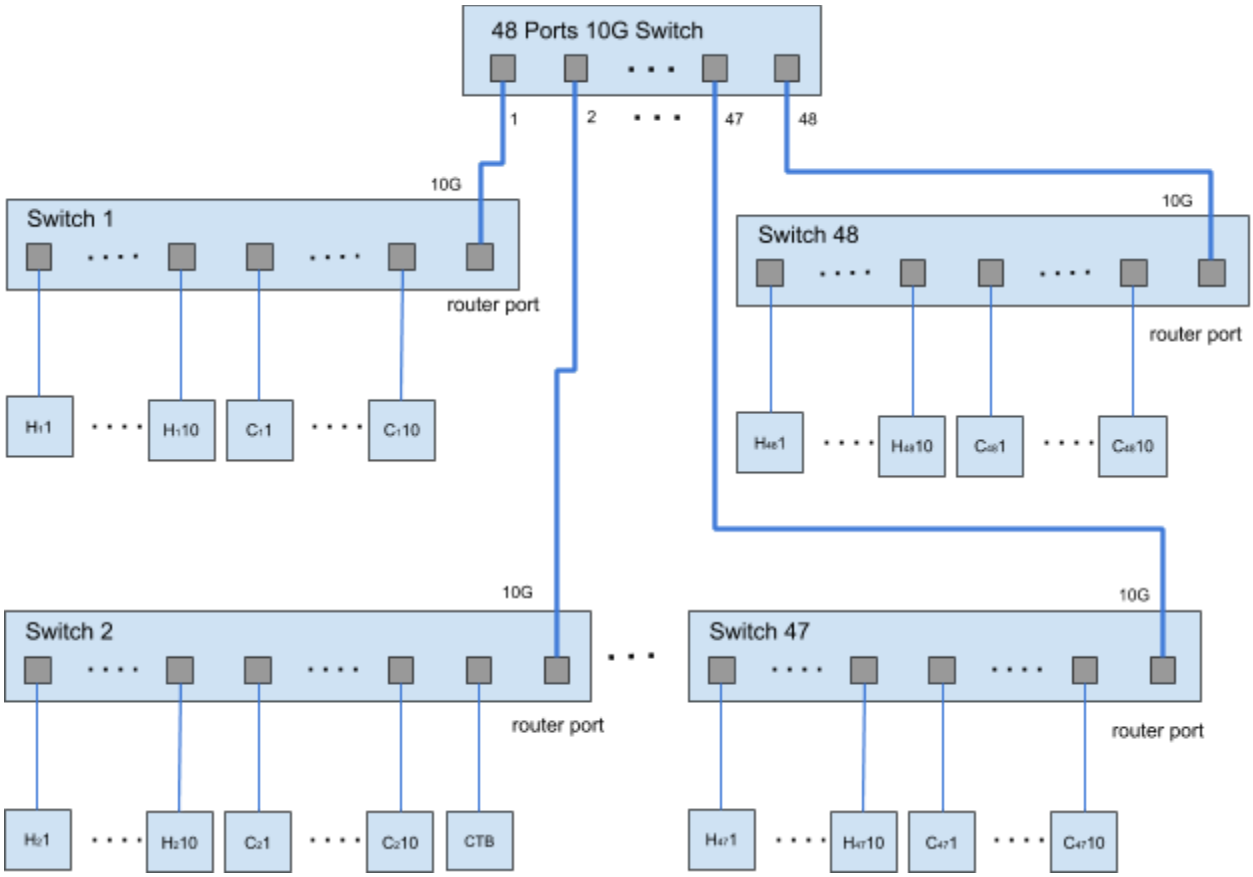
Switch Stacking - 20Tx20R



Host: 20 (Tx), Hsn is the Host #n connected to switch #s
Client: 20 (Rx), Csn is the Client #n connected to switch #s
CTB: control box
Trunk: a point-to-point link between the device and another networking device. The bandwidth of Trunk is the key parameter to determine how many Tx can work simultaneously. If one Tx requires 1Gbps network bandwidth, then 10 Tx requires 1 x 10 = 10Gbps Trunk port bandwidth. Since Ethernet switch nowadays runs full duplex mode, so, a 10Gbps Trunk port can provide 10Gbps upstream and 10Gbps downstream bandwidth.

