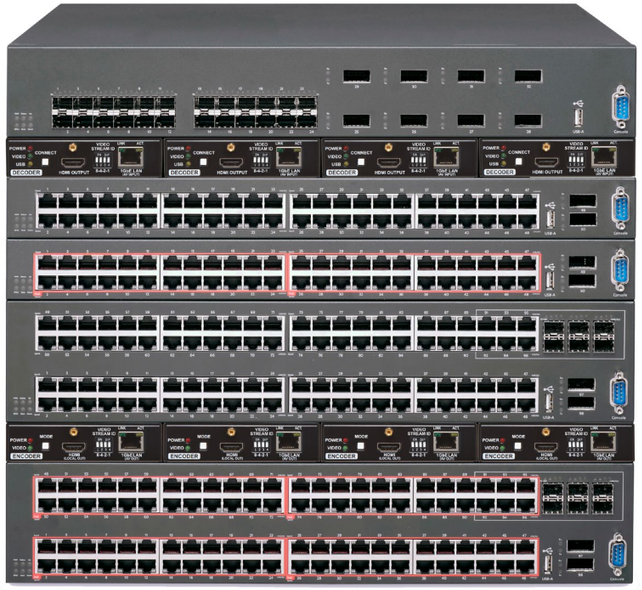
visual engineering
LIGHTWARE

VINX
VIDEO NETWORK EXTENDER

Application Notes



Installation and Network Setup Guide for VINX

Table of Contents

Document Information

Document revision: 2.5
Release date: 16-01-2023
Editor: Emil Balogh, Gabor Kocsis, Laszlo Zsedenyi

Contact Us

sales@lightware.com
+36 1 255 3800

support@lightware.com
+36 1 255 3810

Lightware Visual Engineering PLC.
Peterdy 15, Budapest H-1071, Hungary
www.lightware.com

1

Introduction

The first chapter is about the technical background of the functions and features that will be introduced in the following chapters. These are important to understand what is happening and why in a VINX network.

1.1. Network Properties

Network-based AV products use different network protocols for different operations. The network protocol can be UDP/IP and TCP/IP, the transmission mode can be Broadcast, Unicast, and Multicast.

These network protocols should be familiar to any network engineer. Because our network-based AV solutions bridge the gap between the audio-visual (AV) and information technology (IT) worlds, Lightware suggests involvement of both AV and IT departments in any installation.

Lightware products are designed to be plug-and-play. The figures in the next section illustrate the basic installation of one Decoder and one Encoder. A video source provides the digital video content for the Encoder which converts it to Ethernet packets and sends it to the attached Decoder. The Decoder reconstitutes the video with synchronized audio for presentation to the attached display.

Point-to-point vs Network Connection

VINX Encoders and Decoders have two typical applications:

- Point-to-point connection
- Point-to-multi point connection

Point-to-point Connection (Unicast mode)

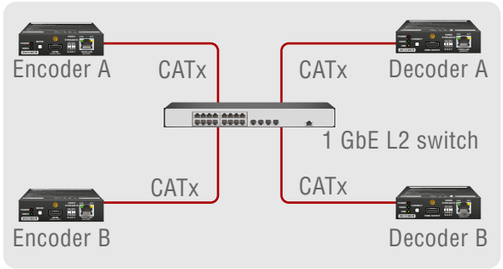
Unicast transmission mode uses a one-to-one association between the source and the destination: each destination address uniquely identifies a single Decoder endpoint.

Point-to-Multi Point Connection (Multicast mode)

Multicast transmission mode uses a one-to-one or one-to-many association; multicast datagrams are forwarded simultaneously in a single transmission to many recipients through an L2 swithed network. There can be multiple encoders in a L2 subnet. The decoders have to be in the same subnet.

Unicast Routing

The packet forwarding requirement of the VINX devices for point-to-point connection is the unicast switching. Please note that the unicast mode is not the default setting of the Encoder and Decoder, users have to set it in the devices.



Hardware Requirement:

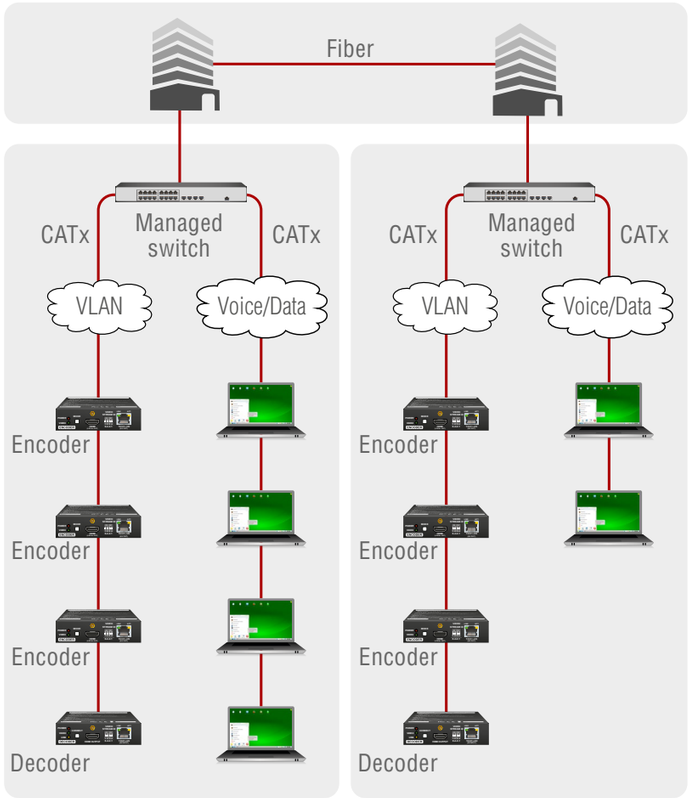
- 1 GbE Layer 2 (L2) switch

ATTENTION! VINX devices send certain system commands over multicast packages. If the multicast packet forwarding is disabled on the network, the signal transmission can fail.

Managed Switch for Multicast Routing

In TCP/IP terminology Layer 2 is the data link layer that is responsible for splitting the information coming from higher layers in the TCP/ IP stack into Ethernet frames. An Ethernet frame includes, among others, labeling information with source and destination physical addresses (called source and destination MAC address). These physical addresses uniquely identify the source and destination physical devices (e.g. a VINX Encoder and a VINX Decoder). Ethernet frames provide error resilience by incorporating a redundancy check field through which transmission errors can easily be detected. The device that uses only the physical address information found in the Ethernet frame to forward a packet from one of its input ports to one or more of its output ports is an unmanaged switch.

A managed switch, on the other hand, can handle the traffic and forward input packets to output packets by utilizing information from higher layers. This gives the managed switch more flexibility and also allows for more sophisticated functions, like multicast forwarding. Since even a simple VINX network, where one VINX Encoder supplies more VINX Decoders, relies on multicasting, a multicast capable switch (i.e. a managed one) is mandatory. If non-managed switches transmit the multicast packages, the multicast traffic is usually broadcasted over all interfaces.



Hardware Requirement:

- 1 GbE Layer 3 (L3) switch or managed L2 switch

Why is it important?

By default, Lightware Video-over-IP Encoders and Decoders use multicast packet forwarding. The switches in the network shall offer the following capabilities:

- IGMPv2
- IGMP snooping
- IGMP fast leave
- IGMP Querier
- Multicast filtering
- 9k MTU - Jumbo/Giant frames

Managed Switch Properties in Details

IGMPv2

IGMPv2 is version 2 of the Internet Group Management Protocol. This protocol is used by end-point devices to signal their interest in receiving a specific multicast content via subscribing to the multicast group corresponding to the content. Using IGMPv2 packets, the end-point devices can send a leave message to indicate that they are no longer interested in receiving the stream of the multicast group. Moreover, a multicast capable router can periodically poll the end-point devices on its interfaces which multicast streams they are interested to receive. The answer to such a query is called a membership report. IGMPv2 must be supported by the managed switch.

IGMP Snooping

IGMP snooping is a feature that allows the switch to monitor IGMP traffic when enabled. The information collected from the IGMP packets is used by the managed switch to determine which interfaces the multicast traffic should be forwarded to. In other words, IGMP snooping is used to converse bandwidth by allowing the switch to forward multicast traffic to those interfaces where it is really required.

IGMP Fast Leave

IGMP fast leave (or immediate leave), when configured, reduces the amount of time it takes for the managed switch to stop sending multicast traffic (corresponding to a multicast group defined by a multicast address) to an interface, where all end-point devices that used to be interested in a stream have sent an IGMP leave message. Without fast leave being enabled, the managed switch would first send out a query message and then would stop forwarding when no end-points answered within a pre-specified time interval. If fast leave is enabled, the switch stops forwarding the traffic without sending a query message.

IGMP Querier

In order for IGMP snooping to work properly, IGMP messages must traverse in the subnet between managed switches. However, if there is no multicast capable router present periodically sending out query messages and receiving answers to those queries, IGMP messages are usually not forwarded upstream from one switch to another. By enabling the IGMP querier feature in a managed switch, the managed switch will act like a router and periodically query the devices in the subnet (even other managed switches) to send their membership reports. From those reports all of the listening switches with IGMP snooping enabled will be able to determine where multicast traffic should be sent to.

Multicast Filtering

Some control information from VINX devices is transmitted via multicast packets. However, these packets are not registered during certain startup intervals, or not registered at all. In order for all VINX devices in the subnet to receive such control information, multicast filtering must be set up, so that unregistered groups are forwarded to all interfaces on the managed switch.

Jumbo/Giant Frames

Ethernet frames consist of a header and a payload. Since the header has a fixed length (20 or 26 bytes) the bigger the payload, the higher the useful bandwidth is. Similarly, the higher the useful bandwidth, the better the picture quality of the encoded video stream will be. To maximize picture quality, the Ethernet frame size (and consequently, the payload) should be as high as possible. In a normal Ethernet frame, the payload can be at most 1500 bytes. An Ethernet jumbo frame, however, can carry up to 9000 bytes of payload.

Since the goal of the transmission is to provide the best possible picture quality in all circumstances, the VINX Encoder device produces Ethernet jumbo frames. Thus, the handling of jumbo frames has to be enabled in the managed switches.

Trunk Port / Multicast Router / MRouter / Router Port / IGMP Querier Mode

Configures a static connection to a multicast router. Trunk port or Multicast router port (mrouter port or router port) is where the Multicast Router option is enabled.

