Luminex

#AVNetworkingMadeEasy

IP Multicast and IGMP

Benjamin Wahiche & Hans Vandermaesen

Contents

1. Introduction 3

2. Internet Group Management Protocol (IGMP) 3

2.1 Receivers 3
2.2 Senders 3
2.3 Multicast Streams 3
2.4 Network Switches 4
2.4.1 Querier election process 4
2.4.2 General Query 4
2.4.3 Routing 4
2.4.4 Settings in GigaCore 4

3. Schematic overview 5

3.1 IGMP 5
3.2 Querier 5
3.3 Multicast routing: all devices correctly implemented IGMP 7
3.3.1 Normal operation 7
3.3.2 Different Querier 8
3.3.3 Without Unknown Flooding 8
3.3.4 IGMP Snooping disabled 9
3.4 Multicast routing: none of the Receivers implemented IGMP correctly 9
3.4.1 Normal operation 9
3.4.2 Different Querier 10
3.4.3 Without Unknown Flooding 10
3.4.4 IGMP Snooping disabled 11
3.5 Multicast routing: mix of compliant and non-compliant Receivers 11
3.5.1 Normal operation 11
3.5.2 Different Querier 12
3.5.3 Without Unknown Flooding 12
3.5.4 IGMP Snooping disabled 13

4. Conclusion 13

1. INTRODUCTION

IP Multicast is a method of sending IP packets to a group of interested Receivers in a single transmission. It uses specially reserved Multicast Address blocks (Class D : 224.0.0.0 – 239.255.225.255). It is often employed for streaming data protocols in our industry like MA-Net, sACN, Dante and many more.

To take full advantage of the benefits of IP Multicast, it is a requirement that Receivers (end devices that want to receive a particular Multicast Stream) and network switches fully support the Internet Group Management Protocol (IGMP) for IPv4 or the Multicast Listener Protocol (MLD) for IPv6.

This document gives a basic explanation of IGMP functionality and some basic use cases to explain in detail the consequences of the different settings and to point out some unintuitive behavior in the protocol. These explanations and use cases are for IGMP, but as MLD is very similar, they are also valid for MLD.

2. INTERNET GROUP MANAGEMENT PROTOCOL (IGMP)

This is the protocol which makes sure that Multicast Traffic is only forwarded to the registered Receivers. The network switches will gather this information using IGMP snooping. We will describe how this mechanism takes place and how it can impact traffic across the network.

2.1 Receivers

Receivers are end devices that are interested in one or more Multicast Streams. They can subscribe for these streams by sending out 'Membership Reports'. This message holds the Multicast Address of the stream they are interested in.
To keep the Multicast subscriptions up to date, Receivers also need to answer General Queries from the network switches (see next chapters) with Membership Reports.
If a Receiver is no longer interested in a certain Multicast Stream, a 'Leave Message' can be used to unsubscribe for this stream.

For example, a Multicast Receiver can be a Dante Speaker, a sACN node or an IP video decoder.

2.2 Senders

For Senders of Multicast Data, there are no IGMP requirements. They just can send the Multicast Streams to their specific Multicast Addresses.

For example, a Multicast Sender can be a Dante stage box, a sACN lighting console or an IP video encoder.

2.3 Multicast Streams

A Multicast Stream is the flow of data transmitted in Multicast from a Sender to one or multiple Receivers. In the case of a Multicast Stream, instead of being sent with a device's IP address as the destination, it is sent to a Multicast IP address. Multicast IP addresses are a specific range between 224.0.0.0 and 239.255.255.255. This is also known as Class D. Any packet sent with a destination IP address in this range will be treated as Multicast.

A few practical examples of Multicast Streams:

- Dante Multicast flows are composed of up to 8 channels of audio
- sACN universes are transported as a Multicast Stream. In that case, the Multicast Address is defined by the universe number.
- Video streams are commonly transmitted as Multicast Streams. In many cases, the audio attached to the video will be transmitted in a separate stream making it possible to send it to additional Receivers while not using the bandwidth of the full video stream. Some manufacturers use Dante for this purpose.

2.4 Network Switches

Also, network switches will need to have both IGMP Snooping and Querier functionality. When it comes to IGMP, a network switch can have 2 roles: **Querier** or **non-Querier**. The election of the Querier is done based on the lowest IP-address. It is therefore very important that all IGMP switches have a different IP-address.