IGMP v2 Snooping: Enable
Immediate Leave: Enable, on each port except Trunk port
Querier: Disable
IGMP Proxy: Disable
Router port: Must only enable on one end of Trunk i.e. choose neither port #M of Switch 1 or port #N of Switch 2.

Switch Stacking - 480Tx480R

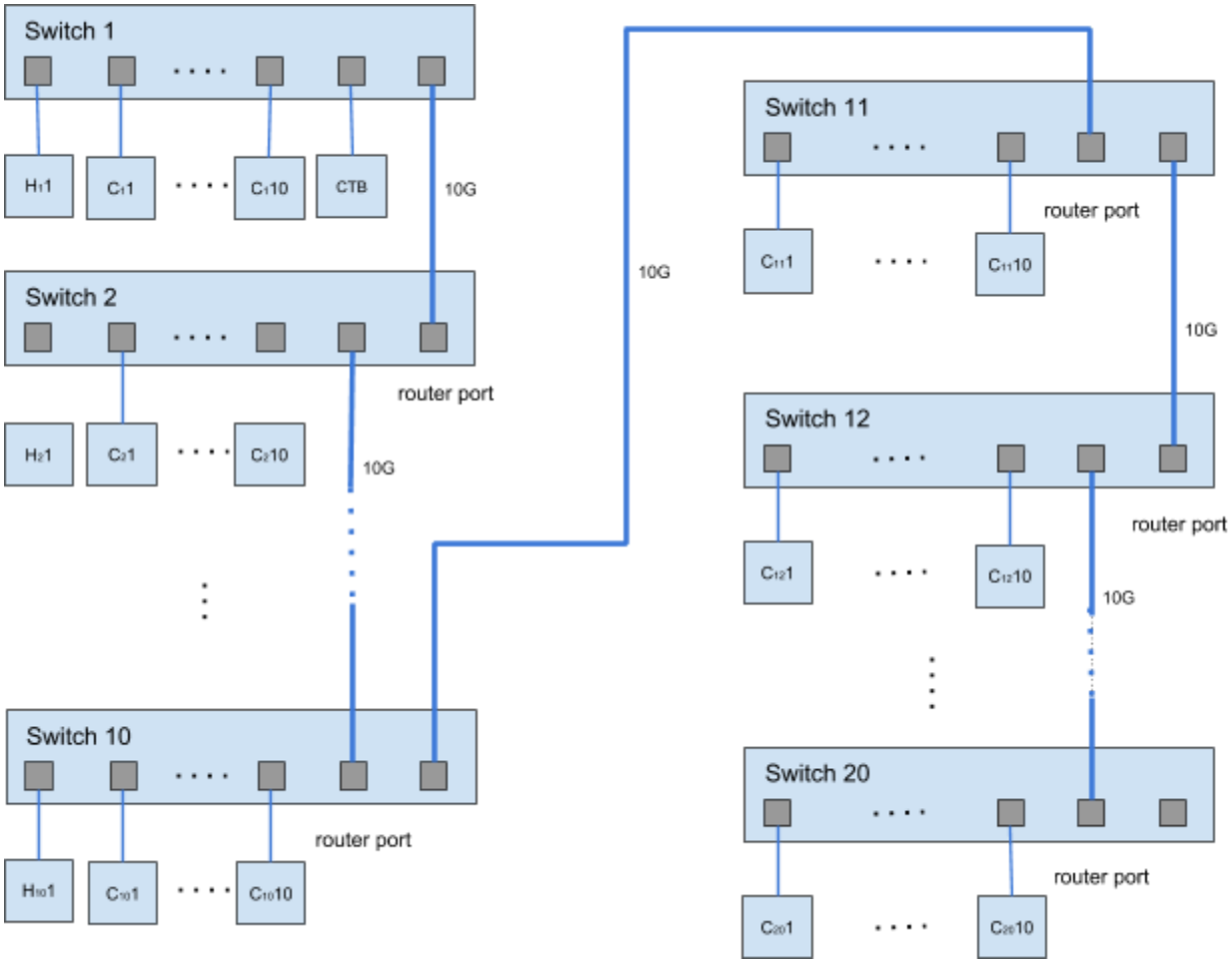


Host: 480 (Tx), Hsn is the Host #n connected to switch #s
Client: 480 (Rx), Csn is the Client #n connected to switch #s
CTB: control box
User can extend to 960(Tx) x 960 (Rx) scale with a 96-port 10G switch.

