

# Optimizing multicast performance in professional AV networks.

**A Comprehensive Guide to IGMP Snooping**



# Contents

- 1. Introduction..... 3
- 2. Understanding Multicast..... 3
- 3. The Role and Mechanisms of IGMP Snooping ..... 3
  - 3.1 Understanding IGMP Message Types.....3
  - 3.2 IGMP querier election and the role of the querier .....4
  - 3.3 Example Network Scenarios for IGMP Snooping.....5
- 4. Advanced IGMP Snooping Techniques and GigaCore Configuration 7
- 5. Common Issues and Troubleshooting Strategies..... 8
  - 5.1 Issue: No IGMP Snooping Enabled.....8
  - 5.2 Issue: Specific Devices Not Receiving Multicast .....8
  - 5.3 Issue: Unknown Flooding.....8
  - 5.4 Issue: Multicast Forwarding Database Capacity .....9
  - 5.5 Final Thoughts on Troubleshooting .....9
- 6. FAQ ..... 11
- 7. References ..... 12

## 1. INTRODUCTION

In modern professional audiovisual installations, reliable high-bandwidth data delivery is a critical requirement. Ensuring that multicast streams are efficiently managed is of paramount importance. As AV networks continue to evolve with increasingly demanding applications, understanding how multicast technology functions and how IGMP snooping can be leveraged to optimize network performance is essential knowledge for any technician working in these environments. This document provides a thorough exploration of multicast fundamentals, explains the intricate working principles of IGMP snooping, and delves into the configuration and troubleshooting techniques required for a robust ProAV network.

## 2. Understanding multicast

Multicast is a network communication method, designed to deliver a single data transmission to multiple recipients simultaneously, thereby significantly reducing bandwidth consumption compared to traditional unicast communications. Unlike unicast transmissions—which create separate, repetitive streams for each destination—and broadcast communications—which indiscriminately send data to every device on a segment regardless of need, multicast allows for the targeted delivery of data to a defined group of devices. In this context, devices that subscribe to a particular stream join what is referred to as a multicast group, which enables switches and routers to forward packets only to those segments where active listeners exist. This selective forwarding minimizes unnecessary network traffic and contributes to overall efficiency in environments where multiple endpoints require access to the same data.

## 3. The role and mechanisms of IGMP snooping

In professional AV networking, the efficient transmission of multicast data depends on managing group memberships through the Internet Group Management Protocol (IGMP). IGMP snooping allows network switches to optimize multicast traffic by analyzing IGMP messages exchanged between hosts and routers. Instead of forwarding multicast packets indiscriminately to all devices,

an IGMP-snooping switch intelligently filters multicast streams, ensuring that only subscribed devices receive the data.

This chapter provides a detailed breakdown of the different IGMP message types and explains how IGMP snooping functions in various network scenarios.

### 3.1 Understanding IGMP Message Types

IGMP relies on three primary message types to manage multicast group memberships: Membership Query, Membership Report and the Leave Group message.

#### Membership Query

The IGMP querier—typically a network router or an elected switch—periodically sends membership query messages to determine which devices want to receive multicast data. Queries can be:

- **General Membership Queries:**  
Sent to all devices in the network, asking them if they require multicast traffic from any group.
- **Group-Specific Membership Queries:**  
Target a particular multicast group (e.g., multicast group 239.255.0.1), asking whether any devices need data from that specific stream.

#### Example

Consider a lighting control system with multiple fixtures subscribing to different multicast streams. Every 125 seconds, the network's IGMP querier sends a general query asking, "Which devices need multicast?" In response, fixtures receiving lighting control commands via multicast protocols (like sACN) will confirm their membership with a Membership Report, ensuring that their data flow is maintained.

## Membership Report

When a device wishes to receive a specific multicast stream, it responds to a querier's Membership Query or initiates its own membership request by sending an IGMP membership report. The membership report informs the network that the device wants to receive traffic from a designated multicast group (e.g., multicast group 239.255.0.2).

Sending out an unsolicited membership report right after a connection is established, instead of waiting for the next membership query, will result in the device receiving the requested multicast data faster.

### Example

Imagine an audio system in a concert venue where loudspeakers are connected via multicast audio streams. When the querier asks, "Who needs multicast?" speakers assigned to process multicast group 239.255.0.3 will send membership reports indicating their desire to receive data from this stream. The switch then forwards only the relevant multicast packets to those speakers, reducing unnecessary traffic.