2.4.1 Querier election process

The election process goes as follows:

- Every switch starts up in the Querier role and starts sending out General Queries.
- If a switch receives a General Query with a lower IP address than its own, it goes to the non-Querier role.
- The remaining Querier will keep sending out these General Queries on a fixed interval on all its ports.
- When the other switches don't receive new General Queries for a number of Query intervals (the Querier is shut off or disconnected), they go to the Querier role and the election process starts over.

So apart from the start up of a network or the disappearing of the Querier, a stable network will only have one Querier.

2.4.2 General Query

A General Query is a message send out only by the Querier, that basically asks Receivers to subscribe to new Multicast Streams they are interested in or the confirm existing subscriptions. The General Query is repeated on a fixed interval. The Querier sends these messages out on all its ports.
A downstream switch will forward this General Query on all its ports. So, in the end all end devices will be reached.

2.4.3 Routing

A non-Querier switch will set a forwarding rule for ALL Multicast Data on the port the General Query is received (Router Port). This means that incoming Multicast Streams on any other port will always be forwarded through the Router Port towards the Querier.
For each Multicast Address in a Membership Report received on a port of a switch, a forwarding rule is set.

This rule states that a Multicast Stream with this Multicast Address is forwarded to this port. A non-Querier switch will forward the Membership Reports through the Router Port towards the Querier.

One important consequence of this routing method is that all Multicast Streams are always forwarded form the Sender towards the Querier. Behind the Querier (seen from the perspective of the Sender) the forwarding is depending on the forwarding rules and some other settings.
It is also worth mentioning that a switch with no IGMP capabilities will forward all Multicast Traffic to all ports, just like it would for broadcast data.

2.4.4 Settings in GigaCore

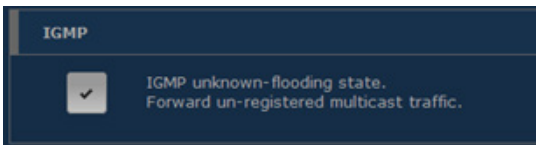
- **IGMP snooping enable/disable**
  IGMP Snooping is enabled by default on all groups. Disabling IGMP snooping will cause Multicast Traffic to be broadcasted on the network.

- **Querier enable/disable**
  By default, the Querier option is enabled. This defines if the switch is allowed to participate in the Querier election process. Disabling this setting prevents the switch to go into Querier role. Make sure that, at least one switch has the Querier option enabled for IGMP to function.

- **Unknown Flooding enable/disable**
  Unknown Flooding means that Multicast Streams coming into a switch, will be forwarded to all ports if there is no forwarding rule set for this stream. By disabling this setting, data streams with no forwarding rules will only be forwarded through the Multicast Router Port towards the Querier.

Advanced Group Settings

Global Settings



3. SCHEMATIC OVERVIEW

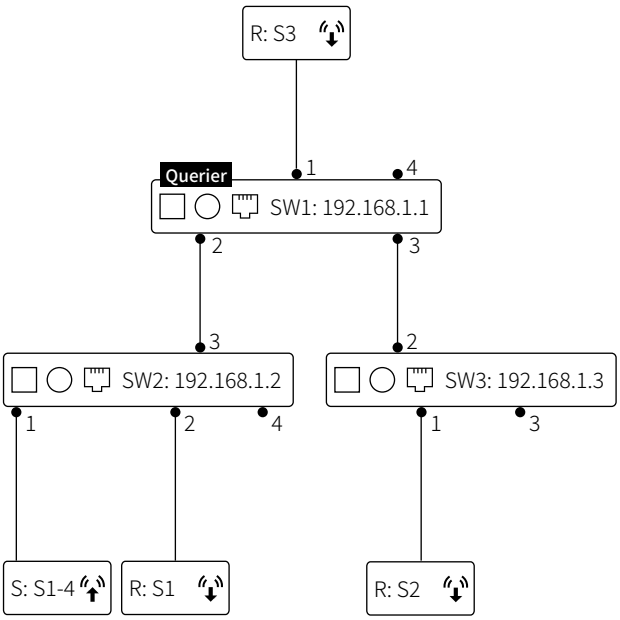
In the below figures we use the following abbreviations:

- GQ : General Query
- MR:Sx : Membership Report with the Multicast Address for stream x
- S:Sx-y : Sender for streams x to y
- R:Sx : Receiver interested in stream x
- SW: Switch

3.1 IGMP

Figure 1 shows a basic setup with 3 switches. The switch with the lowest IP, switch 1, becomes the Querier. On each switch is a Receiver interested in a stream and on switch 2 is a Sender connected which sends out stream 1-4.