10G switch:
- IGMP v2 Snooping: Enable
- Immediate Leave: Disable
- Querier: Disable
- IGMP Proxy: Disable
- Router port: Disable

1G switch:
- IGMP v2 Snooping: Enable
- Immediate Leave: Enable on each port except Trunk port
- Querier: Disable
- IGMP Proxy: Disable
- Router port: Enable only on the port connect to 10G switch

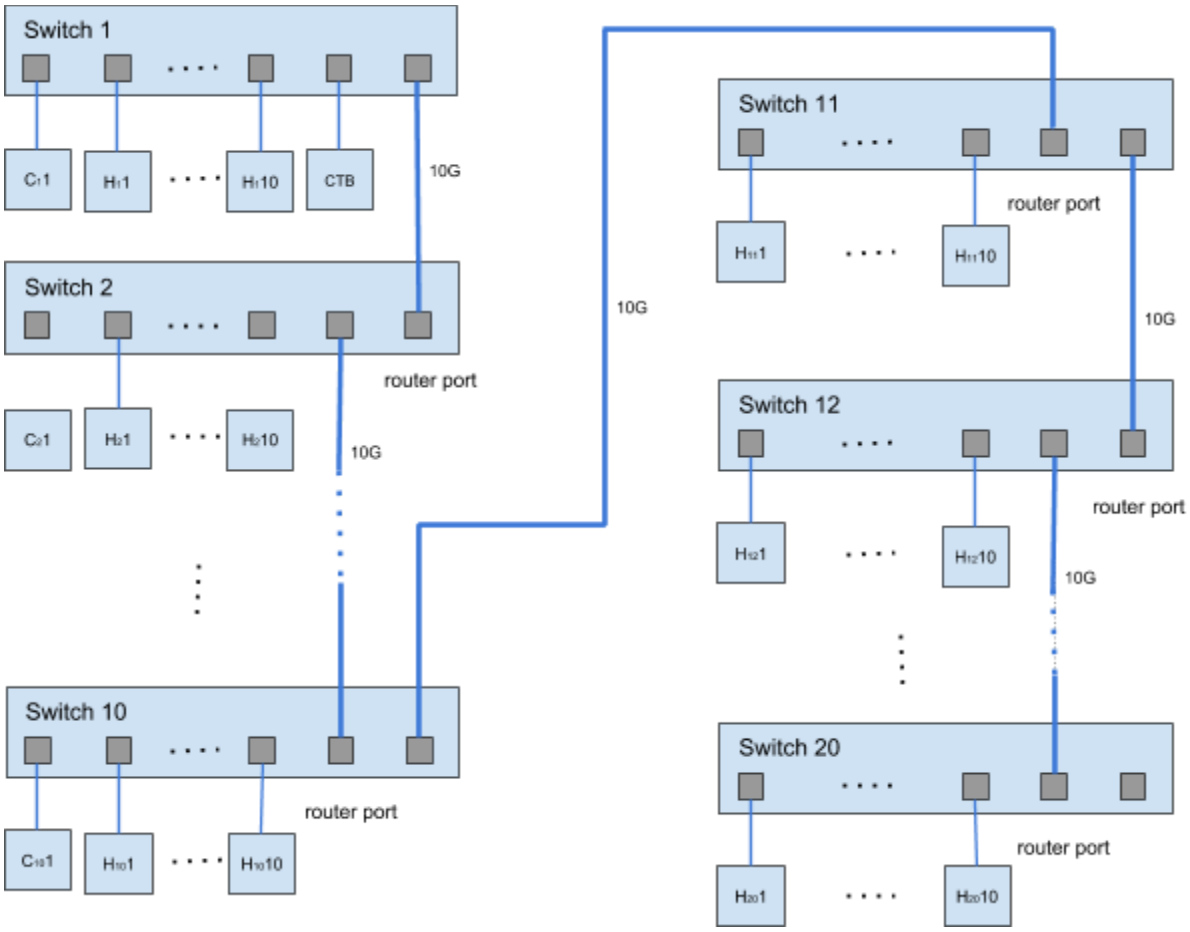
Switch Stacking - few T x many R



Host: 10 (Tx), Hsn is the Host #n connected to switch #s. The number of Tx is limited by sum of bandwidth of Tx which cannot exceed Trunk bandwidth. We can extend to 20 Tx if Trunk works at 20Gbps.
Client: 950 (Rx), Csn is the Client #n connected to switch #s
CTB: control box

IGMP v2 Snooping: Enable
Immediate Leave: Enable on each port except the Trunk port
Querier: Disable
IGMP Proxy: Disable
Router port: Switch 2 ~20, enable only on the port connect to Switch(n-1)

Switch Stacking - many T x few R



Host: 950 (Tx), Hsn is the Host #n connected to switch #s
Client: 10 (Rx), Csn is the Client #n connected to switch #s. The number of Rx is limited by sum of bandwidth of Rx which cannot exceed Trunk bandwidth. We can extend to 20 Rx if Trunk works at 20Gbps.