## Leave Group

When a device no longer requires multicast data, it sends a leave message to indicate that it is unsubscribing from the multicast stream. The querier may then issue a Group-Specific Query to confirm whether any remaining devices in the network still require the multicast data for that group address. If no responses are received, the querier instructs the switch to stop forwarding that stream towards the device that issued the Leave Group message.

### Example

A video distribution system in a broadcast facility is streaming a feed via multicast group 239.255.0.4. If an inactive receiver stops replaying the stream, it sends a leave message to the network. The querier may issue a follow-up group-specific query to check if other devices in that network segment still need the stream. If no other devices respond, the network stops forwarding that multicast feed to the one, inactive receiver.

## 3.2 IGMP Querier Election and the Role of the Querier

### The role of the IGMP Querier

In an IPv4 multicast-enabled network, the IGMP querier plays a vital role in coordinating multicast group memberships. Without a querier, multicast devices would not receive periodic membership queries, making it difficult to maintain an accurate list of active multicast group participants. The querier ensures that devices that need multicast traffic remain registered while those that no longer require it are removed from the forwarding table. By periodically sending general membership queries, the querier prompts all multicast receivers in the network to confirm their continued membership in multicast groups. Additionally, the querier issues group-specific queries when a device leaves a multicast group to determine whether any other devices still require data from that particular stream. This process ensures that multicast traffic is efficiently routed to only the necessary endpoints, preventing unnecessary data transmission across the network.

### IGMP Querier Election Process

In networks with multiple IGMP querier-capable devices, an election process determines which device will assume the role of the querier. This election is crucial because a network must have exactly one active querier per VLAN to ensure proper multicast group management. The election follows these key principles:

#### ■ 1. Lowest IP Address Wins

IGMP querier election is based on the device's IGMP querier IP address. The device with the lowest IGMP querier IP address in the subnet becomes the active querier and takes responsibility for sending queries. You can compare the IGMP querier IP address with a priority number as used in other protocols such as PTPv2 Priority1 or RTSP Bridge priority.

#### ■ 2. Automatic Querier Replacement

If the active querier fails or is removed from the network, the remaining IGMP-capable devices reinitiate the election process. The device with the next lowest IP address takes over as the new querier.

### 3. Querier Election in Multi-Switch Networks

When multiple switches support IGMP querier functionality, only one querier is active at any given time within a VLAN. If a higher-priority switch joins the network with a lower IP address, it will take over querier duties, replacing the previous querier.

#### Impact of the Querier on IGMP Snooping

IGMP snooping depends on the presence of an active querier because it relies on membership queries to detect which ports should receive multicast traffic. Without a querier:

- Switches may fail to maintain multicast group registrations, leading to unwanted traffic flooding or dropped multicast streams.
- Some devices may lose access to multicast streams because there are no active queries prompting their membership reports.
- The network may experience delays in processing leave messages, causing lingering multicast traffic to be delivered to unsubscribed devices.

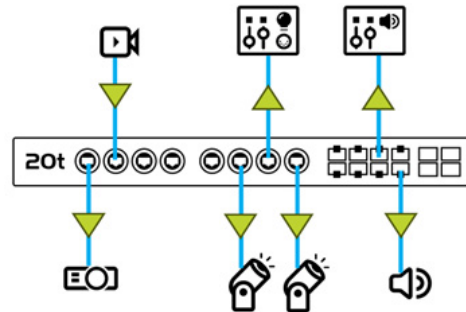
For this reason, it is essential that at least one IGMP-capable device participates in querier elections and remains active in the network.

### 3.3 Example Network Scenarios for IGMP Snooping

Below are three practical examples illustrating how IGMP snooping ensures multicast traffic is managed efficiently.