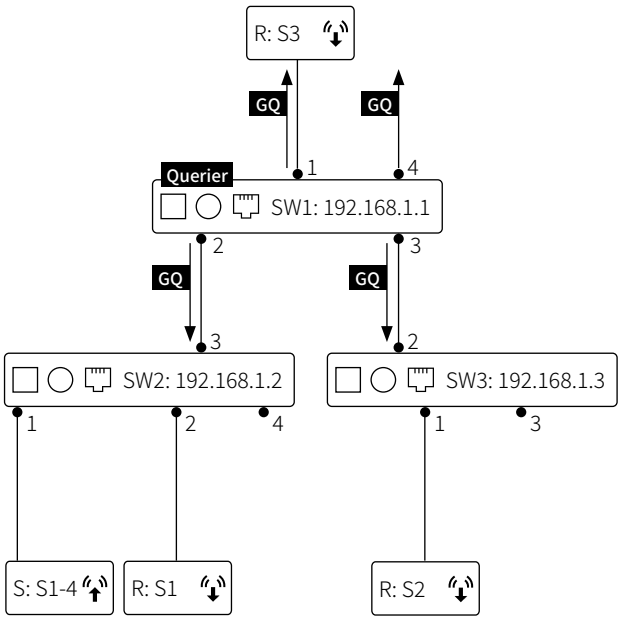
Figure 1: Basic network setup with Multicast/IGMP



3.2 Querier

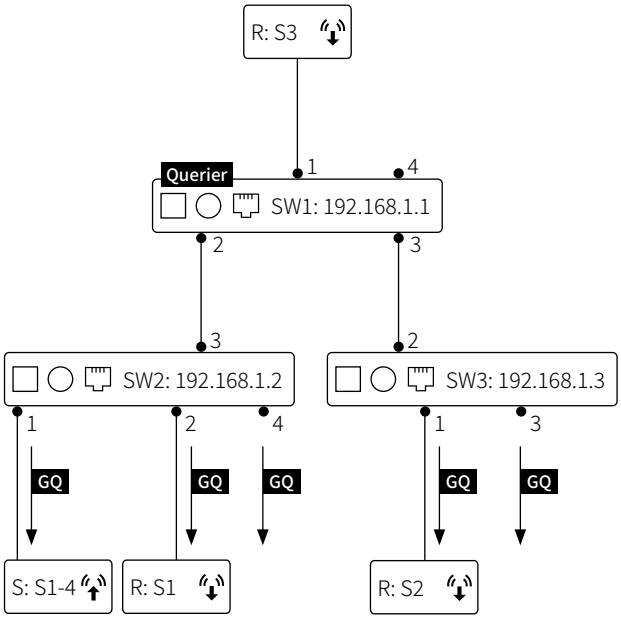
Figure 2 shows the Querier sending out General Queries on all of its ports.

Figure 2: General Queries from the Querier



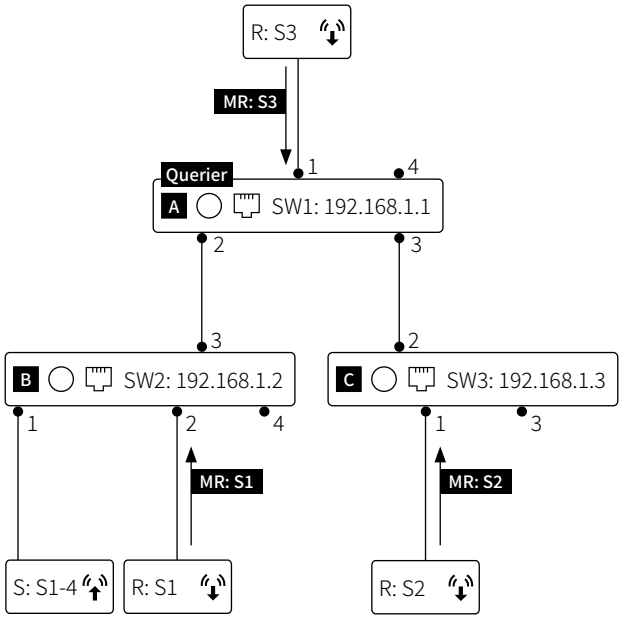
A downstream switch will set the port on which the General Query is received as its Router Port. The switches will forward the General Query on all of its active ports.

Figure 3: General Queries forwarding and handling



A Receiver interested in a stream will answer on the General Query with a Membership Report for the stream in question. The receiving port sets a forwarding rule: forward this stream to the receiving port.

