Application Note
Plena matrix network connection – v1.0

Related Products:
Plena matrix

Severity:
☐ Immediate action required
☐ Action strongly recommended
☒ Informative

Plena matrix network connection

This Application Note describes how to solve Plena matrix loss of connection when connected to a network with lots of multicast traffic.

Table of Contents

1. Introduction

The Plena matrix mixer and amplifier both have an Ethernet connection. With the PC GUI's both devices can be configured and also controlled once an Ethernet connection with the device is established. The protocol used is UDP and the ports used are 12128 (incoming port of Plena matrix) and 12129 (outgoing port of Plena Matrix). These ports need to be open and not firewalled.

With the iOs app it is possible to control the devices as well. When the Plena matrix devices are connected to e.g. an Ethernet port of a WiFi router the iOS devices can control Plena matrix via the wireless network. This is a good solution for small buildings like a shop, bar, gym etc.

For larger solutions like e.g. a hotel, shopping mall, holiday resort etc. a bigger network might be required. In most cases all kind of devices are connected to such a network like e.g. office PC's, video surveillance etc. All these devices generate traffic on the network and some of them require a large bandwidth in order to operate properly. When Plena matrix is connected to a network with UDP multicast traffic the Ethernet connection to the Plena matrix devices might be lost. In those cases it is not possible anymore to configure or control the system via the PC GUI's or iOS app.

This Application Note describes how to examine the network and look for the multicast sources on the network. It explains how to prevent connection loss when Plena matrix is connected to a network with multicast traffic. Note that the example used in this Application Note is specific for the CISCO SG350-10MP 10-Port Gigabit PoE Managed Switch. The feature used in this switch to prevent connection loss of a Plena matrix device might not be available in any other type or brand managed switches.

2. Network connection

The Plena matrix mixer and amplifier both have a 100 Mbps network interface. Both devices have a RJ45 Ethernet communication socket at the rear. In order to simulate a connection loss of a Plena matrix device which is connected to a network the following equipment and software was used:

1. Plena matrix Mixer (PLM-8M8)
2. Plena matrix Power amplifier (PLM-4P220)
3. Plena matrix Call station (PLM-8CS)
4. Plena matrix Wall control panel (PLM-WCP)
5. Plena easy Music source (PLE-SDT)
6. Focusrite 8 channel analog to Dante converter (RedNet 4)
7. PC with Dante controller, Wireshark- and iPerf software (server)
8. PC with Plena matrix GUI's- and iPerf software (client)
9. Cisco SG350-10MP 10-Port Gigabit PoE Managed Switch