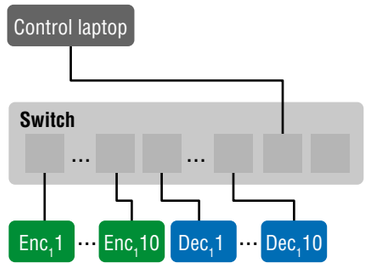
Two critical things occur when the switches know about a multicast router port:

- 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

1.2. Configuration Samples

Using One Switch (10x10)

Layout

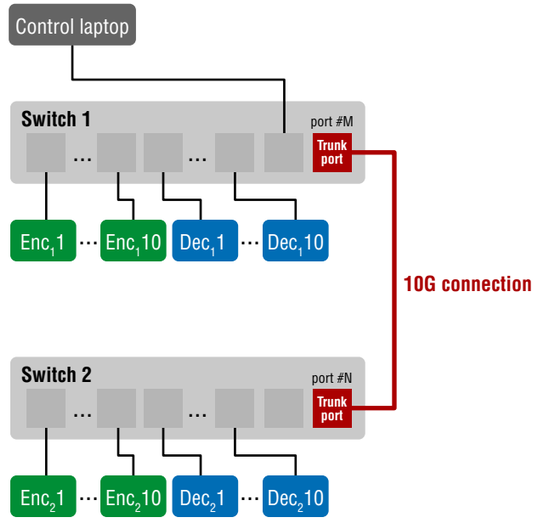


Settings

- **Enc$_n$1, Enc$_n$2, ..., Enc$_n$10:** the Encoders (10) connected to the switch.
- **Dec$_n$1, Dec$_n$2, ..., Dec$_n$10:** the Decoders (10) connected to the switch.
- **IGMP v2 Snooping:** Enabled.
- **Immediate Leave:** Enabled, on each port.
- **Querier:** Enabld.
- **IGMP Proxy:** Disabled.
- **Trunk Port:** Disabled.

Using Two Switches (20x20)

Layout

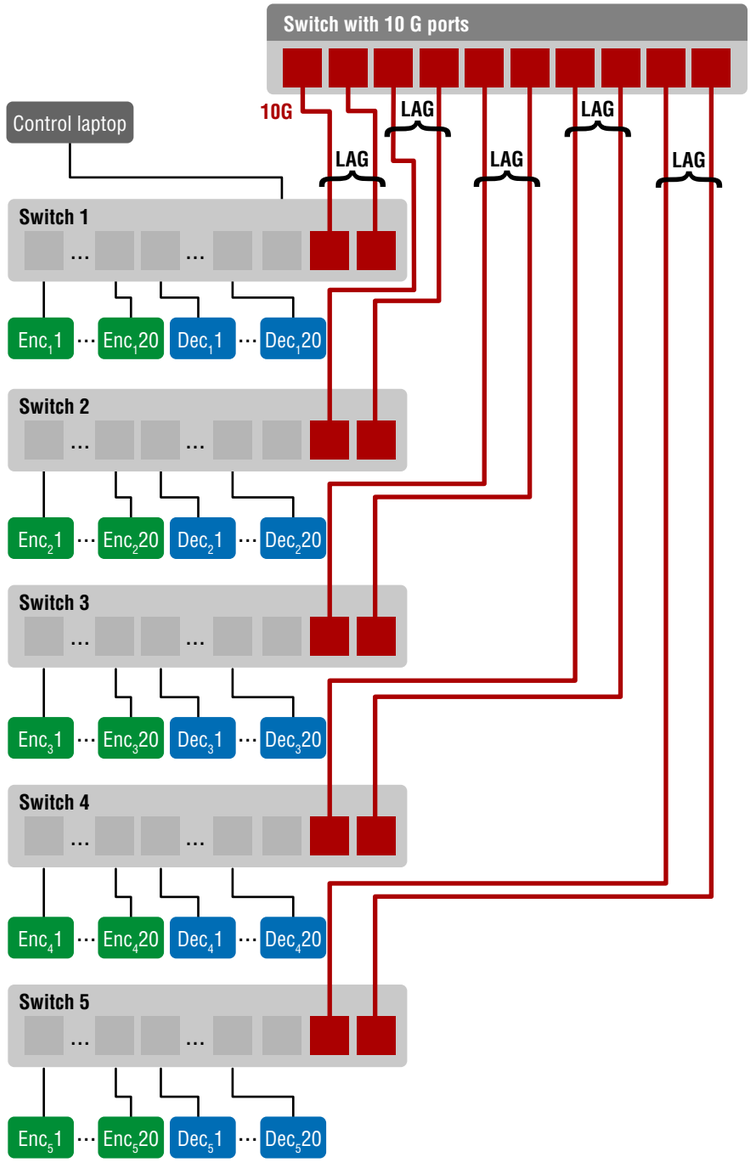


Settings

- **Enc$_m$1, Enc$_m$2, ..., Enc$_m$10 and Dec$_m$1, Dec$_m$2, ..., Dec$_m$10:** 10 encoders and 10 decoders connected switch 1.
- **Enc$_n$1, Enc$_n$2, ..., Enc$_n$10 and Dec$_n$1, Dec$_n$2, ..., Dec$_n$10 :** 10 encoders and 10 decoders connected switch 2.
- **port#M - port#N**: a point-to-point link between the two network devices. The bandwidth between them is the key parameter to determine how many encoder and decoder can work simultaneously. One Encoder requires 1Gbps network bandwidth, then 10 Encoders require 10Gbps bandwidth. Since an Ethernet switch nowadays runs full duplex mode, a 10Gbps port can provide 10Gbps upstream and 10Gbps downstream bandwidth.
- **IGMP v2 Snooping:** Enable.
- **Immediate Leave:** Enable, on each port except port #M and #N.
- **Querier:** Enable.
- **IGMP Proxy:** Disable.
- **Trunk port:** Must only enable on both end of trunk.

Using Multiple Switches (100x100)

Layout



Settings

- **Enc$_n$1, Enc$_n$2, ..., Enc$_n$20:** the Encoders connected to the switch #n.
- **Dec$_n$1, Dec$_n$2, ..., Dec$_n$20:** the Decoders connected to the switch #n.

Settings of the 10G switch

- **IGMP v2 Snooping:** Enable.
- **Immediate Leave:** Disable.
- **Querier:** Enable.
- **IGMP Proxy:** Disable.
- **Trunk port:** Disable.
- **Link Aggregation (LAG):** set for each port pairs.

Settings of the 1G switch

- **IGMP v2 Snooping:** Enable.
- **Immediate Leave:** Enable on each port except Trunk port.
- **Querier:** Enable.
- **IGMP Proxy:** Disable.
- **Trunk port:** Enable only on the port connect to 10G switch.
- **Link Aggregation (LAG):** set for each port pairs.

2

Configuration Steps - Ubiquiti EdgeSwitch 48 Lite

The following chapter is about the configuration of an Ubiquiti switch. The steps described here help to have a properly configured switch for a VINX network.

2.1. First Steps

2.1.1. Configuration Methods

You can arrange the settings in the following ways:

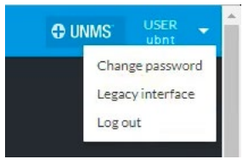
- **Uploading a configuration file** to the switch with the necessary settings in a browser window,
- Configuration over GUI: setting the **parameters in a browser**, or
- Change the parameters one-by-one by **sending commands** by a simple Terminal software (e.g. Putty).

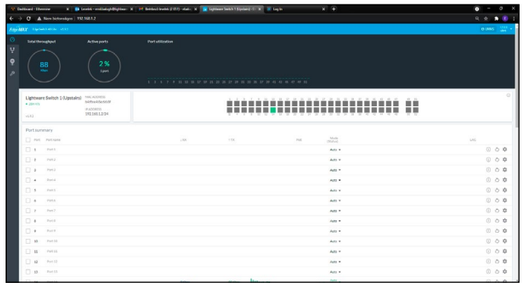
2.1.2. Accessing the Switch

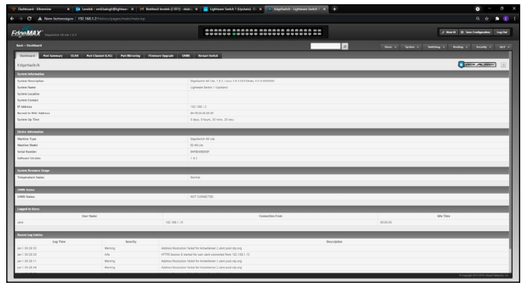
Factory default settings:

- **IP address** (if there is no DHCP server): 192.168.1.2
- **User name**: ubnt
- **Password**: ubnt

After a successful login you have the option to arrange the settings via the **New** or the **Legacy interface**. It can be selected from the **upper right menu**. Usually we use the legacy interface.