#### Scenario 1: Uncontrolled Multicast Traffic Without IGMP Snooping

In an unmanaged network where IGMP snooping is disabled, multicast traffic behaves similarly to broadcast traffic. Consider a network with multiple lighting fixtures, loudspeakers, and video processing devices, all connected in the same VLAN:

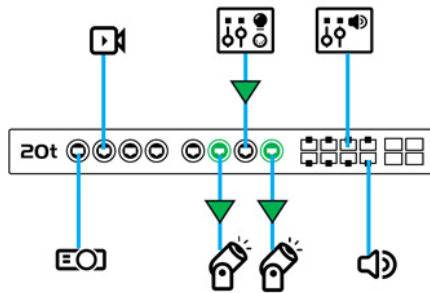


▼ = Video stream with destination IP 239.255.0.10

- The video camera transmits a video stream using multicast group 239.255.0.10.
- Without IGMP snooping, every device receives these packets, even if they do not need them.
- Devices not participating in the multicast group waste processing power handling unnecessary traffic.
- Without multicast filtering, excessive traffic can congest network bandwidth, degrade performance, and cause delays in sensitive AV applications.

### Scenario 2: Optimized Multicast Routing with IGMP Snooping

Consider a well-configured AV installation using IGMP snooping:



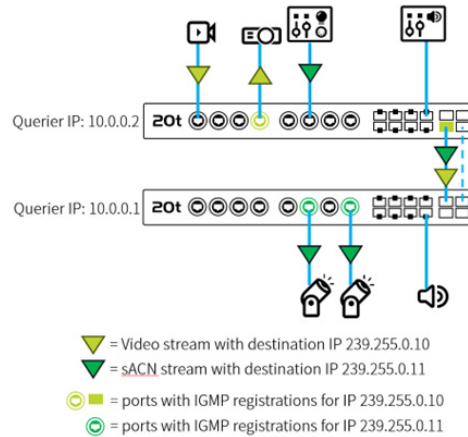
- ▼ = sACN stream with destination IP 239.255.0.11
- = ports with IGMP registrations for IP 239.255.0.11

- A lighting console sends multicast control commands via multicast group 239.255.0.11 (sACN universe 11).
- Fixtures in the network subscribe to this multicast group by responding to queries with membership reports.
- The network switch records IGMP registrations and forwards data only to the subscribed fixtures.
- Devices that did not request multicast group 239.255.0.11 do not receive unnecessary traffic, ensuring optimized bandwidth usage.

IGMP snooping enables efficient routing, reducing multicast congestion, and improving overall network stability.

### Scenario 3: Querier Election and Multicast Data Flow

In a large-scale concert venue using multiple inter-connected switches, an IGMP querier election ensures structured multicast flow:



- Several network switches participate in querier election.
- The switch with the lowest IP address (e.g., 10.0.0.1) is elected as the IGMP querier.
- The querier sends general membership queries at 125-second intervals.
- Multicast traffic from the source is efficiently routed through the switch network, ensuring only subscribed devices receive the audio stream.
- All multicast data will always be forwarded in the direction of the IGMP querier.

This structured approach ensures that multicast packets flow efficiently, and that redundant traffic is eliminated.

## 4. Advanced IGMP snooping techniques and GigaCore configuration

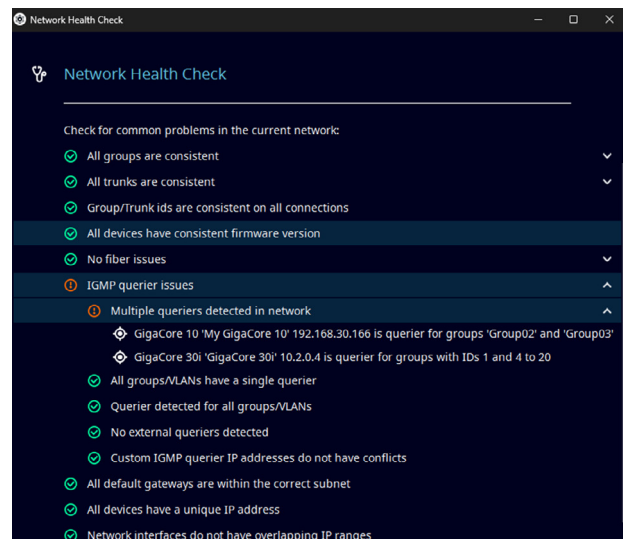
Modern ProAV networks often rely on advanced switching solutions to fully harness the benefits of IGMP snooping, and the Luminex GigaCore series is a prime example of hardware that integrates this capability seamlessly. In these systems, IGMP snooping is enabled by default, which allows the switches to automatically evaluate IGMP messages and maintain an up-to-date forwarding database without requiring extensive manual intervention. The GigaCore configuration includes several finely tuned parameters that can be adjusted to match the specific demands of a given network environment.