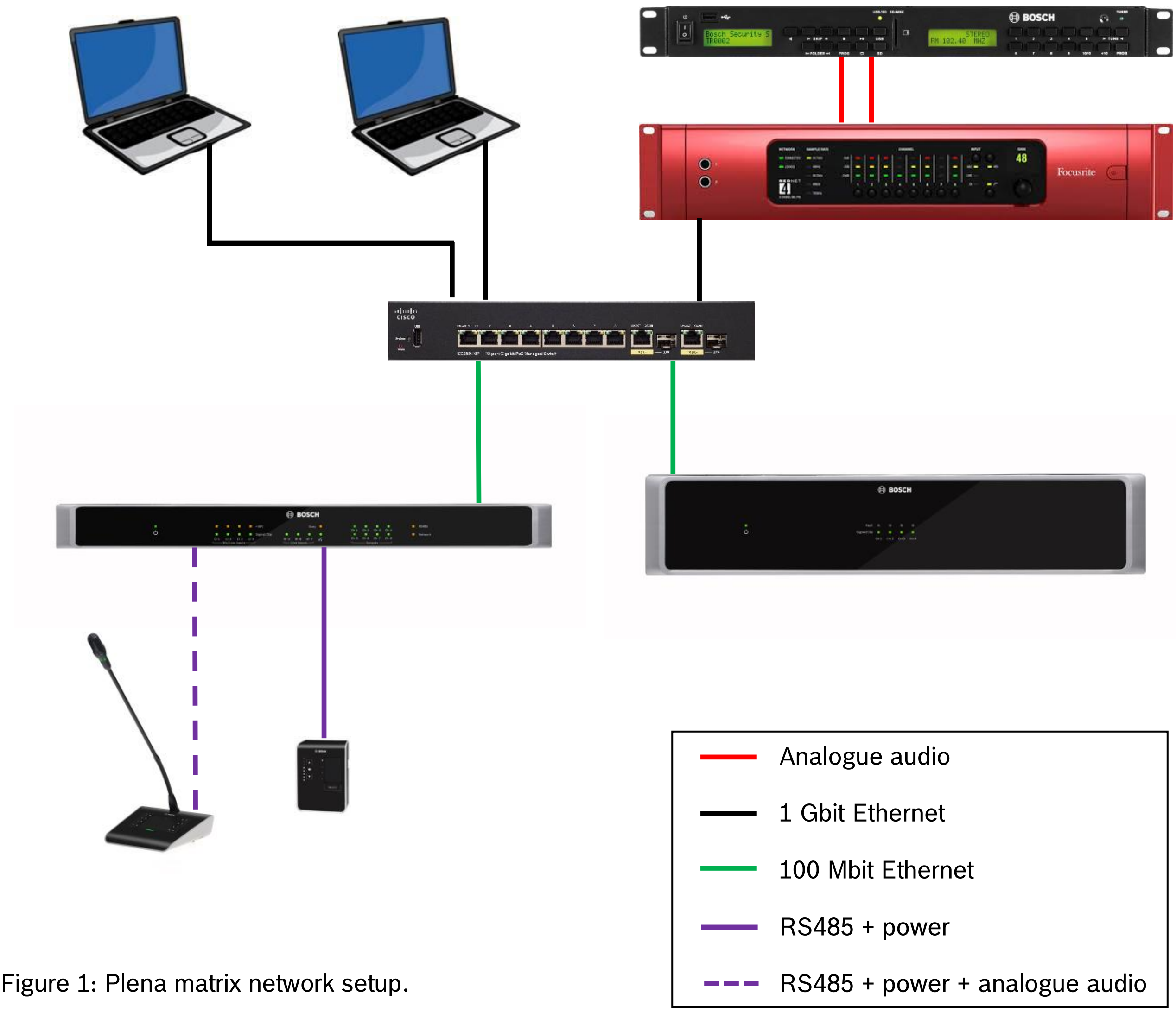
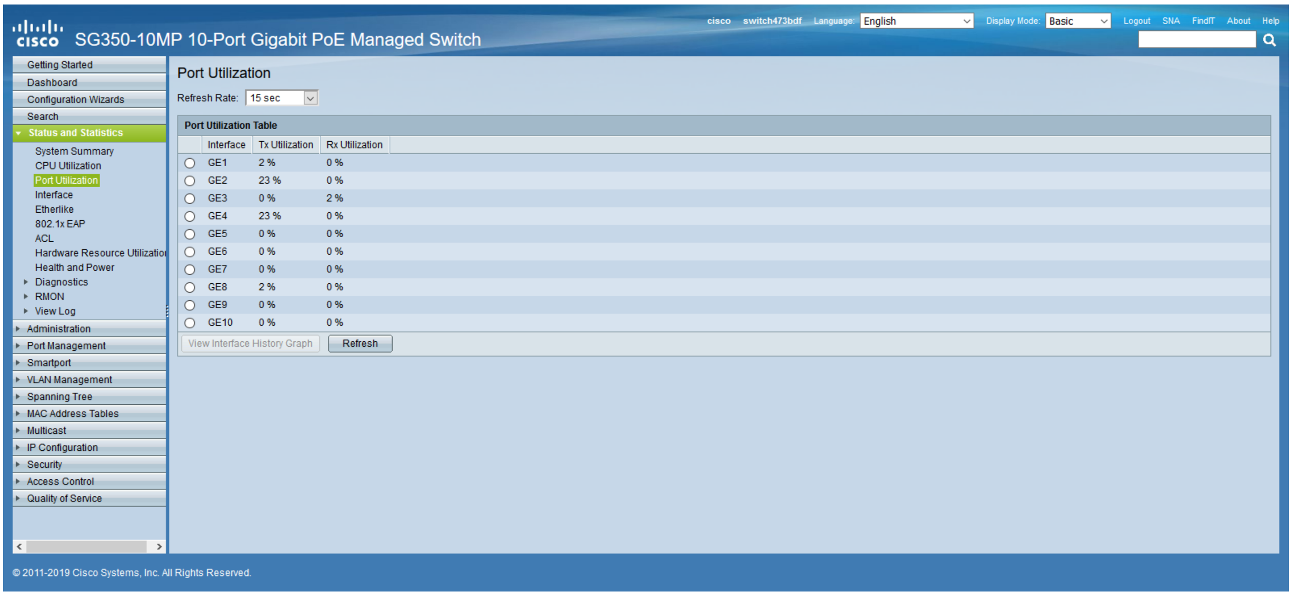


Figure 1: Plena matrix network setup.

3. Multicast network load

In the network setup, see figure 1, the PLE-SDT has two analogue audio connections to the Focusrite RedNet which has a Gigabit Ethernet connection to the Cisco SG350-10MP 10-Port Gigabit PoE Managed Switch. The audio is streamed to the network by the Focusrite RedNet device via Dante™ audio-over-IP. The PC with Dante Controller manages the Dante audio connections and the audio is audible on this PC.

Via the user interface of the Cisco switch the load of the used ports on the switch can be monitored, see figure 2 below. The Focusrite RedNet is connected to port 3 and utilizes 2 % of the bandwidth of the Gigabit port. Both PC's, one on port 1 and the other on port 8, receive this traffic and also utilize 2 % of the bandwidth of their Gigabit connection. Both Plena matrix devices however, amplifier connected to port 2 and mixer connected to port 4, have an utilization of 23 % of their 100 Mbps connection. Note that on these ports the Rx Utilization is 0 %. This means that both Plena matrix devices themselves do not generate any load on the network.