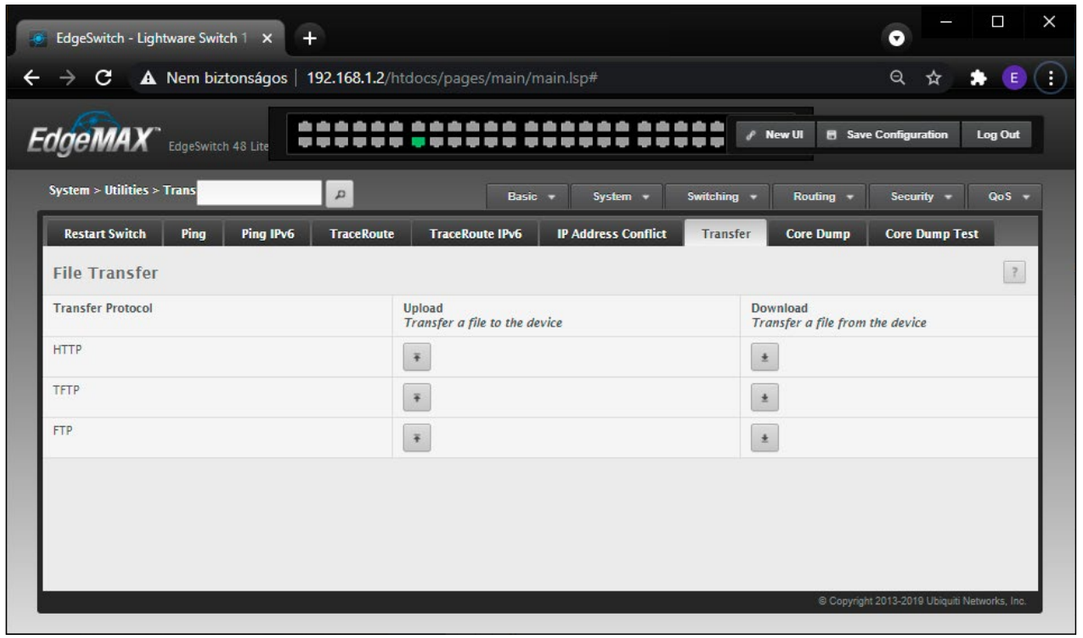
The New Interface / The Legacy Interface (preferred)

2.2. Uploading a Configuration File

If you have a config file containing the necessary settings, the easiest way is to upload it via the browser window. A configuration file with the necessary settings is available by the following link:

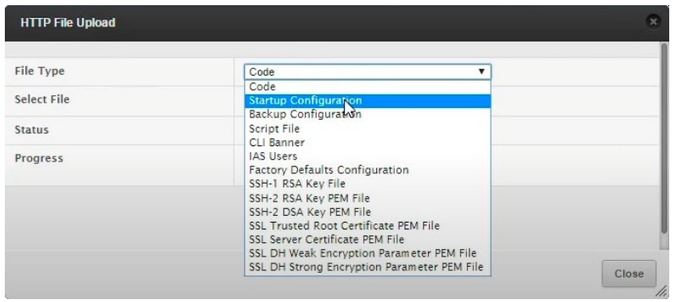
https://lightware.com/catalogsearch/result/?q=Vinx+Configuration+for+Ubiquiti+ES-EdgeSwitch-EdgeMax

Navigate to the **System/Utilities/Transfer** menu; press the desired button to upload a system configuration over HTTP, TFTP or FTP.



File Transfer page

ATTENTION! If you upload the **Startup configuration**, do not press save, just restart the switch without saving.

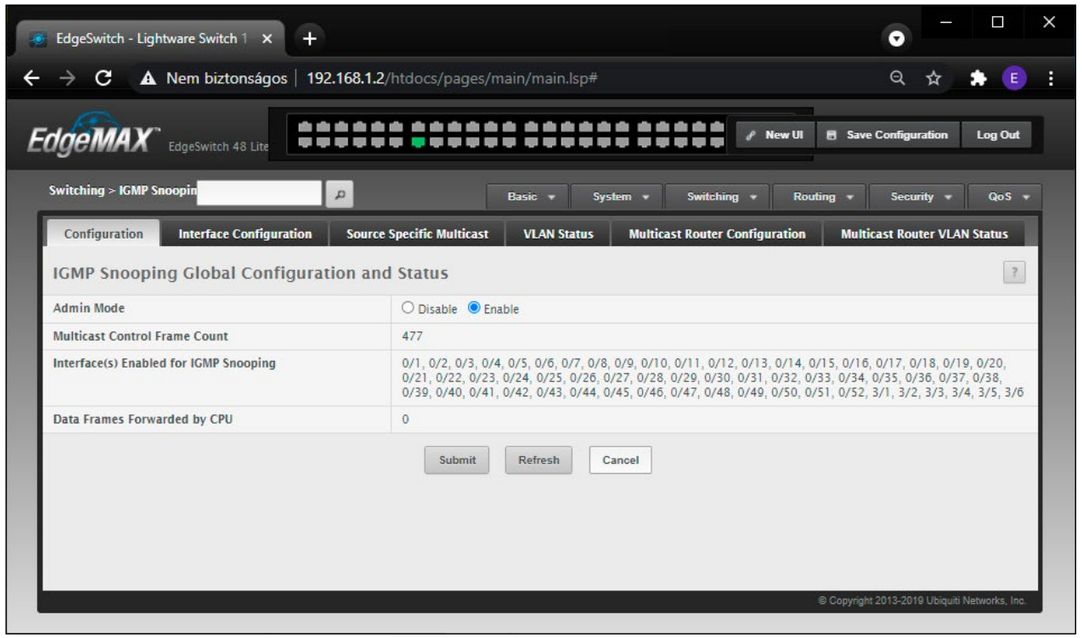


2.3. Configuration over GUI

Connect to the switch as described in the Accessing the Switch section.

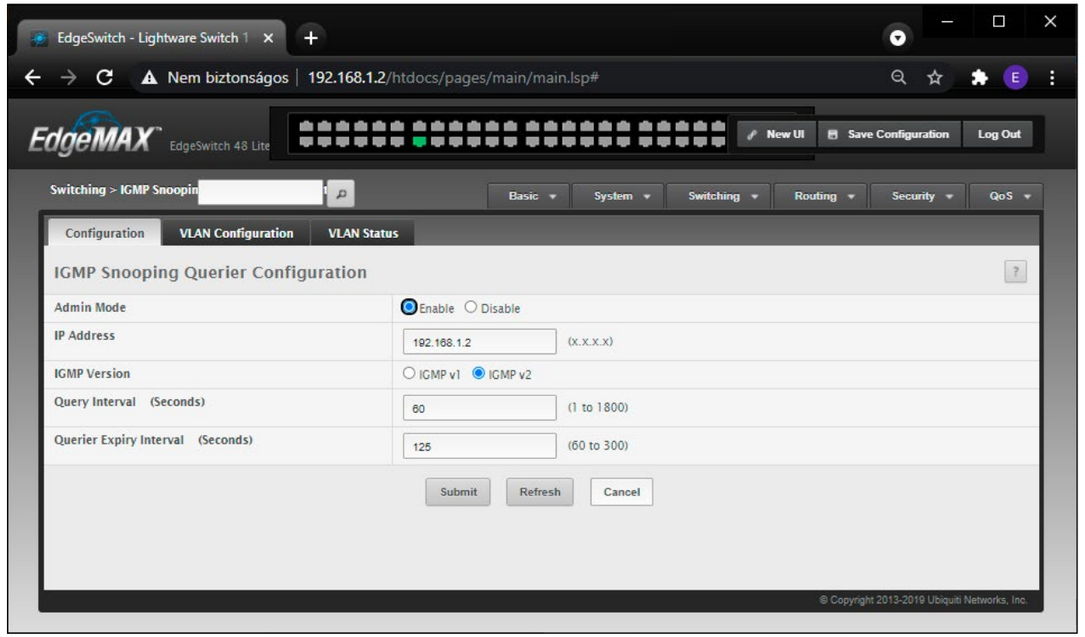
Step 1: IGMP Snooping Global Configuration

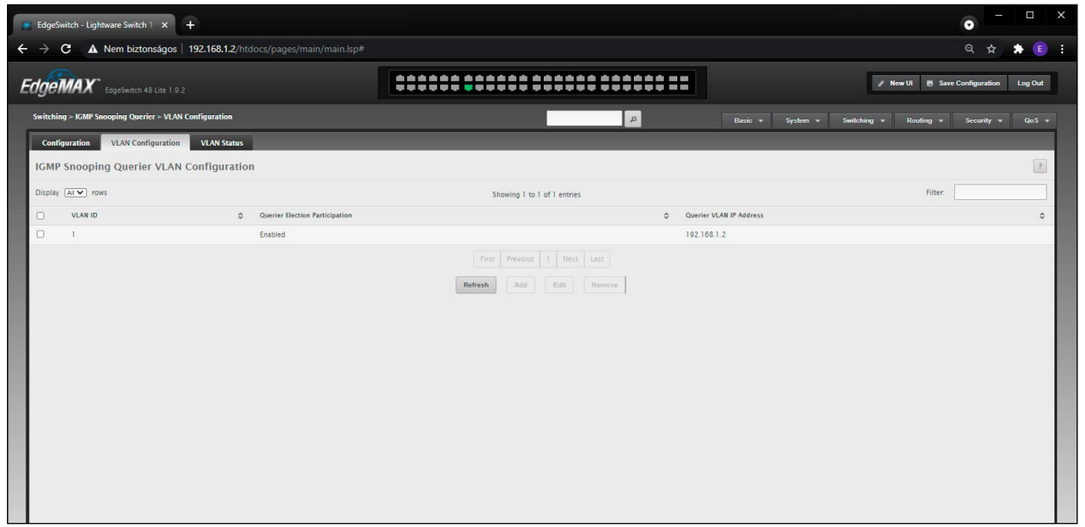
You have to enable IGMP Snooping globally; select the **Switching / Snooping** submenu and set as seen below:



Step 2: IGMP Querier Configuration

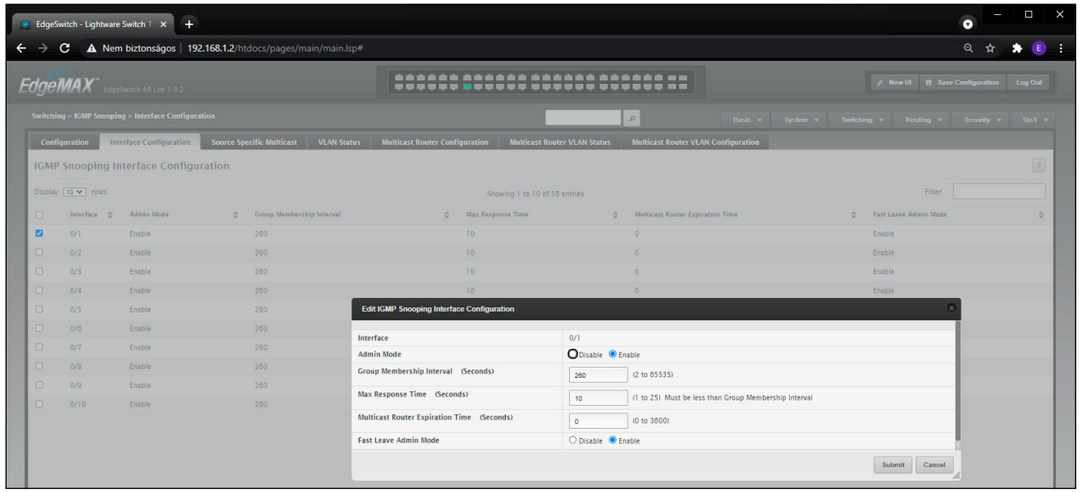
Set the IGMP Snooping Querier option to **Enabled** in the Switching / IGMP Snooping submenu.