For example, one critical setting is the handling of unknown multicast traffic. When multicast packets arrive that do not have an associated IGMP registration, the decision must be made whether to treat these packets as requiring immediate broadcast to all network segments or to drop them entirely. In many cases, unknown flooding is disabled to prevent inadvertent network congestion, ensuring that only explicitly registered multicast streams are forwarded. Enabling unknown flooding can be necessary to allow multicast data in VLANs with IGMP disabled.

Another parameter is the “Fast Leave” feature, which allows the network to immediately cease forwarding a multicast stream to a port as soon as it receives an IGMP leave message from the last known device in a network segment that was subscribed to that multicast stream. This immediate cutoff is particularly valuable in high-data-rate scenarios, such as video feeds, where timely removal of unneeded streams can conserve precious bandwidth.

One of the more complex aspects of configuring IGMP snooping in networks involves the determination of the IGMP querier. In a typical network segment, the device with the lowest IP address is elected to assume this role, thereby coordinating the IGMP query messaging process across the network. It is not uncommon for large networks to require customized querier IP addresses to ensure that the designated querier is optimally positioned within a specific subnet, a matter that is crucial

for maintaining efficiency in multicast registration and traffic distribution. In addition to these system-level configurations, tools such as Araneo’s health checks and IGMP overlay provide technicians with visual insight into the location of the querier and the current state of multicast registrations. This level of monitoring and diagnostic capability enables proactive troubleshooting and robust network management.



## 5. Common issues and troubleshooting strategies

Despite the advantages of IGMP snooping in optimizing multicast traffic, several challenges can arise in professional AV networks. If not correctly configured, multicast traffic may be inefficiently transmitted, causing unnecessary congestion, device malfunctions, or system instability. This chapter outlines some common issues encountered in IGMP-managed networks, along with structured troubleshooting approaches to resolve them.

### 5.1 Issue: No IGMP Snooping Enabled

#### Problem Overview

In networks where IGMP snooping is disabled or unsupported, multicast traffic can be treated as broadcast, or multicast data can be completely blocked by the switches. This can depend on the 'unknown flooding' setting inside the switches.

When multicast data is handled as broadcast, it means that every device on the network receives multicast packets, even if they are not intended to process them. Such behavior can lead to network congestion, excessive bandwidth consumption, and overloaded devices.

#### Symptoms

- Increased network traffic with unnecessary multicast flooding.
- Certain devices experiencing performance degradation or dropped packets.
- High CPU utilization on endpoints due to unwanted traffic processing.

#### Troubleshooting & Solutions

##### 1. Verify IGMP Snooping Capability

- Confirm that network switches support IGMP snooping.
- All Luminex GigaCore switches have IGMP snooping enabled by default.

##### 2. Ensure IGMP Snooping is Enabled

- Access the switch configuration interface and check IGMP snooping settings.
- Validate that snooping is active using Araneo health checks.

##### 3. Confirm IGMP Querier Presence

- IGMP snooping requires an active querier; ensure at least one switch participates in the querier election.
- Use Araneo's IGMP overlay to verify the querier location.

### 5.2 Issue: Specific Devices Not Receiving Multicast

#### Problem Overview

In some cases, certain devices fail to receive multicast traffic due to incomplete IGMP implementations or incompatibilities. This issue is often observed with devices that do not properly register to receive multicast data.

#### Symptoms

- One brand or model of devices does not respond to multicast.
- The affected devices do not appear in the IGMP registration table.
- Other devices receive multicast normally.

#### Troubleshooting & Solutions

##### 1. Check IGMP Registrations

- Use Araneo's IGMP registration analysis to verify multicast group memberships.

## 2. Investigate Device IGMP Implementation

- Some devices may lack IGMP support entirely.
- If the device runs (embedded) Linux, “Reverse Path Filtering” might be enabled—this may block multicast traffic if the Querier IP address is not in the same subnet as the device IP.

## 3. Adjust IGMP Querier IP Address

- Modify the querier IP to match the same subnet as the affected device.

## 4. Consider Workarounds

- Disable IGMP snooping on specific network segments (⚠ this converts multicast to broadcast). If unknown flooding is a device setting, it might be required to turn it on when IGMP is disabled so that multicast will not be dropped.
- Specific to lighting networks:
  1. Place incompatible devices in separate groups (VLANs) and use Luminex LumiCore to route sACN to those groups.
  2. Switch to alternative protocols such as Art-Net or sACN unicast. Art-Net uses broadcast data transmission by default and therefore does not need IGMP.
- Use an inline device with correct IGMP implementation as an intermediary to receive and forward multicast data.