SG350-10MP 10-Port Gigabit PoE Managed Switch

Language: English

Display Mode: Basic

Port Utilization

Refresh Rate: 15 sec

Port Utilization Table

	Interface	Tx Utilization	Rx Utilization
○	GE1	2 %	0 %
○	GE2	23 %	0 %
○	GE3	0 %	2 %
○	GE4	23 %	0 %
○	GE5	0 %	0 %
○	GE6	0 %	0 %
○	GE7	0 %	0 %
○	GE8	2 %	0 %
○	GE9	0 %	0 %
○	GE10	0 %	0 %

© 2011-2019 Cisco Systems, Inc. All Rights Reserved.

Figure 2: Cisco switch port utilization.

With this multicast load on the switch Plena matrix will not show any problem. The connection will not be lost, the "Online" notification of the PC GUI is lit, see figure 3 below. Configuration and control will function as normal.

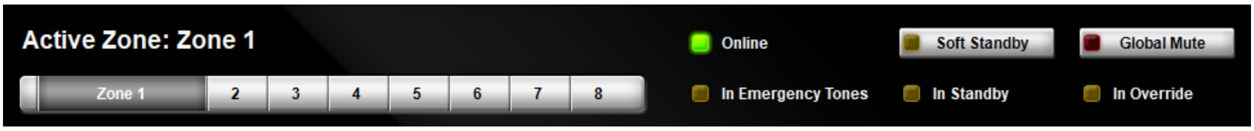
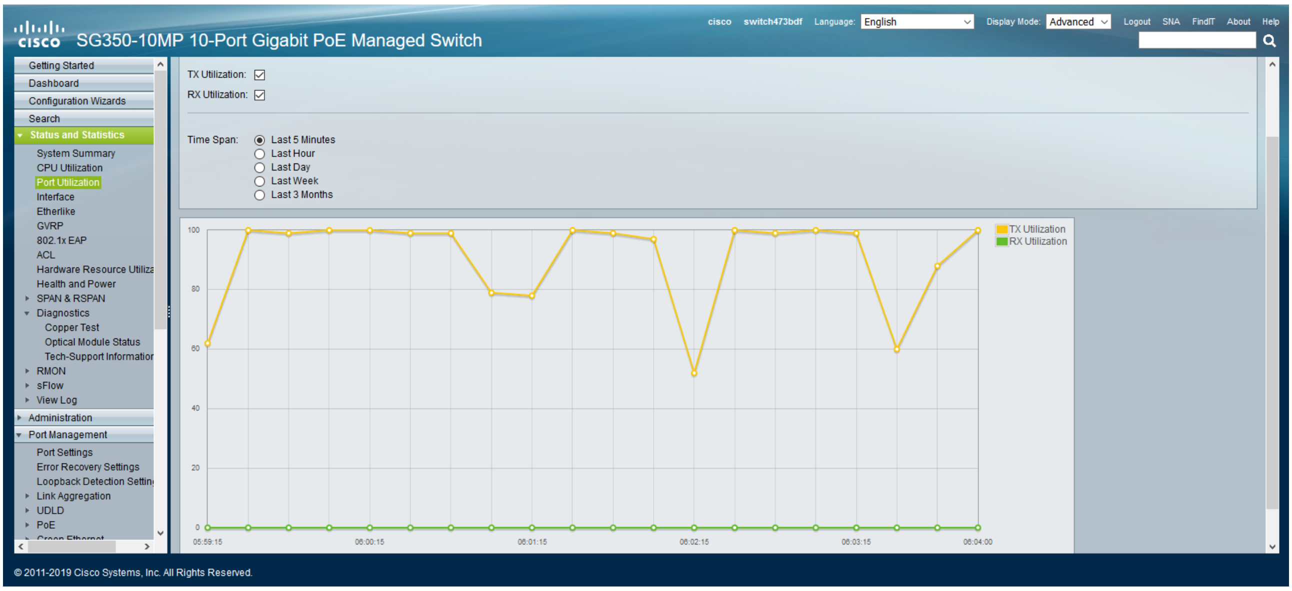


Figure 3: Plena matrix "Online".

In order to increase the multicast traffic in the switch the iPerf software on the PC's is used. iPerf is a widely used tool for network performance measurement and tuning. Iperf has client and server functionality, and can create data streams to measure the throughput between the two ends in one or both directions. Typical Iperf output contains a time-stamped report of the amount of data transferred and the throughput measured.

The data streams can be either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). When used for testing UDP capacity, Iperf allows the user to specify the datagram size and provides results for the datagram throughput and the packet loss. With a bandwidth of 100 Mbps or more the port utilization of the Plena matrix port reaches 100 %, see figure 4 below.