CTB: control box

IGMP v2 Snooping: Enable
Immediate Leave: Enable on each port except Trunk port
Querier: Disable
IGMP Proxy: Disable
Router port: Switch 2 ~ 20, enable only on the port connect to Switch (n-1)

Note:

Because maximum number of Tx that can run simultaneously is limited by Trunk bandwidth,

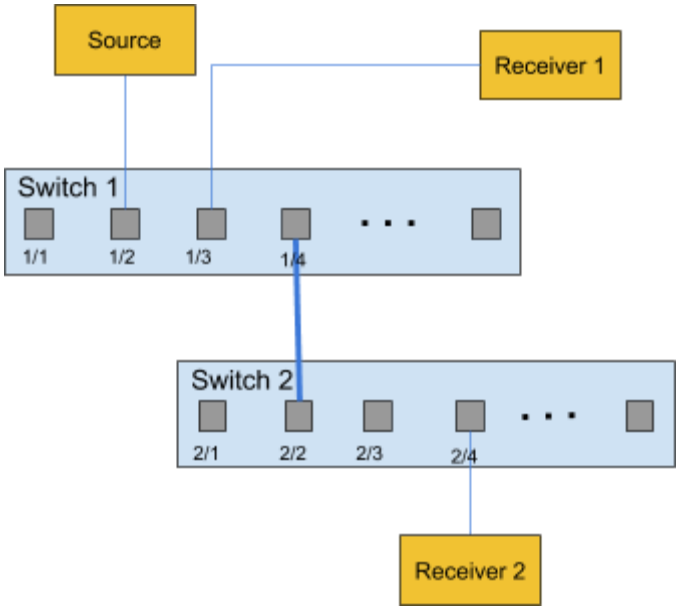
users have to suspend the streaming if no Rx is interested in it.

An option, v_eng_drv_option, (available after A7.2.1) allows user to stop video multicast streaming when no client connected. Please reference to "**All About astparam**" document for more details about it.

Appendix A. Multicast Does Not Work across Switches

Problem

Multicast traffic does not seem to pass across switches.



The multicast source is connected to Switch 1. Receiver 1 is connected to Switch 1, and Receiver 2 is connected to Switch 2. There is a Layer 2 link, either access or trunk, between Switch 1 and Switch 2. In this setup, Receiver 1, which is on the same switch as the source, gets the multicast stream without problems. However, Receiver 2 does not get any multicast traffic.