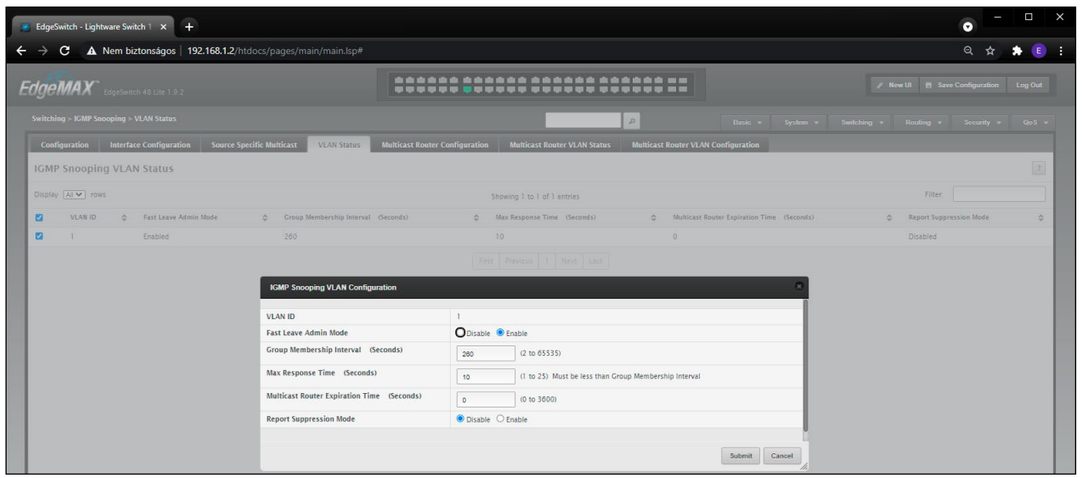
Step 3: Fast Leave Configuration

Select the **Switching/IGMP Snooping/Interface Configuration** menu. Select the interfaces (ports) where VINX devices are connected; the settings can be done in one window and applied to all.



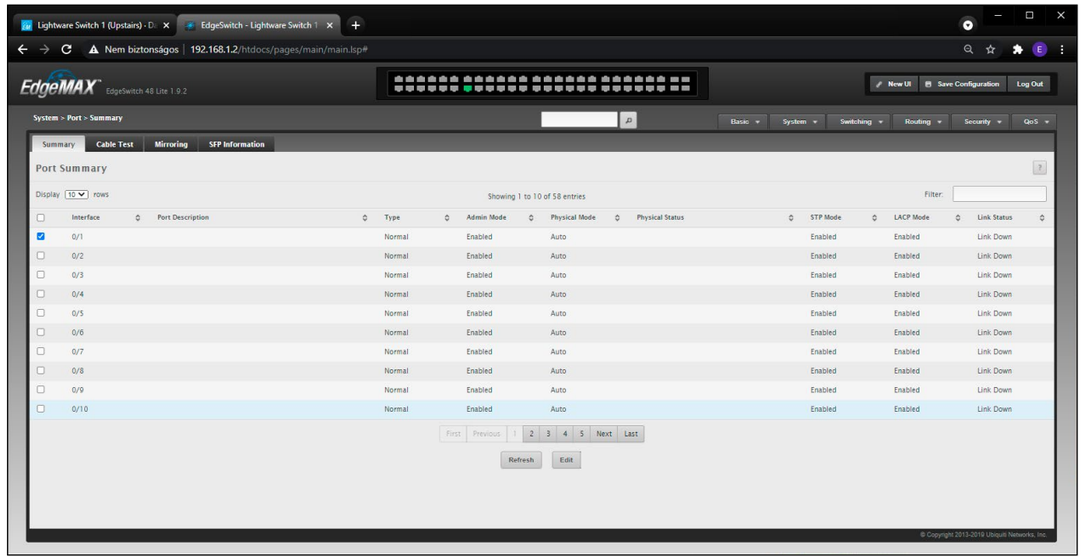
Step 4: IGMP Snooping VLAN Configuration

Select the **Switching/IGMP Snooping/VLAN Status** menu.

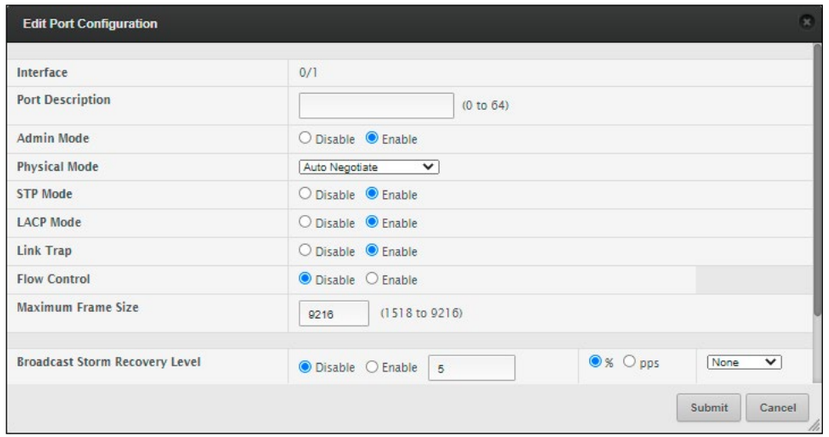


Step 5: Jumbo Frame Setting

Navigate to the **System /Port / Summary** submenu.



When this window is opened, you can not see Jumbo Frame options. Select a port and press the **Edit** button. Set the **Maximum Frame Size** parameter to 9216; thus, jumbo frame will be revealed:



2.4. Configuration Commands

This section is about the commands of the configuration file, which can be downloaded from the following:

https://lightware.com/catalogsearch/result/?q=Vinx+Configuration+for+Ubiquiti+ES-EdgeSwitch-EdgeMax

ATTENTION! The lines starting with an exclamation mark (!) are comments, which will not be processed.

Naming the switch

```
hostname "Lightware Switch 1 (Upstairs)"
```

The host name of the switch is defined between quotations marks for easier identifying.

```
network protocol none
```

Thus, the DHCP client is switched off, IP address will not be received from the DHCP server.

IP address settings

```
network parms 192.168.1.2 255.255.255.0 192.168.1.1
```

Structure: <switch IP address> <subnet mask> <gateway IP address> (divided by spaces).

Setting the querier in vlan 1

```
vlan database
set igmp querier 1 address 192.168.1.2
set igmp 1
set igmp fast-leave 1
set igmp querier 1
set igmp querier election participate 1
exit
ip http session hard-timeout 168
ip http session soft-timeout 60
ip http secure-session hard-timeout 168
ip http secure-session soft-timeout 60
configure
no device analytics
line console
exit
line telnet
exit
line ssh
exit
snmp-server sysname "Lightware Switch 1 (Upstairs)"
```

IGMP settings and Jumbo Frame global settings

```
set igmp
no set igmp header-validation
set igmp querier
set igmp querier address 192.168.1.2
```

Setting **IGMP querier** and IP address.

IGMP and Jumbo Frame also have to be set on ports, port settings

```
interface 0/1
set igmp
set igmp fast-leave
mtu 9216
lldp transmit-tlv port-desc
lldp transmit-tlv sys-name
lldp transmit-tlv sys-desc
lldp transmit-tlv sys-cap
lldp transmit-mgmt
lldp notification
exit
```

The commands above must be sent to all interfaces from 0/1 to 0/52, with only the first line being different. These commands set the **Fast leave** and **Jumbo frame** settings. The lldp (LLDP) commands are in connection with the Link Layer Discovery Protocol, which is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet.

Interface lag commands

```
interface lag 1
set igmp
set igmp fast-leave
mtu 9216
exit
```

The **IGMP** and **Fast leave** setting commands must sent to: interface lag 1 to lag 6.

3

Configuration Steps - Netgear M4300 series

The following chapter is about the configuration of a Netgear switch. The steps described here help to have a properly configured switch for a VINX network.

3.1. Preparation

3.1.1. Factory Reset

If the device has to be put into factory default state, press the hidden button on the left front side:

- When pressed for **2 sec** or more, but less than 5 sec, the button will initiate a **soft reset** of the switch.
- When pressed for **5 sec or more**, it will trigger a **factory reset** operation by restoring the switch to its factory default settings.

Out Of Band (OOB) Port Setting

If the device is in factory default state, DHCP mode is active. If no DHCP server is present, the IP address will be **192.168.0.239**.

3.1.2. Login

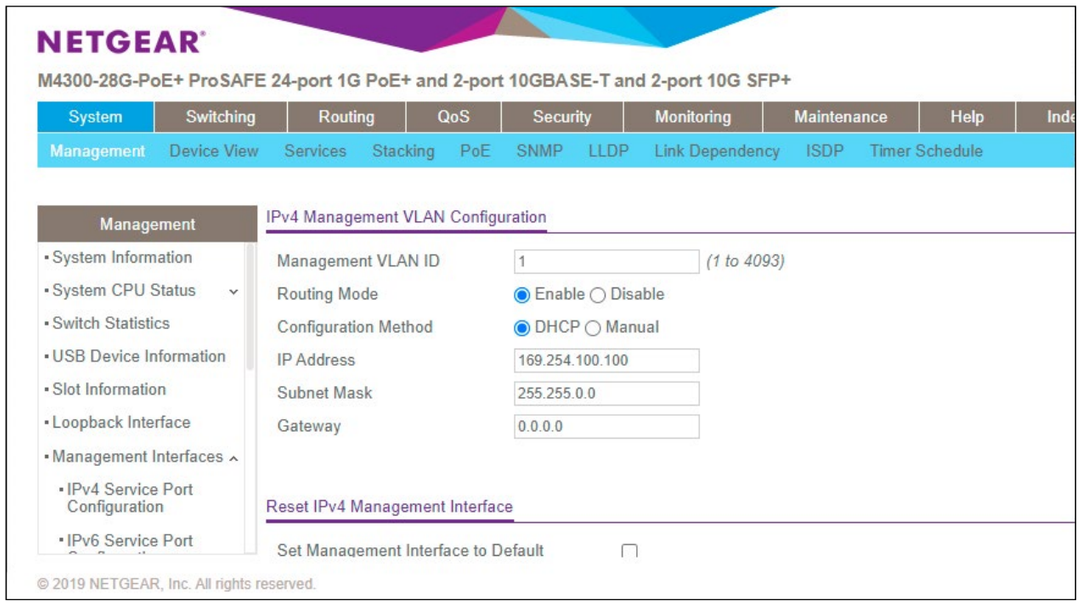
The device management is available over a browser via the OOB port or any Ethernet port.