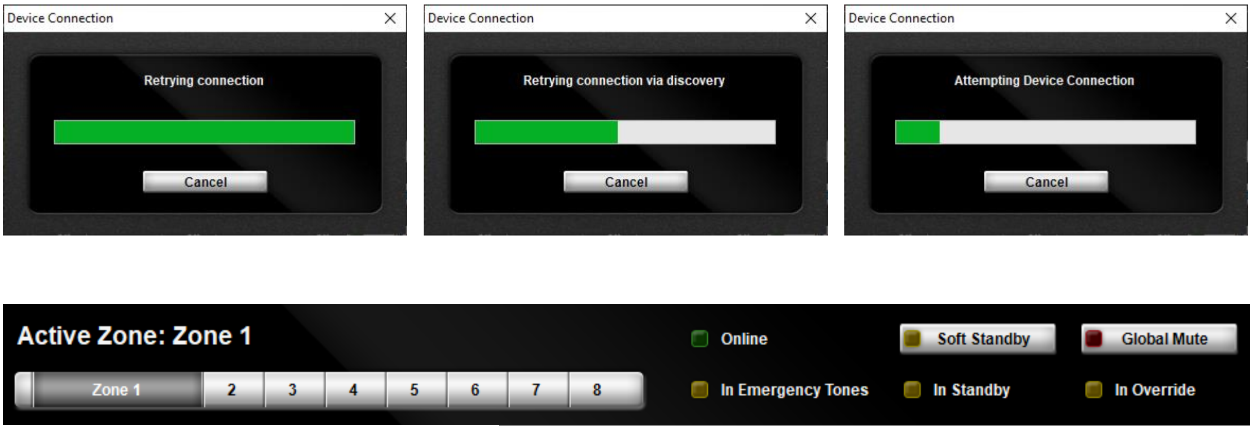


TX Utilization: ☑
RX Utilization: ☑

Time Span: ● Last 5 Minutes ○ Last Hour ○ Last Day ○ Last Week ○ Last 3 Months

Figure 4: Cisco switch port utilization.

When the multicast traffic is increased to approximately 300 Mbps the Ethernet connection with the Plena matrix device is lost. When using the PC GUI a "Device Connection" pop up window will appear, see sequence in figure 5 below. Cancel this attempt to connect to the device and notice that the "Online" notification of the PC GUI is not lit anymore.



Retrying connection

Retrying connection via discovery

Attempting Device Connection

Active Zone: Zone 1

Figure 5: Plena matrix offline.

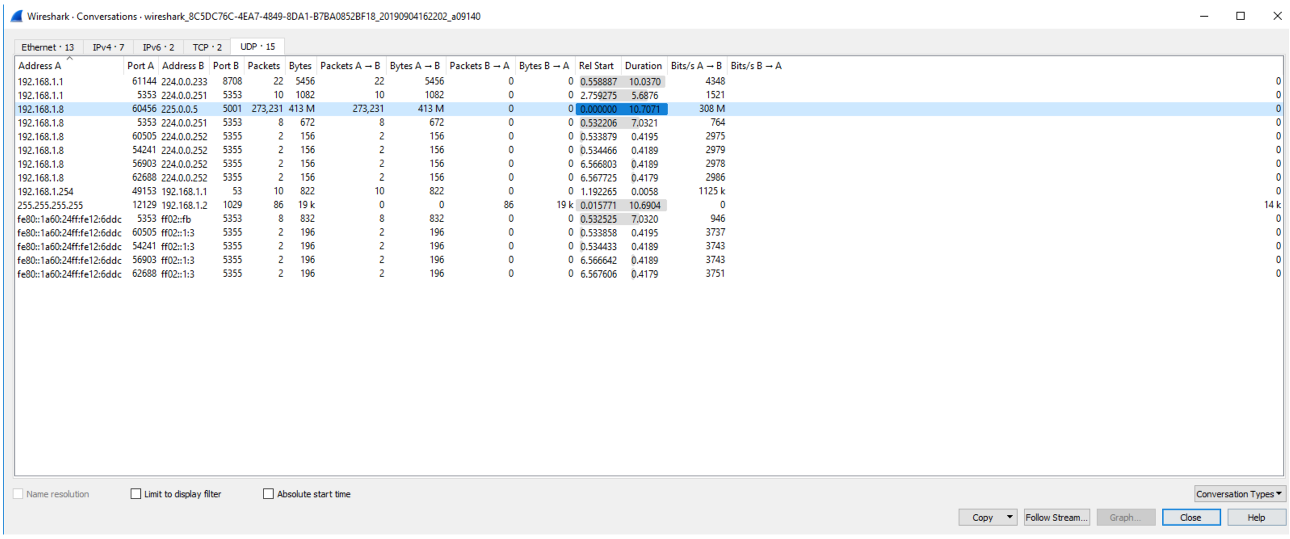
4. Multicast filtering

In order to be able to filter out the Multicast traffic on the port where the Plena matrix devices are connected to it must be clear where it originates from and what the destination is. Once this data is known that specific traffic can be blocked or ignored at any port of the managed switch where it is not relevant for.

4.1. Look for Multicast streams

The Multicast traffic on a network can be found by using network protocol analyzers like e.g. Wireshark. Start capturing packages by clicking on the blue shark fin icon on the left top corner. Let it run for about 10 seconds and stop capturing by clicking the red square icon next to it. Save this File > Save As… for further investigation.