Understand the Problem and Its Solution

When the source on Switch 1 starts to stream multicast traffic, Switch 1 has "seen" the IGMP report from Receiver 1. As a result, Switch 1 delivers the multicast out port 1/3. But, since Switch 2 "absorbed" the IGMP report from Receiver 2 as part of the IGMP snooping process, Switch 1 does not see an IGMP report (multicast request) on port 1/4. As a result, Switch 1 does not send any multicast traffic out to Switch 2. Therefore, Receiver 2 never gets any multicast traffic, even though Receiver 2 is in the same VLAN but merely on a different switch than the multicast source.

Two critical things occur when the switches learn or statically know about an mrouter port:

- The switch "relays" the IGMP reports from the receivers to the mrouter port, which means that the IGMP reports go toward the multicast router.
- The switch sends the multicast stream out its mrouter port

When the switches know their mrouter port, Switch 2 relays out the IGMP report that the switch received from Receiver 2 to its mrouter port. This port is 2/2. Switch 1 gets this IGMP report on the switch port 1/4. From the perspective of Switch 1, the switch has received merely another IGMP report. Then Switch 1 adds that port into its IGMP snooping table and begins to send out the multicast traffic on that port as well. At this point, both the receivers receive the requested multicast traffic, and the application works as expected.

Solution

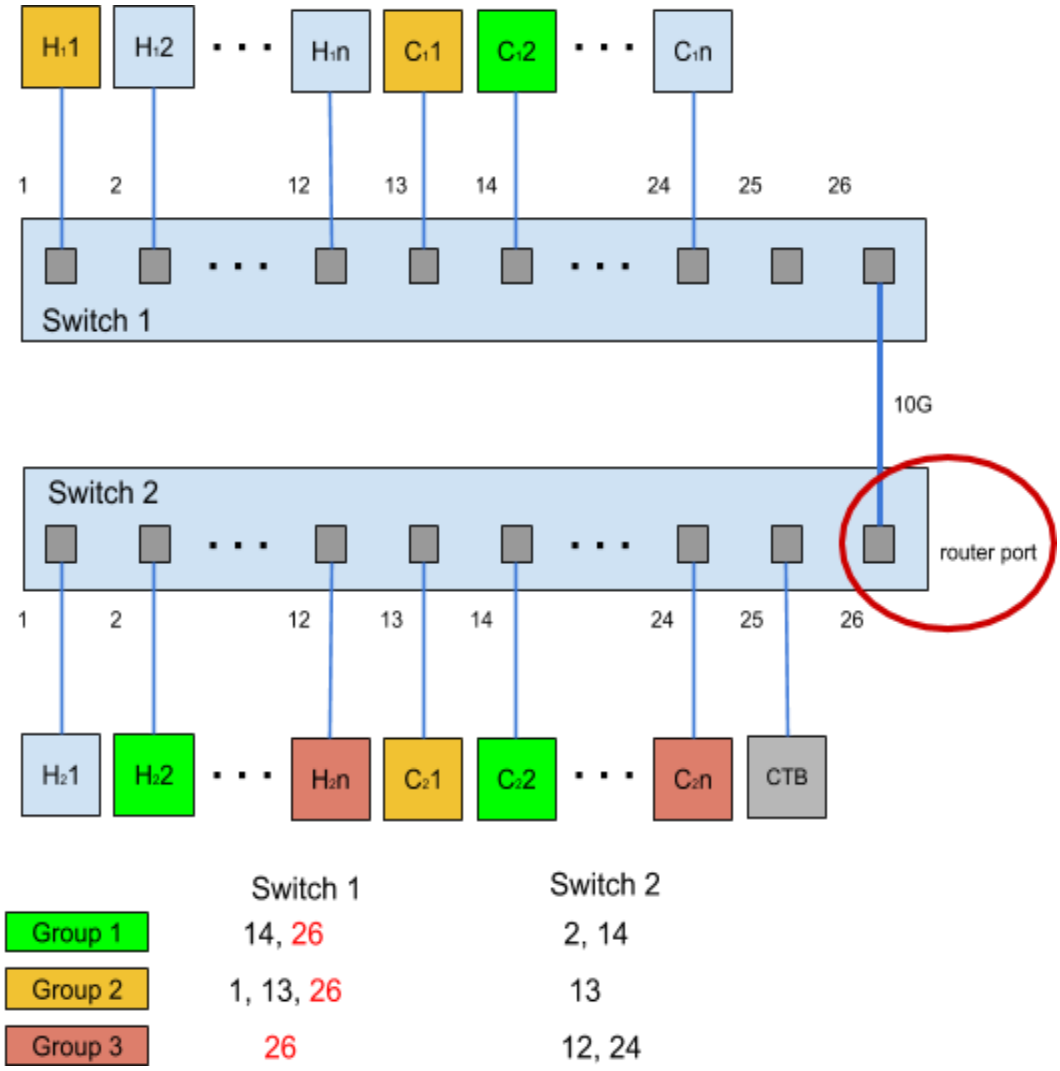
The multicast router port of switches can be identified by static assignment or dynamic detection on IGMP query receiving. We suggest to configure static multicast router port because not all of switches correctly and completely implement IGMP querier.