Factory default IP address: 192.168.0.239

Login name: admin

Password: blank (leave it empty). After login you will have to change the password (min. 8 characters long).

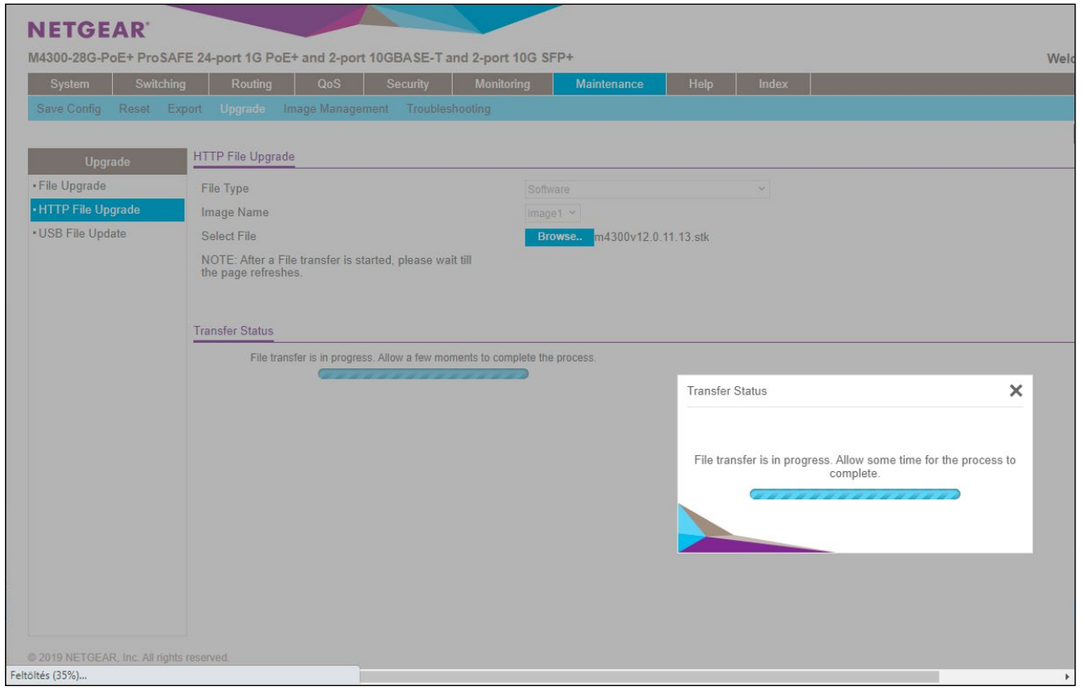
This is where you can set the ip address of the switch – we changed the IP address to **192.168.0.100**:



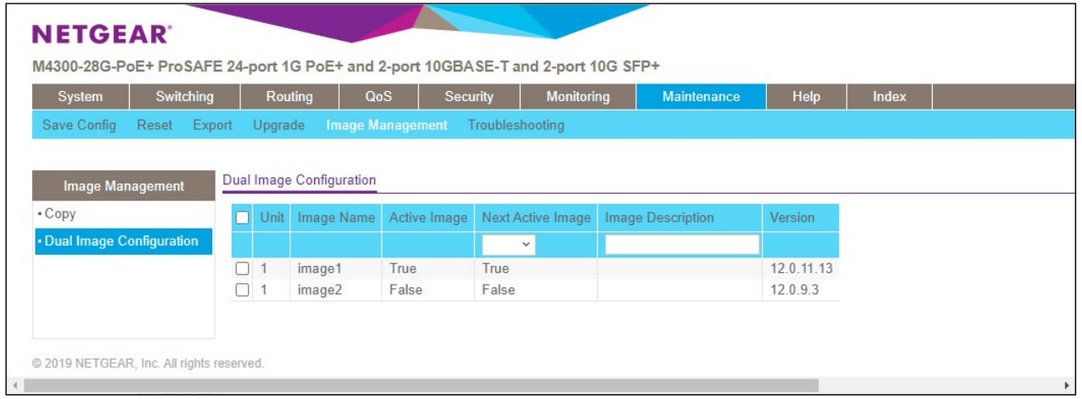
Save the changes by clicking in the upper right corner.

3.1.3. Firmware

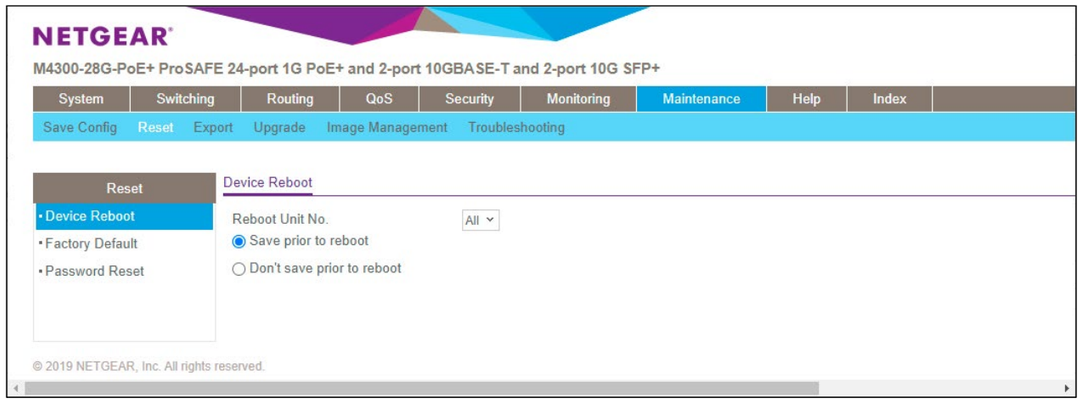
First of all, please check the **firmware** of the device; if it is **12.0.11.8** or newer, you do not have to perfrom an upgrade. The mentioned version contains the "SET IGMP plus" command that is necessary for setting a proper VINX network and if the firmware is older, please perform the upgrade. It can be done by TFTP, SFTP, HTTP or USB.



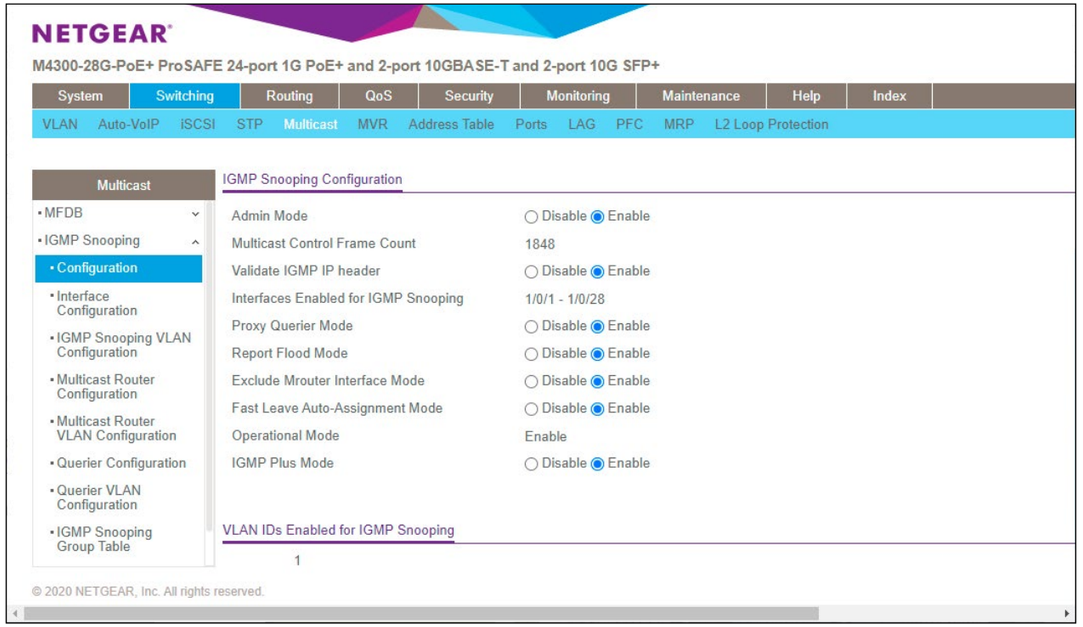
You can see the new image in the switch:



Select the image with version **12.0.11.13**, then **reboot** and **restart**:



IGMP Plus Mode is enabled by default in the new firmware:

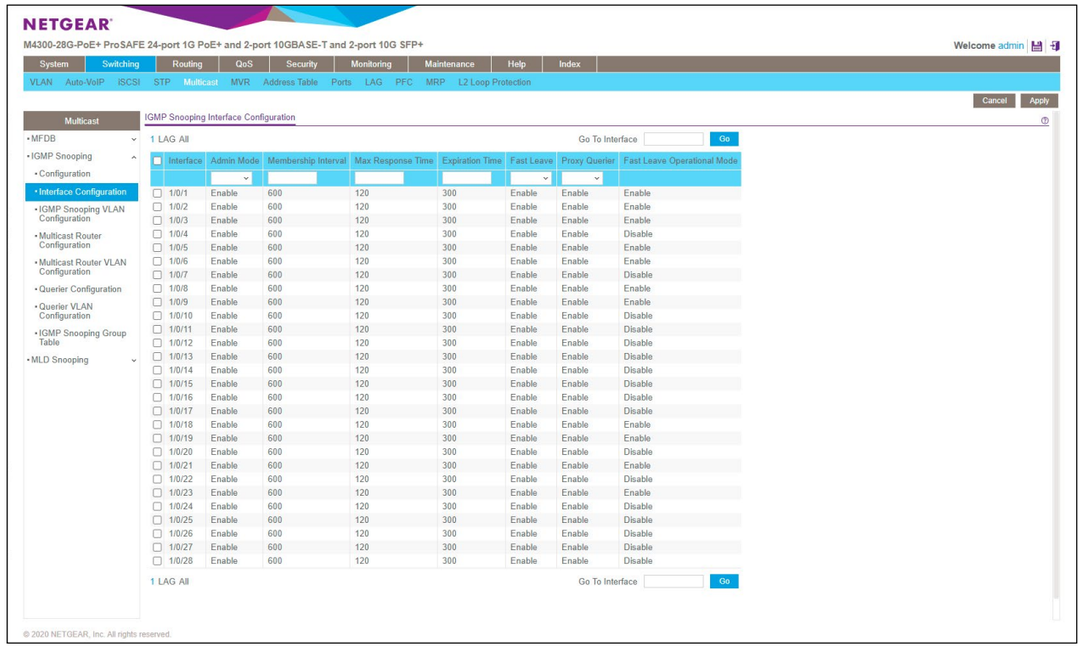


3.2. Settings for a VINX Network

Multicast

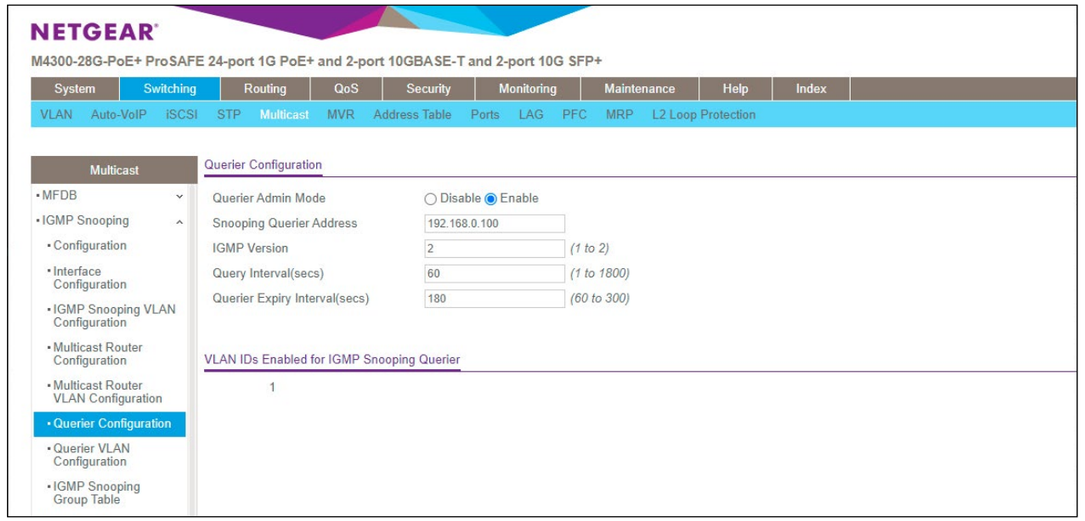
With default settings the VINX network will work:

- **IGMP plus** mode: enable (default)
- **Fast Leave**-t: disable ➔ enable it
- **IGMP snooping Administrativ mode**: disabled ➔ enable it on all ports

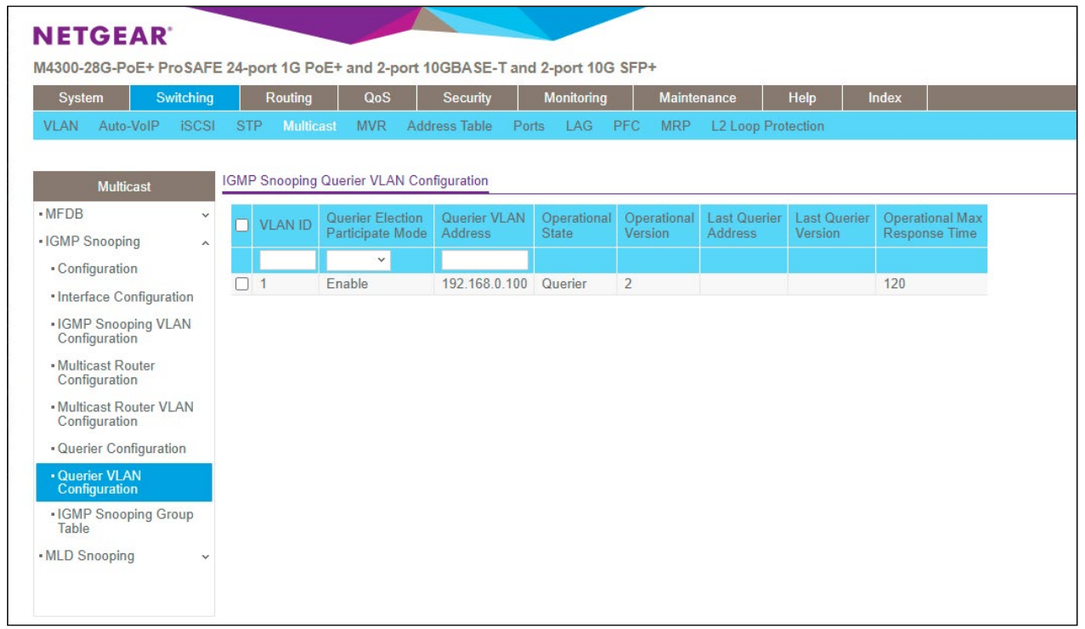


Querier

You have to set Querier, check **IGMP version 2**.

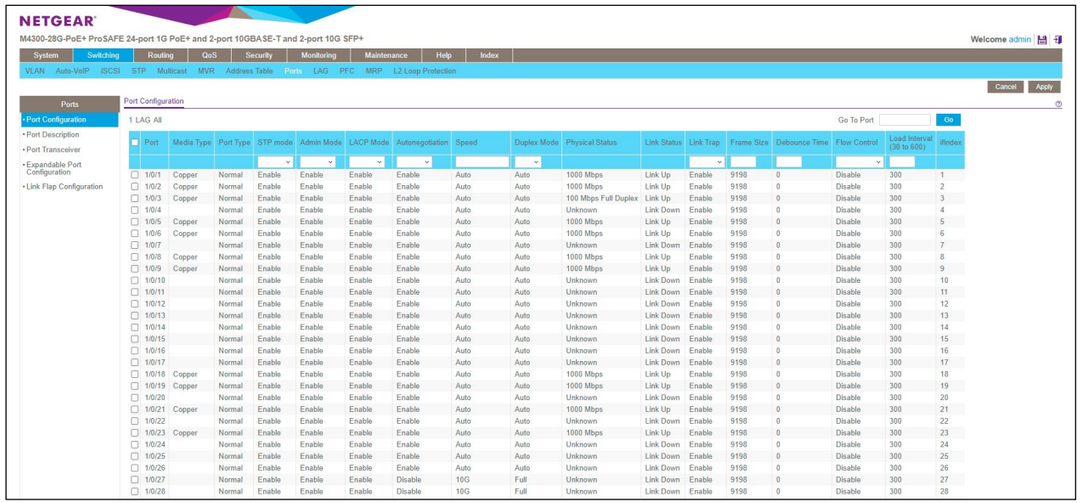


Also here:



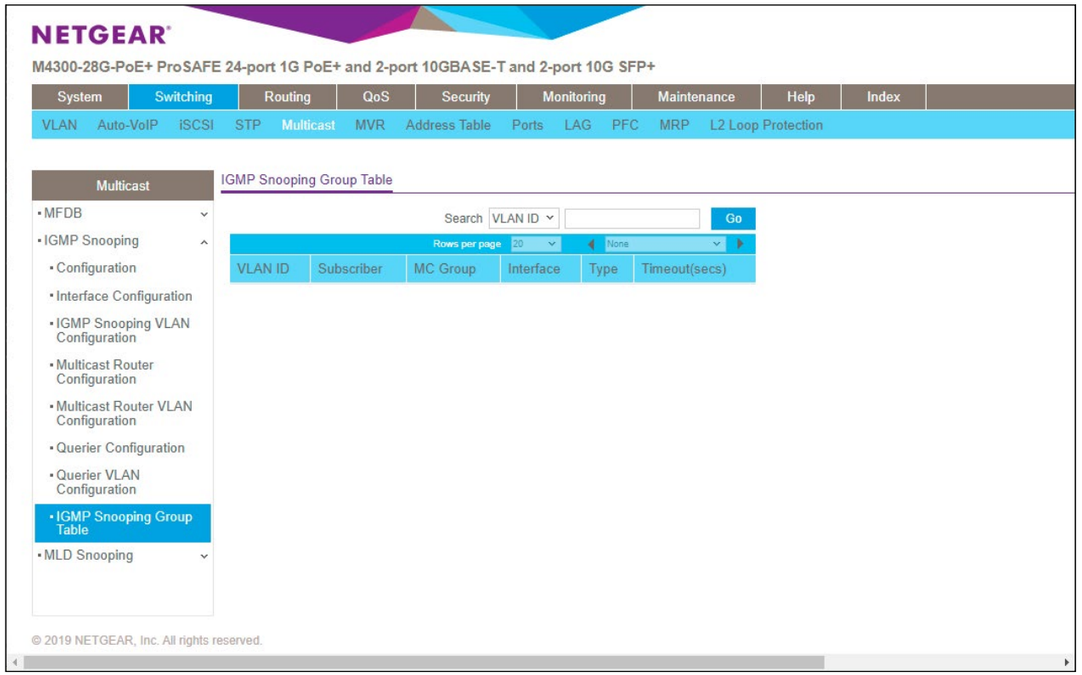
Jumbo (Giant) Frame

Jumbo frame, Giant frame is set by default to 9198, which is ok.



IGMP Snooping Group Table

If VINX devices are not attached, this table is empty:



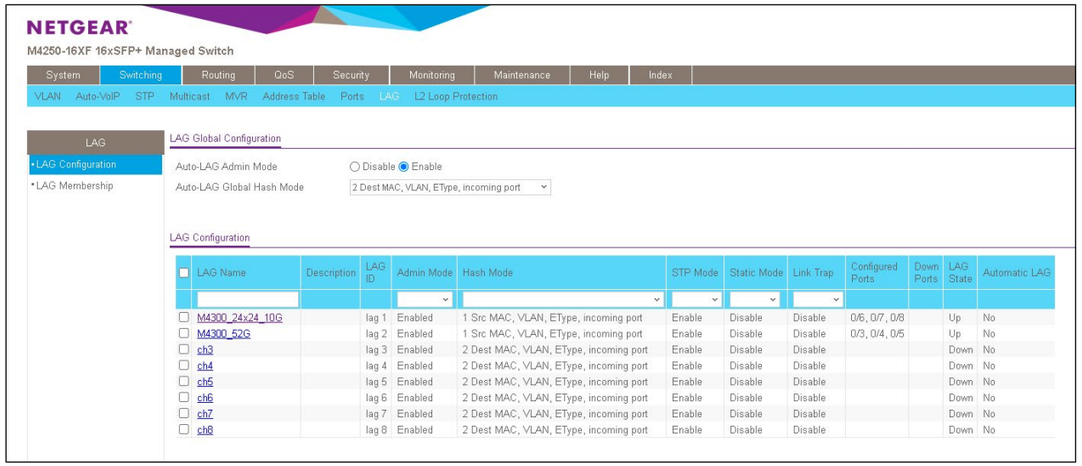
Link Aggregation (LAG)

> DEFINITION: The Link Aggregation Group (LAG) applies to various methods of combining (aggregating) multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain.