In Wireshark under Statistics there is an option called “Conversations”, see figure 6 below.



Wireshark · Conversations · wireshark_8C5DC76C-4EA7-4849-8DA1-B7BA0852BF18_20190904162202_a09140

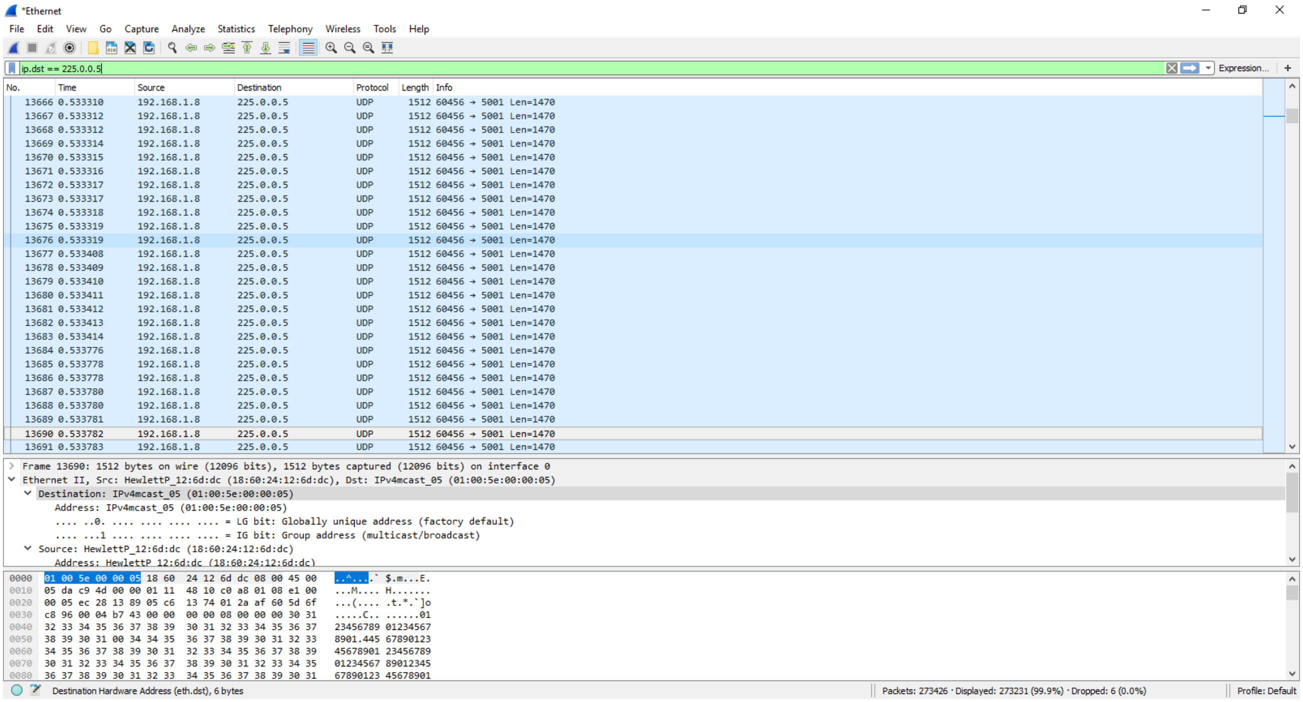
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.1	61144	224.0.0.233	8708	22	5456	22	5456	0	0	0.558887	10.0370	4348	0
192.168.1.1	5353	224.0.0.251	5353	10	1082	10	1082	0	0	2.759275	5.6876	1521	0
192.168.1.8	60456	225.0.0.5	5001	273,231	413 M	273,231	413 M	0	0	0.000000	10.7071	308 M	0
192.168.1.8	5353	224.0.0.251	5353	8	672	8	672	0	0	0.532206	7.0321	764	0
192.168.1.8	60505	224.0.0.252	5355	2	156	2	156	0	0	0.533879	0.4195	2975	0
192.168.1.8	54241	224.0.0.252	5355	2	156	2	156	0	0	0.534466	0.4189	2979	0
192.168.1.8	56903	224.0.0.252	5355	2	156	2	156	0	0	6.566803	0.4189	2978	0
192.168.1.8	62688	224.0.0.252	5355	2	156	2	156	0	0	6.567725	0.4179	2986	0
192.168.1.254	49153	192.168.1.1	53	10	822	10	822	0	0	1.192265	0.0058	1125 k	0
255.255.255.255	12129	192.168.1.2	1029	86	19 k	0	0	86	19 k	0.015771	10.6904	0	14 k
fe80::1a60:24ff:fe12:6ddc	5353	ff02::fb	5353	8	832	8	832	0	0	0.532525	7.0320	946	0
fe80::1a60:24ff:fe12:6ddc	60505	ff02::1:3	5355	2	196	2	196	0	0	0.533858	0.4195	3737	0
fe80::1a60:24ff:fe12:6ddc	54241	ff02::1:3	5355	2	196	2	196	0	0	0.534433	0.4189	3743	0
fe80::1a60:24ff:fe12:6ddc	56903	ff02::1:3	5355	2	196	2	196	0	0	6.566642	0.4189	3743	0
fe80::1a60:24ff:fe12:6ddc	62688	ff02::1:3	5355	2	196	2	196	0	0	6.567606	0.4179	3751	0

Figure 6: Wireshark Statistics - Conversations.