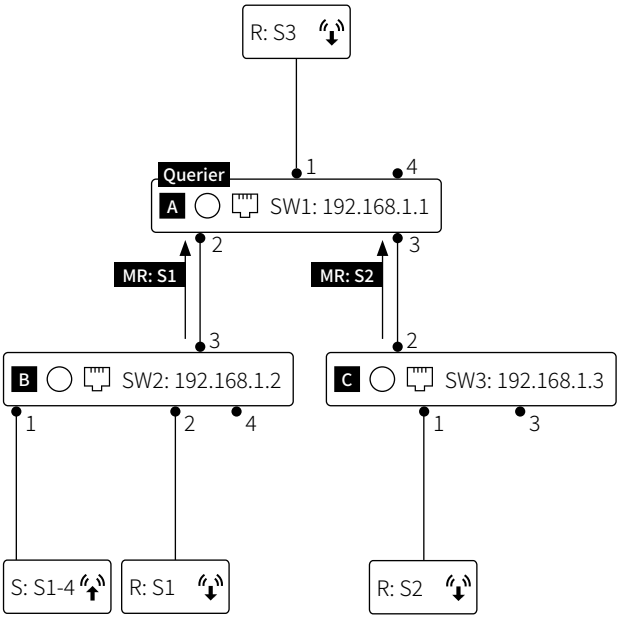
Figure 4: Membership Reports from end devices and handling by switches



A Forwarding rule: Stream 3 to port 1
B Forwarding rule: Stream 1 to port 2
C Forwarding rule: Stream 2 to port 1

Each non-Querier switch will forward the Membership Reports through its Router Ports towards the Querier. The Querier will set forwarding rules for each received Membership Report

Figure 5: Membership Reports forwarding



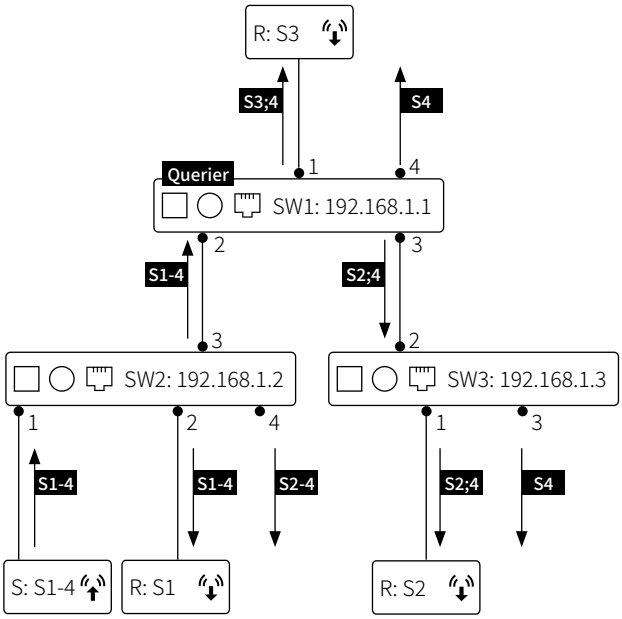
A Forwarding rule: stream 3 to port 1 | stream 1 to port 2 | stream 2 to port 3
B Forwarding rule: stream 1 to port 2
C Forwarding rule: stream 2 to port 1

3.3 Multicast Routing: all devices correctly implemented IGMP

3.3.1 Normal operation

- Querier enabled
- Unknown Flooding enabled
- IGMP Snooping enabled

Figure 6: Multicast Routing



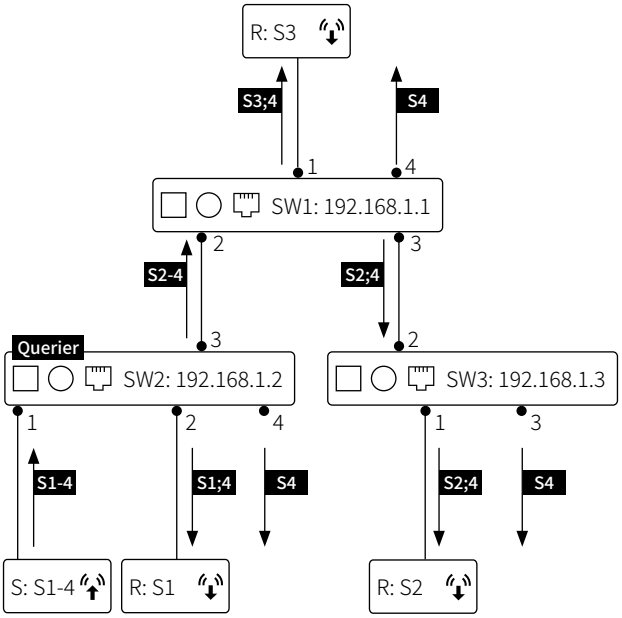
With these settings, depending where the Receiver is located opposite to the Querier and the Sender, the Receiver will be flooded with more streams then requested. Streams with no subscriptions on the network will be broadcasted.