This setting is necessary if you have more network switches in the system and the bandwidth has to be gained between them. A test system has been built for this purpose in Lightware's Test Lab with 63 encoders, 55 decoders and 7 network switches. Please see the details in the Multi-switch_AV_Network_for_VINX document.

Creating LAGs

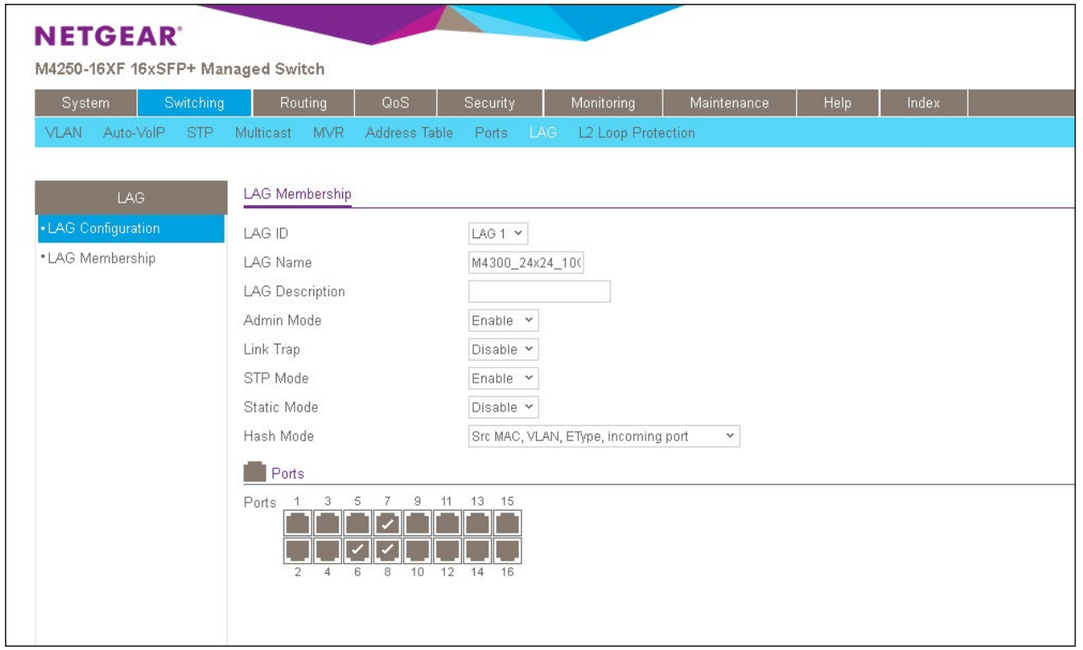
Navigate to the Switching -> LAG -> **LAG Configuration** submenu. All ports and the current LAG states are listed here.



Click on **ch1** (or the defined LAG name) to enter the LAG Membership settings page.

Select the desired ports (which will be be connected to the other switch) in the graphic port table. Press **Apply** when a LAG has been configured.

Please pay attention to the **Hash Mode**: set **the same mode** in both network switches on the affected ports.



4

Configuration Steps - HP Aruba 2930F

The following chapter is about the configuration of an HP Aruba switch. The steps described here help to have a properly configured switch for a VINX network.

4.1. Preparation

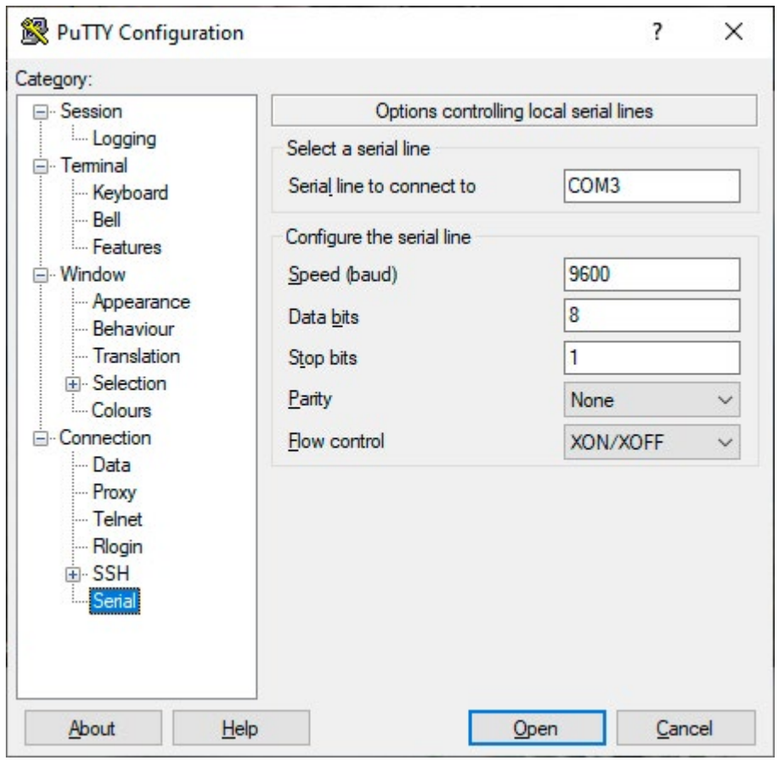
This switch does not have a Graphical User Interface (GUI). Everything has to be **done via Command Line Interface (CLI)**.

Initial Serial Connection:

Port settings are as follows: 9600 baud, data bit 8, stop 1, parity none.

Putty Configuration

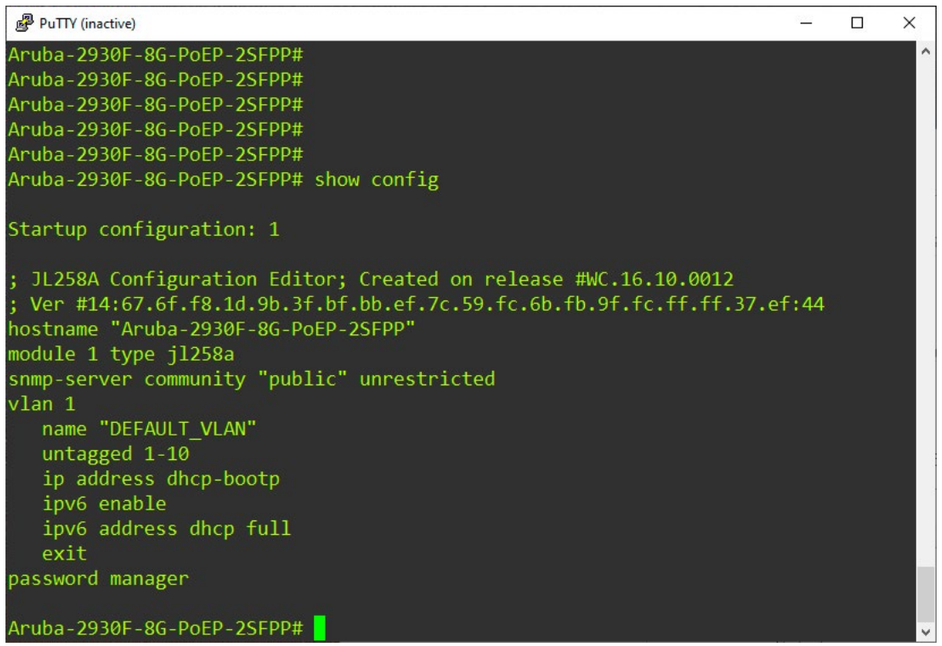
The commands will be sent from a terminal software, e.g. PUTTY. (https://www.putty.org/).



4.2. Configuration Steps

Initial Configuration

```
Startup configuration: 1
; JL258A Configuration Editor; Created on release #WC.16.10.0012
; Ver #14:67.6f.f8.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:44
hostname "Aruba-2930F-8G-PoEP-2SFPP"
module 1 type jl258a
snmp-server community "public" unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-10
   ip address dhcp-bootp
   ipv6 enable
   ipv6 address dhcp full
   exit
password manager
```



Login Credentials

User: admin

Password: admin

Entering Configuration Mode

```
1st : login
2nd: enable
3rd: configure
```

After this propt will look like this:

```
Aruba-2930F-8G-PoEP-2SFPP(config)#
```

In this mode you may enter the commands below.