Select the tab ‘UDP • 15’ and look for the row with a large number of Packets. Note the destination address, in this case 225.0.0.5. Go back to the main window with all captured packages and filter out this destination by typing in the following on the display filter text field on top:

ip.dst == 225.0.0.5

See the result in figure 7 below.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

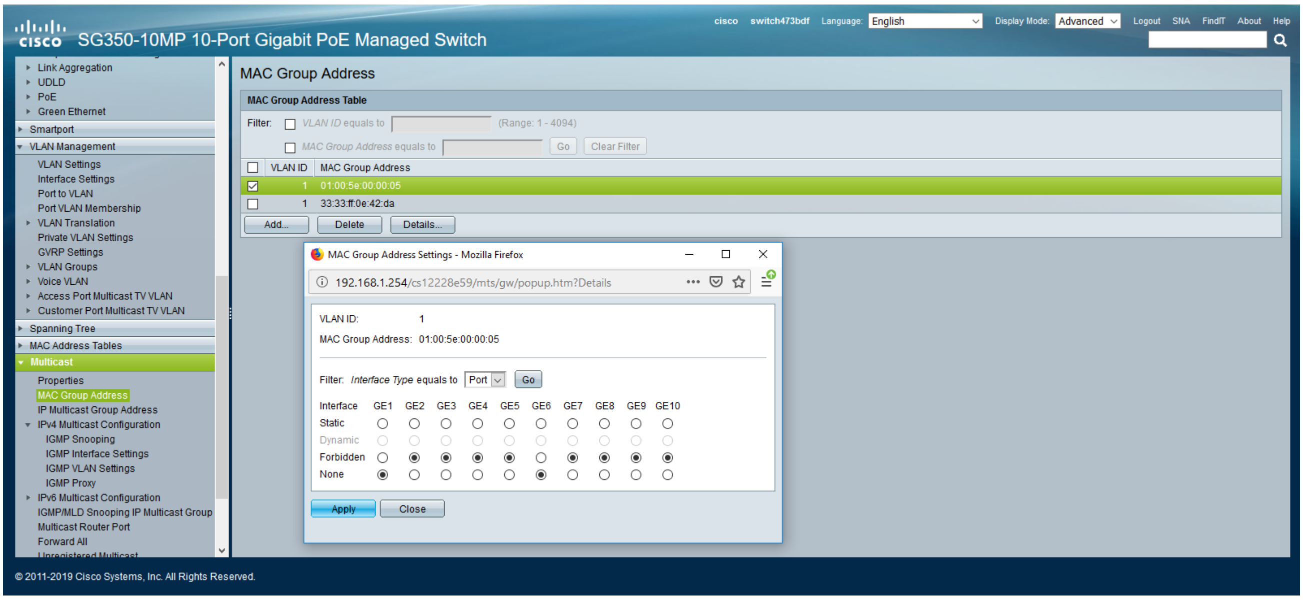
```
ip.dst == 225.0.0.5

No.   Time     Source       Destination  Protocol Length Info
13666 0.533310 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13667 0.533312 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13668 0.533312 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13669 0.533314 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13670 0.533315 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13671 0.533316 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13672 0.533317 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13673 0.533317 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13674 0.533318 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13675 0.533319 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13676 0.533319 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13677 0.533408 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13678 0.533409 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13679 0.533410 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13680 0.533411 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13681 0.533412 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13682 0.533413 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13683 0.533414 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13684 0.533776 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13685 0.533778 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13686 0.533778 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13687 0.533780 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13688 0.533780 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13689 0.533781 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13690 0.533782 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470
13691 0.533783 192.168.1.8  225.0.0.5    UDP      1512 60456 → 5001 Len=1470

> Frame 13690: 1512 bytes on wire (12096 bits), 1512 bytes captured (12096 bits) on interface 0
v Ethernet II, Src: HewlettP_12:6d:dc (18:60:24:12:6d:dc), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
  v Destination: IPv4mcast_05 (01:00:5e:00:00:05)
      Address: IPv4mcast_05 (01:00:5e:00:00:05)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: HewlettP_12:6d:dc (18:60:24:12:6d:dc)
      Address: HewlettP_12:6d:dc (18:60:24:12:6d:dc)

0000  01 00 5e 00 00 05 18 60  24 12 6d dc 08 00 45 00   ..^....` $.m...E.
0010  05 da c9 4d 00 00 01 11  48 10 c0 a8 01 08 e1 00   ...M.... H.......
0020  00 05 ec 28 13 89 05 c6  13 74 01 2a af 60 5d 6f   ...(.... .t.*.`]o
0030  c8 96 00 04 b7 43 00 00  00 00 08 00 00 00 30 31   .....C.. ......01
0040  32 33 34 35 36 37 38 39  30 31 32 33 34 35 36 37   23456789 01234567
0050  38 39 30 31 00 34 34 35  36 37 38 39 30 31 32 33   8901.445 67890123
0060  34 35 36 37 38 39 30 31  32 33 34 35 36 37 38 39   45678901 23456789
0070  30 31 32 33 34 35 36 37  38 39 30 31 32 33 34 35   01234567 89012345
0080  36 37 38 39 30 31 32 33  34 35 36 37 38 39 30 31   67890123 45678901

Destination Hardware Address (eth.dst), 6 bytes    Packets: 273426 · Displayed: 273231 (99.9%) · Dropped: 6 (0.0%)    Profile: Default
```