## 5.3 Issue: Unknown Flooding

### Problem Overview

Unknown flooding occurs when multicast packets that lack registered recipients are automatically broadcasted to the entire network. This can lead to excessive data transmission and unexpected behavior when devices receive unnecessary traffic.

### Symptoms

- Multicast traffic behaves like broadcast, reaching unintended devices.
- Excessive traffic volume and network congestion.
- Multicast flows seem unpredictable when new devices or applications are introduced. The introduction of those devices or applications can result in certain multicast streams being ‘known’. From that point on, the streams will only be forwarded to receivers that have subscribed to the address and any device that did not register will no longer get the multicast data.

### Troubleshooting & Solutions

#### 1. Understand the Risks of Unknown Flooding

- When enabled, all unknown multicast streams are treated as broadcast, potentially overwhelming the network.
- When disabled, unregistered multicast streams are dropped, reducing unnecessary traffic.

#### 2. Disable Unknown Flooding (Recommended and default setting)

- Navigate to the GigaCore IGMP settings and ensure unknown flooding is turned off.

#### 3. Confirm Proper Multicast Registration

- Unexpected multicast behavior may result from missing or delayed device registrations.
- Ensure all multicast clients correctly request IGMP group membership. This can be validated using the Araneo device IGMP table.

	Group	Trunk	VLAN ID	Multicast Address	Ports	Protocol (*)
Traffic	Ravenna		300	224.0.1.129	20, 22	PTP/primary
PoE	Ravenna		300	236.4.1.0	28	MA-Net3 Admin
AVB	Ravenna		300	239.192.243.243	28	RLinkX
IGMP	Ravenna		300	239.192.243.244	28	Araneo Telemetry
MA-Net	Ravenna		300	239.255.255.250	28	Simple Service Discovery Protocol
System	sACN		700	239.255.255.255	20, 22	Dante (AES67 discovery) / SAP
	sACN		700	238.210.10.3	1, 28	RTTRPL
	sACN		700	239.255.0.1	28	Streaming ACN (Universe 1)
	sACN		700	239.255.0.2	28	Streaming ACN (Universe 2)
	sACN		700	239.255.0.3	28	Streaming ACN (Universe 3)
	sACN		700	239.255.0.4	28	Streaming ACN (Universe 4)
	sACN		700	239.255.0.5	28	Streaming ACN (Universe 5)
	sACN		700	239.255.0.6	28	Streaming ACN (Universe 6)
	sACN		700	239.255.0.7	28	Streaming ACN (Universe 7)
	sACN		700	239.255.0.8	28	Streaming ACN (Universe 8)
	sACN		700	239.255.0.9	28	Streaming ACN (Universe 9)

## 5.4 Issue: Multicast Forwarding Database Capacity

### Problem Overview

Network switches maintain an internal Multicast Forwarding Database (MFDB), which stores entries for multicast streams. However, every switch has a finite number of MFDB entries, and exceeding this limit can disrupt multicast traffic.

### Symptoms

- Additional multicast streams fail to register or reach intended devices.
- Unexpected drops in multicast traffic as entries are overwritten or discarded.
- Certain multicast traffic behaves like a broadcast, reaching unintended devices.

### Troubleshooting & Solutions

#### 1. Determine MFDB Capacity

- Standard switches typically support 256–512 multicast entries.
- Luminex GigaCore switches support 980 entries.

#### 2. Optimize Multicast Usage

- Each multicast address, so also each sACN universe, consumes one MFDB entry.
- Minimize unnecessary multicast groups if nearing hardware limitations.

#### 3. Evaluate Scaling Options

- Consider network segmentation strategies to distribute multicast load.
- Consider enabling unknown flooding such that streams that don't get registered because of the limit will be flooded in the network.
- Upgrade switch hardware if multicast usage is expected to exceed current MFDB limits.
- Luminex is working on solutions to extend the network-wide limit beyond 1,000 multicast entries.