It is worth noting that, since SW2 is upstream in relation to the querier, it is not aware of any registration for stream 2 and 3 (which are received on SW3 and SW1). The consequence is that, on SW2, streams 2 and 3 are flooded just like stream 4 even if they are registered downstream to the querier.

3.3.2 Different Querier

- Querier **disabled** on Switch 1, Switch 2 becomes Querier
- Unknown Flooding enabled
- IGMP Snooping enabled

Figure 7: Multicast Routing, different Querier

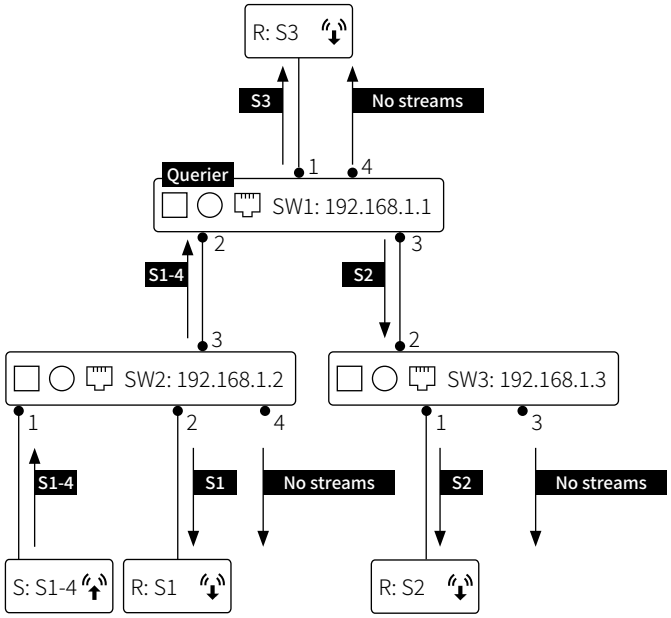


By influencing the Querier election, you can limit the flooding on Receivers, but this will only help when all sources are connected to one switch in the network. Unsubscribed streams are still broadcasted.

3.3.3 Without Unknown Flooding

- Querier enabled
- Unknown Flooding **disabled**
- IGMP Snooping enabled

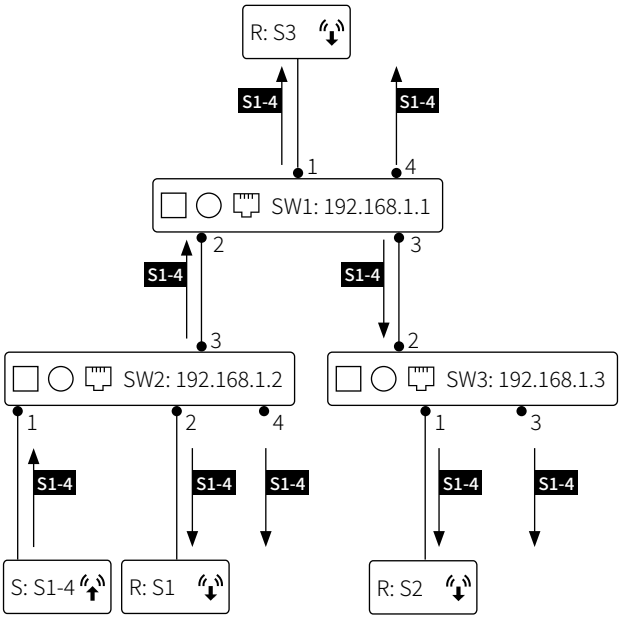
Figure 8: Multicast Routing, without Unknown Flooding



With these settings you get the most optimal situation if all the Receivers are IGMP compliant. Receivers only receive streams they have requested.