Figure 7: IP destination filter.

Below the packet trace look for the IPv4mcast_05 MAC address, in this case 01:00:5e:00:00:05. This MAC address will be used in the Multicast filter settings of the Managed Switch.

4.2. Filter Multicast traffic

Note that the example below is specific for the CISCO SG350-10MP 10-Port Gigabit PoE Managed Switch. In this switch it is possible to create a Multicast MAC Group Address. Create a MAC Group Address for 01:00:5e:00:00:05 in this case. Within this group it is possible to exclude specific ports of the switch from this group, see figure 8 below. In this example port 1 and port 6 are excluded. When the Plena matrix devices are connected to one of these ports they will not receive any multicast traffic for that specific destination. In that way the network interface of the Plena matrix devices will not be overloaded and will stay connected without any issue.



MAC Group Address

MAC Group Address Table

Filter: □ VLAN ID equals to (Range: 1 - 4094)

□ MAC Group Address equals to Go Clear Filter

□	VLAN ID	MAC Group Address
☑	1	01:00:5e:00:00:05
□	1	33:33:ff:0e:42:da

Add... Delete Details...

MAC Group Address Settings - Mozilla Firefox

192.168.1.254/cs12228e59/mts/gw/popup.htm?Details

VLAN ID: 1

MAC Group Address: 01:00:5e:00:00:05

Filter: *Interface Type* equals to Port Go

Interface	GE1	GE2	GE3	GE4	GE5	GE6	GE7	GE8	GE9	GE10
Static	○	○	○	○	○	○	○	○	○	○
Dynamic	○	○	○	○	○	○	○	○	○	○
Forbidden	○	●	●	●	●	○	●	●	●	●
None	●	○	○	○	○	●	○	○	○	○

Apply Close

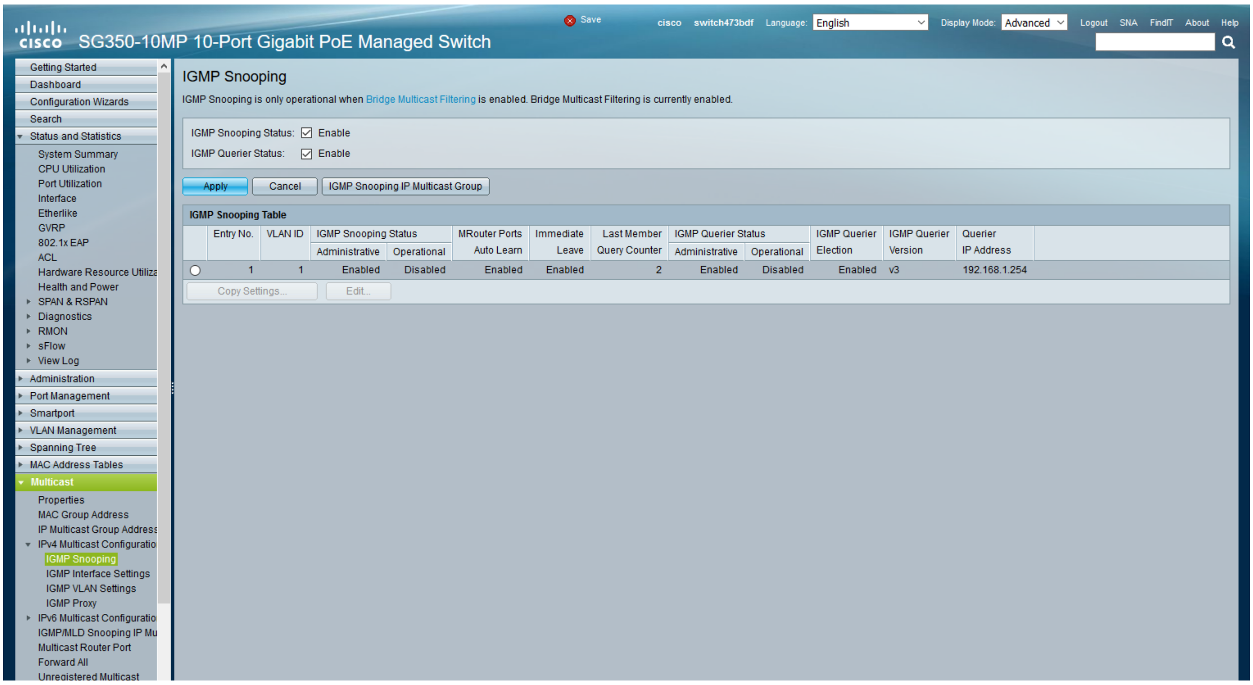
© 2011-2019 Cisco Systems, Inc. All Rights Reserved.