## 5.5 Final Thoughts on Troubleshooting

When working with IGMP snooping in ProAV networks, structured diagnostics and proper configuration are crucial to maintaining optimal performance. Whether the issue is related to snooping misconfigurations, device compatibility or unknown flooding, technicians can mitigate problems through proactive monitoring and effective system adjustments. Tools like Araneo provide real-time visibility into network behavior, assisting in issue detection and resolution before network congestion or failures occur.

## 6. FAQ

### What happens when an unmanaged switch is connected to a network with IGMP enabled?

This unmanaged switch should be configured to flood all multicast data, including the IGMP messages themselves. The managed switches will only forward multicast data to the unmanaged switch if one of the connected devices is registered to that data. Consequently, the unmanaged switch will flood this data to all connected devices instead of only the device(s) that registered for that specific multicast address.

### In a network with a mix of different switch manufacturers, is IGMP compatible across brands?

IGMP (Internet Group Management Protocol) is defined by the IETF (Internet Engineering Task Force) as an open standard, which means it is designed to work across different vendors. If all switches implement IGMP according to the standard and use consistent timing settings, interoperability is generally achievable.

However, it's important to note that there is no widely adopted certification program specifically for IGMP compatibility. This means that while cross-vendor compatibility is possible, it's not guaranteed. In contrast, certain other networking technologies—such as Audio Video Bridging (AVB)—do have formal certification programs, like those offered by the Avnu Alliance, to ensure interoperability.

### Do you need IGMP snooping in an Art-Net network?

Art-Net itself uses broadcast and unicast packets and therefore does not need IGMP snooping. However, the Art-Net equipment in the network might use other (proprietary) protocols that do use multicast data. Therefore, it can still be a good idea to leave IGMP snooping enabled.

Additionally, Art-Net allows the use of sACN as the DMX data stream. In this case, leaving IGMP snooping in place is very relevant.

### How fast can a newly plugged client register to a specific stream?

Multicast receivers are recommended to transmit an “unsolicited” membership response on a link-up event or when they would like to receive another multicast stream. They don't have to wait on the next membership query message, which can take up to a full query interval, which is by default 125 seconds. These unsolicited membership responses can result in very fast multicast forwarding to the receivers, typically well below 1 second.

### IGMP snooping is disabled, but I don't get Multicast data to the receivers, what can be wrong?

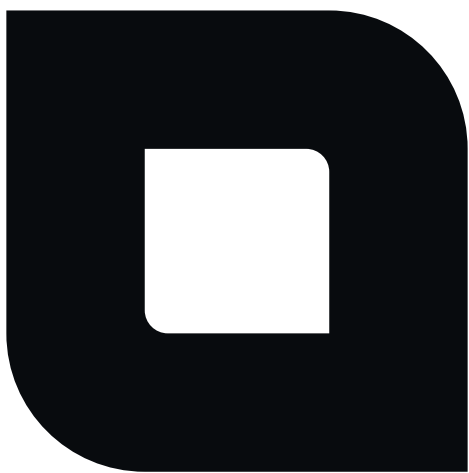
When IGMP snooping is disabled, some switches require that “unknown multicast flooding” is explicitly enabled for multicast traffic to reach the receivers. Without this setting, the switch may block multicast packets altogether.

The behavior varies by switch vendor:

- On some switches, disabling IGMP snooping automatically manages multicast flooding per VLAN.
- On others, “unknown multicast flooding” is a global (device-wide) setting that must be manually enabled. This affects all VLANs on the switch—not just the one where IGMP snooping is disabled—so use caution when changing it.

## 7. References

1. | IGMP White Paper:  
<https://www.luminex.be/wp-content/uploads/2021/08/IP-Multicast-and-IGMP-White-Paper-20210826-REV-1.4-1.pdf>
2. | IETF RFC 2236 – IGMPv2:  
<https://datatracker.ietf.org/doc/html/rfc2236>
3. | IETF RFC 3376 – IGMPv3:  
<https://datatracker.ietf.org/doc/html/rfc3376>
4. | Luminex Knowledge Base:  
<https://support.luminex.be/portal/en/kb/articles/ip-multicast-and-igmp>
5. | IGMP Testing Tool:  
<https://github.com/luminex-lce/igmptester>
6. | Luminex IGMP webinar recording:  
<https://youtu.be/Vyhrd2RnGOo>



**Luminex**

Slamstraat 13 | 3600 Genk | Belgium | T +32 11 812 189 | [info@luminex.be](mailto:info@luminex.be) | [www.luminex.be](http://www.luminex.be)