3.3.4 IGMP Snooping disabled

Figure 9: Multicast Routing, IGMP Snooping disabled



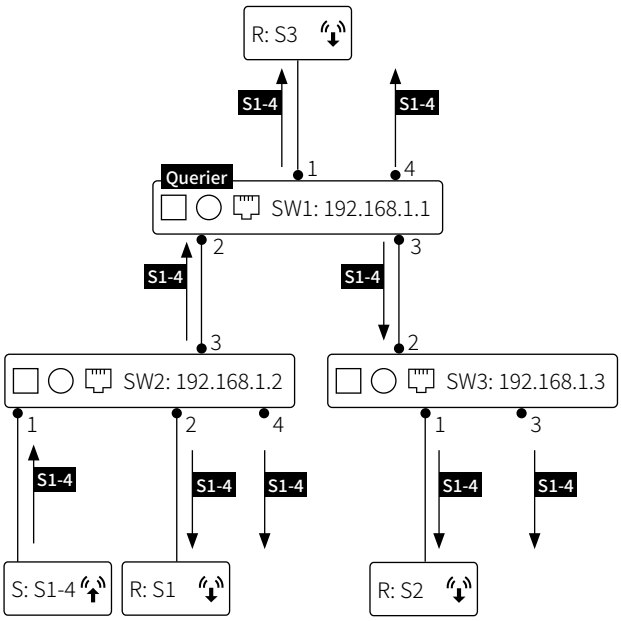
All streams will be broadcasted. You would have the same behaviour when using an unmanaged switch.

3.4 Multicast routing: none of the Receivers implemented IGMP correctly

3.4.1 Normal operation

- Querier enabled
- Unknown Flooding enabled
- IGMP Snooping enabled

Figure 10: Incorrect IGMP implementation

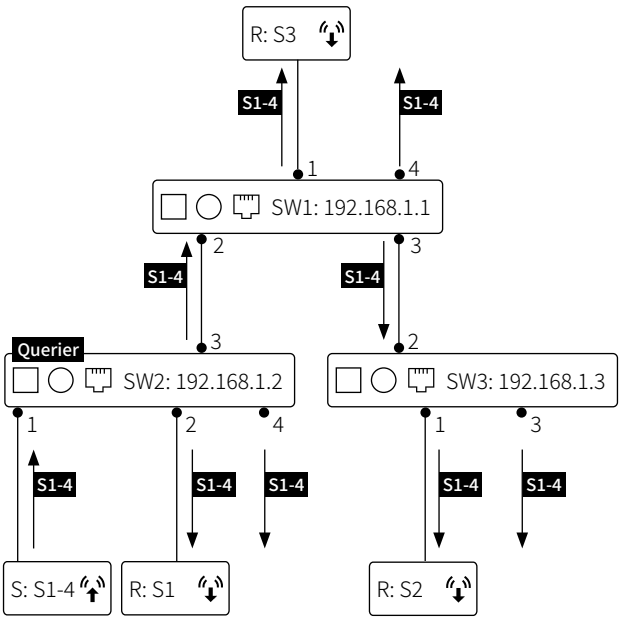


This is the situation you get when Receivers don't support IGMP. You will get the same behavior when using an unmanaged switch or disable IGMP Snooping.
All streams are broadcasted, so all Receivers are flooded with streams they didn't request.

3.4.2 Different Querier

- Querier **disabled** on Switch 1, Switch 2 becomes Querier
- Unknown Flooding enabled
- IGMP Snooping enabled

Figure 11: Incorrect IGMP implementation, different Querier

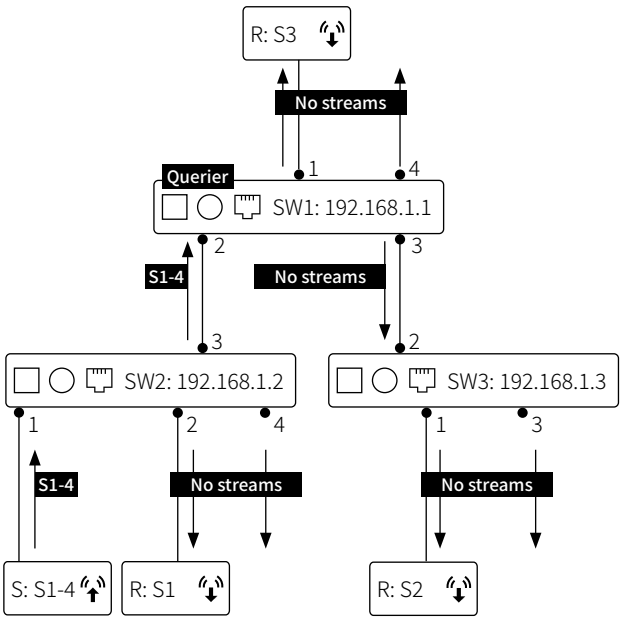


Same behavior as figure 10. The location of the Querier does not make any difference.