Figure 8: MAC Group Address.

4.3. IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol(IGMP) network traffic to control delivery of IP multicasts. Network switches with IGMP snooping listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast transmission. Multicasts may be filtered from the links which do not need them, conserving bandwidth on those links.

The CISCO SG350-10MP 10-Port Gigabit PoE Managed Switch also has the possibility to activate IGMP snooping in the IPv4 Multicast Configuration, see figure 9 below. This is a more generic function that is available on many managed switches from budget to high end.



IGMP Snooping

IGMP Snooping is only operational when Bridge Multicast Filtering is enabled. Bridge Multicast Filtering is currently enabled.

IGMP Snooping Status: ☑ Enable

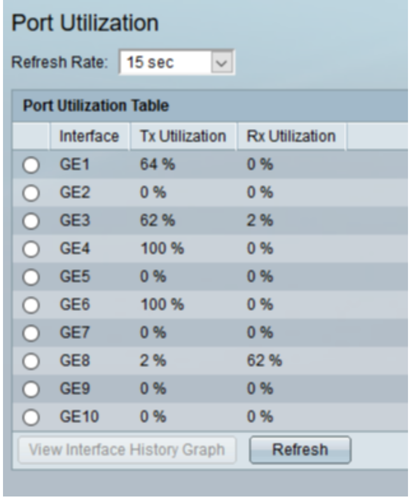
IGMP Querier Status: ☑ Enable

IGMP Snooping Table

	Entry No.	VLAN ID	IGMP Snooping Status		MRouter Ports Auto Learn	Immediate Leave	Last Member Query Counter	IGMP Querier Status		IGMP Querier Election	IGMP Querier Version	Querier IP Address
			Administrative	Operational				Administrative	Operational			
○	1	1	Enabled	Disabled	Enabled	Enabled	2	Enabled	Disabled	Enabled	v3	192.168.1.254

Figure 9: IGMP snooping.

When there is no multicast filtering initiated in the switch and IGMP snooping is not enabled we can see that the ports where the Plena matrix devices are connected to, port 4 and 6, reach a utilization of 100 % when there is multicast traffic in the switch with a bandwidth of approximately 300 Mbps, see figure 10 below. The connection with the Plena matrix devices is lost. It is not possible anymore to configure and control the Plena matrix devices via the PC GUI.



Port Utilization

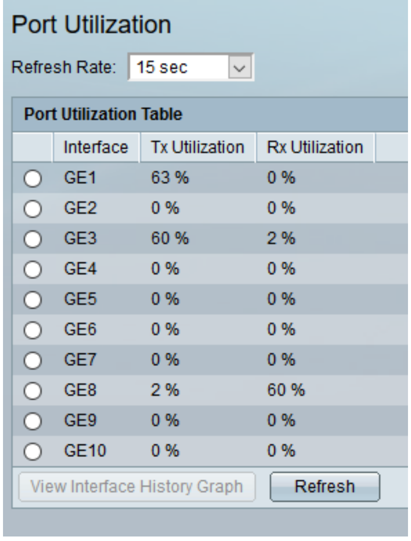
Refresh Rate: 15 sec

Port Utilization Table

	Interface	Tx Utilization	Rx Utilization
○	GE1	64 %	0 %
○	GE2	0 %	0 %
○	GE3	62 %	2 %
○	GE4	100 %	0 %
○	GE5	0 %	0 %
○	GE6	100 %	0 %
○	GE7	0 %	0 %
○	GE8	2 %	62 %
○	GE9	0 %	0 %
○	GE10	0 %	0 %

Figure 10: Port Utilization 100 %.

At the moment IGMP snooping is enabled the utilization of the ports where the Plena matrix devices are connected to, port 4 and 6, is reduced to 0 %, see figure 11 below. The connection with the Plena matrix devices is restored and configuration and control via the PC GUI is functioning again.



Port Utilization

Refresh Rate: 15 sec

Port Utilization Table

	Interface	Tx Utilization	Rx Utilization
○	GE1	63 %	0 %
○	GE2	0 %	0 %
○	GE3	60 %	2 %
○	GE4	0 %	0 %
○	GE5	0 %	0 %
○	GE6	0 %	0 %
○	GE7	0 %	0 %
○	GE8	2 %	60 %
○	GE9	0 %	0 %
○	GE10	0 %	0 %

Figure 11: Port Utilization 0 %.

Bosch Security Systems B.V.
Torenallee 49
NL – 5617 BA Eindhoven
www.boschsecurity.com