Here below is our policy on the determination of multicast router port:

- At most one multicast router port for each switch
- Only choose on either of two ends of Trunk (link between two switches). The prefered one is the end of daisy-chain which means that choose the end close to receiver.

So our solution is to configure static Multicast router port on port 2/2 (Switch 2)

Example of AST1520 series



	Switch 1	Switch 2
Group 1	14, 26	2, 14
Group 2	1, 13, 26	13
Group 3	26	12, 24

Group 1:
$H_2$2 => Switch 2 => Port 14 => $C_2$2
$H_2$2 => Switch 2 => Port 26 => Switch 1 => absorbed
Once $C_1$2 start working, it send IGMP report to join Group 1. Port 14 is a member of Group 1.
$H_2$2 => Switch 2 => Port 26 => Switch 1 => Port 14 => $C_1$2

Group 2
$H_1$2 => Switch 1 => Port 13 => $C_1$1
Once $C_2$1 start working, it send IGMP report to join Group 2. Switch 2 forwards this report to Switch 1 via router port. Switch 1 add new membership on port 26, and a new path was created as following

$H_1$2 => Switch 1 => Port 26 => Switch 1 => Port 14 => $C_1$2

Group 3:
H_2n => Switch 2 => Port 24 => C_2n
H_2n => Switch 2 => Port 26 => Switch 1 => absorbed

Appendix B. Switch Configuration

Zyxel XGS2210-28

1. IGMP Proxy

XGS2210-28 supports IGMP proxy (leave/report proxy) in latest firmware (v4.50). But it only provide command line interface(CLI) to user to configure these options.

Following is the instructions to disable IGMP report proxy in CLI,

```
XGS2210# config
XGS2210(config)# no igmp-snooping report-proxy
XGS2210(config)# exit
XGS2210#  write memory
```

(For more details about how to access and use the CLI / commands, please refer to Zyxel CLI Reference Guide.)

2. Multicast Router Port

'Multicast Router Port' configuration on XGS2210-28 web interface is called '**IGMP Querier Mode**'.

Select 'Fixed' to have the switch use the port as an IGMP query port (Router Port).

Select 'Edge' to stop the switch from using the port as an IGMP query port (Router Port).

Ubiquiti Unifi Switch

1. IGMP Header Validation

'IGMP Header Validation' is enabled by default in Ubiquiti Unifi series switch and can be disabled only in CLI interface or controller interface.

For compatibility, we strongly recommend our users to disable this feature if AST1520 firmware version is not after (and include) A7.3.0.

Following is the instructions to disable 'IGMP Header Validation' in CLI.

```
(UBNT) >en
(UBNT) #config
(UBNT) (Config)#show igmp
(UBNT) (Config)#no set igmp header-validation
```

This only last until next reboot or provisioning. Please contact Ubiquiti if you have to save this setting for next booting.

Appendix C. Switch Known Issue

Zyxel XGS2210-28

Packet loss always occurs at egress of 10G port (SFP+ interface) if more than 8 video transmitters (Tx) send traffics out of 10G port (the aggregate of bandwidth is less than 10Gbps).