3.4.3 Without Unknown Flooding

- Querier enabled
- Unknown Flooding **disabled**
- IGMP Snooping enabled

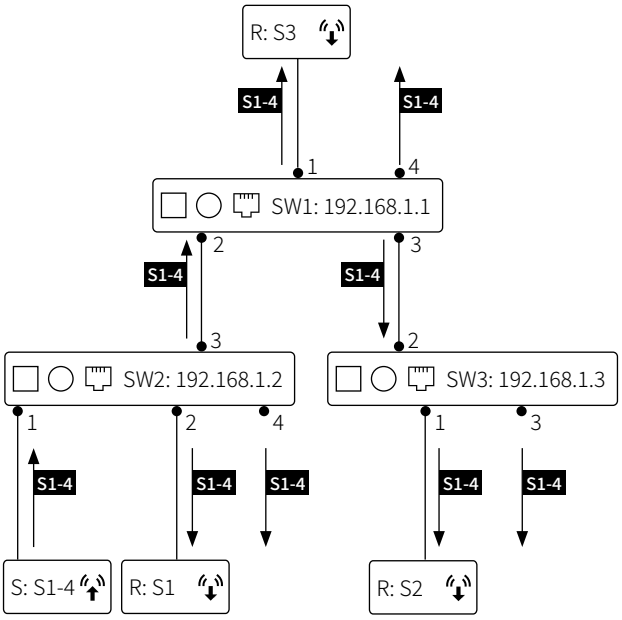
Figure 12: Incorrect IGMP implementation, Unknown Flooding disabled



Disabling Unknown flooding in this situation will prevent streams of reaching the Receivers.

3.4.4 IGMP Snooping disabled

Figure 13: IGMP Snooping disabled



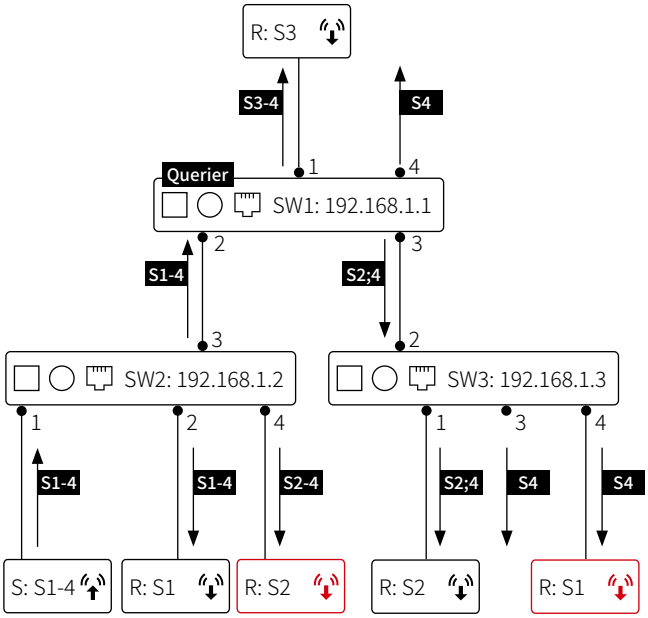
Same as figure 10 and 11. All streams are broadcasted.

3.5 Multicast routing: mix of compliant and non-compliant Receivers

3.5.1 Normal operation

- Querier enabled
- Unknown Flooding enabled
- IGMP Snooping enabled

Figure 14: Compliant and non-compliant Receivers

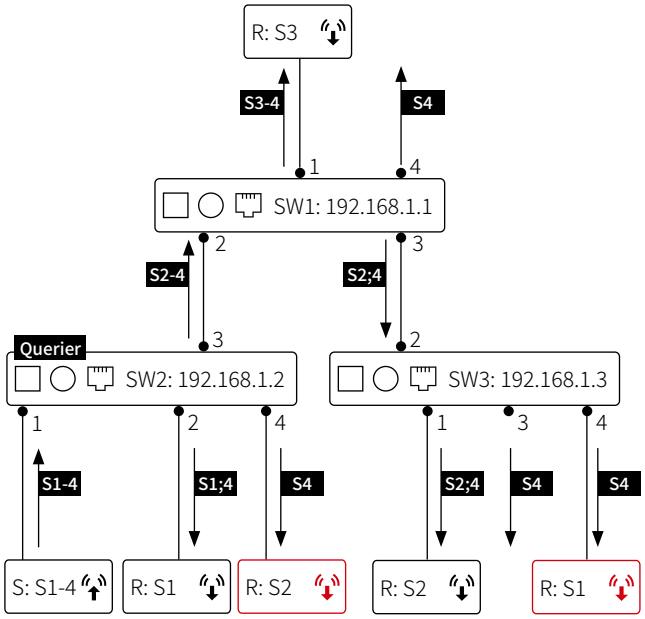


The Receivers in red are non-compliant Receivers. They don't send membership reports. Some Receivers will be flooded, other will not receive the streams they want.

3.5.2 Different Querier

- Querier disabled on Switch 1, Switch 2 becomes Querier
- Unknown Flooding enabled
- IGMP Snooping enabled

Figure 15: Different Querier

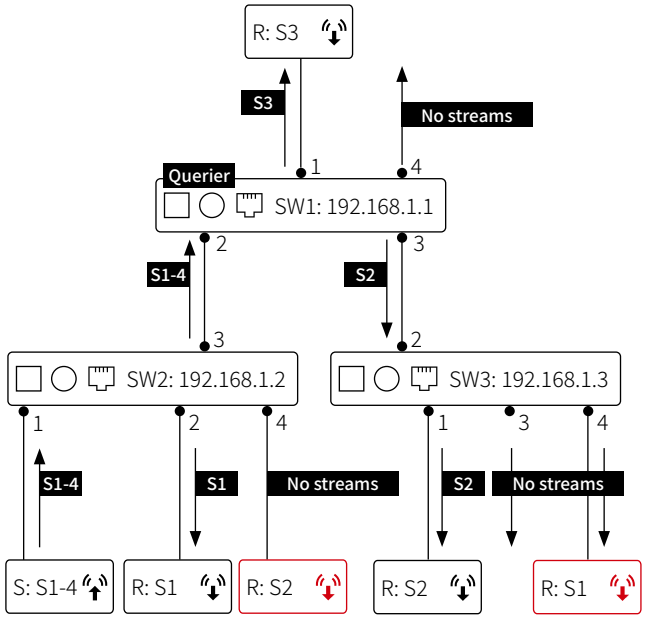


Comparable with the previous situation.
Fewer streams are flooded.

3.5.2 Without Unknown Flooding

- Querier enabled
- Unknown Flooding disabled
- IGMP Snooping enabled

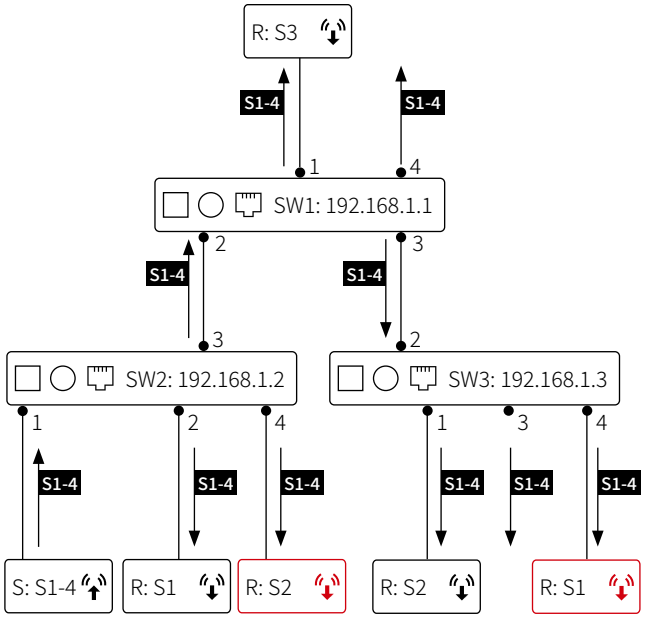
Figure 16: Without Unknown Flooding



No data streams for the non-compliant Receivers.

3.5.4 IGMP Snooping disabled

Figure 17: IGMP Snooping disabled



The streams will be broadcasted.
Every Receiver gets its requested streams but will also be flooded with unwanted streams.

4. CONCLUSION

A correct implementation of IGMP, both at the Receiver and in the switch level, is the best solution to optimize traffic across your network when dealing With Multicast Streams. For that reason, the default settings on all the Gigacore switches are as follows :

- IGMP snooping enabled on all groups : the switch is ready to register and route Multicast Streams.
- Querier is enabled : the switch will participate in the Querier election.
  This ensures that there will be at least one Querier in the network.
- Unknown Flooding is enabled : in case a Receiver doesn't implement IGMP properly, it will have a better chance of receiving the stream for which it is listening. The ideal situation would be to have a correct implementation of IGMP on the switches and the Receivers which would allow to disable unknown flooding. This would prevent any unnecessary forwarding and let the IGMP snooping provide the best traffic optimization.

Hopefully, this document will help make informed choices if you need to modify these settings.

REVISION: 20210826-REV 1.4.

Luminex

Slamstraat 13 | 3600 Genk | Belgium | T +32 11 812 189 | info@luminex.be | www.luminex.world