Configuration Commands

`ip igmp`	- turning on igmp funtions
`ip igmp fastleave all`	- turning fast leave on (on all ports)
`jumbo`	- turning on jumbo (large) frames
`untag all`	- all traffic should be untagged
`exit`	- exit

Configuration Commands Explanation

```
ip igmp
ip igmp fastleave all
jumbo
ip address 192.168.0.10 255.255.255.0
untagged all
exit
```

Saving the Configuration

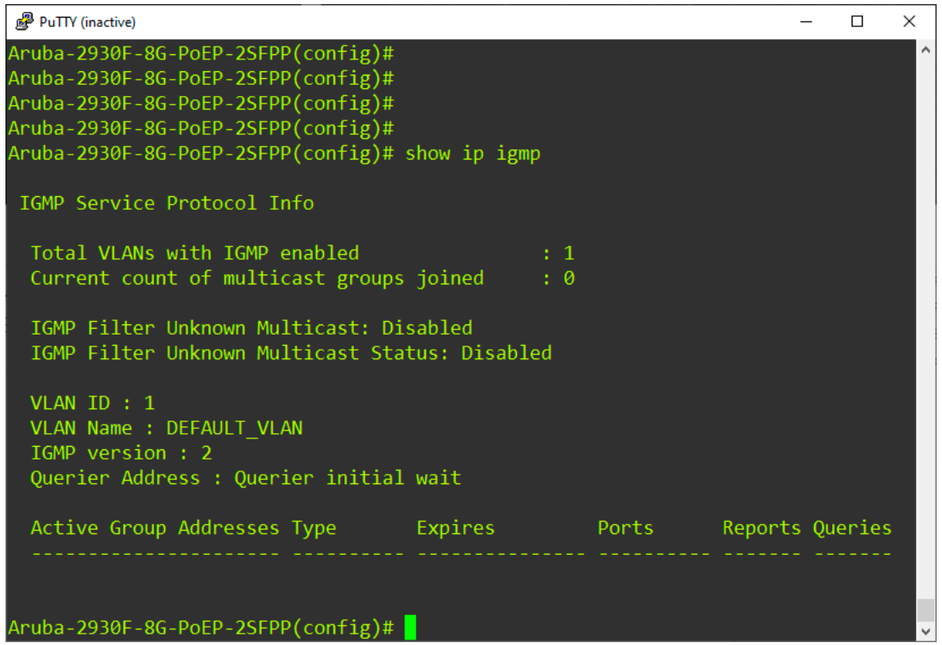
```
write memory
```

Checking the IGMP Status

```
show ip igmp
```

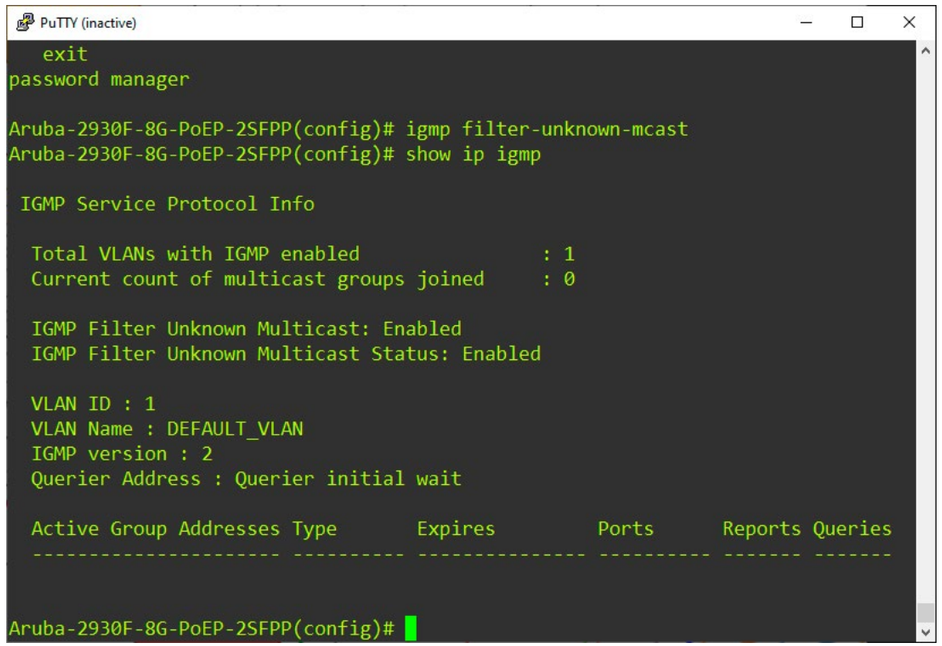
or

```
show ip igmp vlan 1
```



Filtering unknown multicast

```
igmp filter-unknown-mcast
show ip igmp
```



Factory Reset

1. Using pointed objects, simultaneously press both the Reset and Clear buttons on the front of the switch.
2. Continue to press the Clear button while releasing the Reset button.
3. When the Global Status LED begins to quickly flash in amber (after approximately 5 seconds), release the **Clear** button.The switch will then complete its boot.

5

Network Analysis

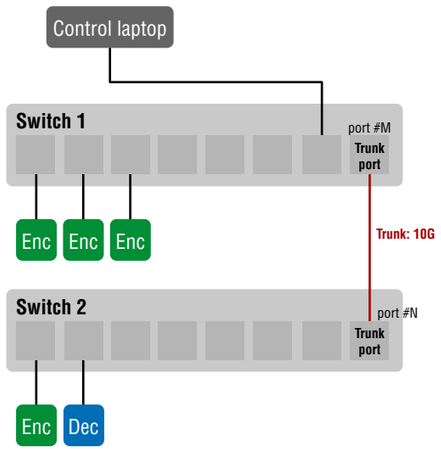
This chapter is about Troubleshooting if you encounter problems with a VINX network. Simple tools can be used to get and analyse the network data and find the root cause of bandwidth-management problems.

5.1. The Benefits

The VINX network analysis helps you to verify whether network switch parameters are correct, and visually inspect the results of potentially incorrect parameters. The method's benefits are demonstrated in the example below.

Participants

- 5 VINX devices in a **stacked switch** setup:
  - 3 Encoders on the top switch,
  - 1 Decoder and 1 Encoder on the bottom switch.
- A **control laptop** (workstation) with:
  - Lightware Device Controller (LDC) software,
  - Wireshark Network Analyzer,
  - Mirosoft Excel.
- One port of the top switch is set to **port mirroring**:
  - The source of the mirroring function is the trunk port of the top switch.



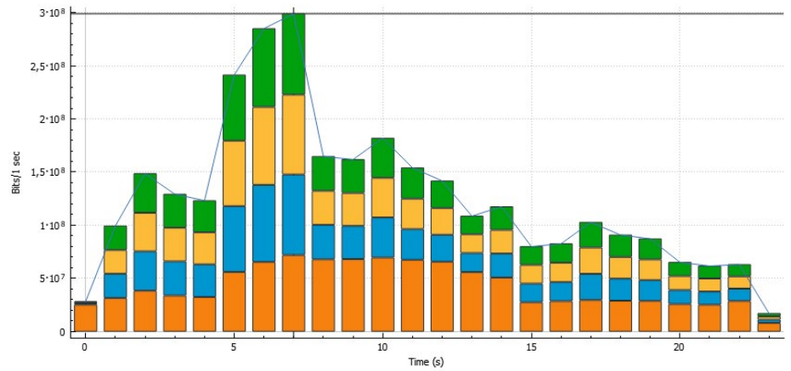
With this setup we can see that instead of IGMP Querying, which is an important feature for stacked switch setups, **IGMP Routing function sends all the traffic across the trunk port.** This is a problem, because in this setup only one encoder's traffic from the top switch should go through the trunk line. But the IGMP routing function sends every VINX encoder's traffic across the trunk line, which can **overload the maximum capacity** of the trunk line.

5.1.1. Wireshark Report

During the Wireshark capture, we notice a significantly higher data traffic than expected. In the captured packet list, we can see that multiple Multicast Group traffic is being sent through the port. We can see four Multicast Group traffic flows (see the Destinations): 225.2.0.4, 225.2.0.7, 225.2.0.9 and 225.2.0.15. In a correct network setup with IGMP Query, only the 225.2.0.4 traffic should be in this flow.

No.	Time	Protocol	Length	Source	Destination	Src.Port	Dst.Port	Info
1	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
2	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
3	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
4	0	UDP	8128	192.168.1.113	225.2.0.4	60134	59200	60134 → 59200 Len=8086
5	0	UDP	8128	192.168.1.116	225.2.0.9	60048	59200	60048 → 59200 Len=8086
6	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
7	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
8	0	UDP	60	192.168.1.116	225.2.0.9	60048	59200	60048 → 59200 Len=18
9	0	UDP	960	192.168.1.116	225.2.0.9	60048	59200	60048 → 59200 Len=918
…	0	UDP	60	192.168.1.114	225.2.0.7	60066	59200	60066 → 59200 Len=18
…	0	UDP	60	192.168.1.113	225.2.0.4	60134	59200	60134 → 59200 Len=18
…	0	UDP	60	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=18
…	0	UDP	960	192.168.1.113	225.2.0.4	60134	59200	60134 → 59200 Len=918
…	0	UDP	960	192.168.1.114	225.2.0.7	60066	59200	60066 → 59200 Len=918
…	0	UDP	4928	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=4886
…	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
…	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086
…	0	UDP	8128	192.168.1.115	225.2.0.15	60170	59200	60170 → 59200 Len=8086

With the I/O Graph settings, we can see that 75% of the network traffic through the trunk port is unexpected. Using the methods described below to adjust the display filters, we can easily identify which data traffic uses significant network bandwidth on the trunk line. This unnecessary, high traffic can cause signal issues on Multicast Group traffic 225.2.0.4, because the trunk overload may result in packets being dropped or missing.



Click to select packet 22998 (7s = 2.991e+08).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets	udp		Line	Bits		None
☑	All Packets	ip.addr == 225.2.0.4		Stacked Bar	Bits		None
☑	All Packets	ip.addr == 225.2.0.7		Stacked Bar	Bits		None
☑	All Packets	ip.addr == 225.2.0.9		Stacked Bar	Bits		None
☑	All Packets	ip.addr == 225.2.0.15		Stacked Bar	Bits		None

5.1.2. Excel Pivot Analysis

Using the Pivot table Analysis, it is easy to recognize that besides the desired Multicast Group traffic 225.2.0.4, there are four other devices that send data through the trunk line. A screenshot of such a table is helpful for the support team to understand the possible issues when attached to the system drawing and flow chart.

Sum of Length			Time									
Source	Destination	Protocol	0	1	2	3	4	5	6	7	8	9
192.168.1.100	230.76.87.82	IGMPv2	60		60		60		60		60	
192.168.1.112	224.0.0.251	IGMPv2		60								
	225.1.0.0	IGMPv2							60			
		UDP	2062	2062	2062	2062	2062	2062	2062	2062	2062	2062
	225.2.0.4	IGMPv2	60		300						60	
		UDP	2392	2950	2702	2826	2640	2578	2578	2640	2764	2578
192.168.1.113	225.1.0.0	IGMPv2	60									
		UDP	2062	2062	2062	2062	2062	2062	2062	2062	2062	2062
	225.1.0.1	IGMPv2						60				
	225.2.0.4	IGMPv2								360		
		UDP	141700	2877362	4656698	3990582	3768832	7797182	9265688	9566080	4097464	3982270
192.168.1.114	224.0.0.251	IGMPv2								60		
	225.1.0.0	UDP	2062	2062	2062	2062	2062	2062	2062	1031	2062	2062
	225.1.0.1	IGMPv2			60							
	225.2.0.7	IGMPv2	360								240	120
		UDP	131464	2795080	4540168	3964296	3779272	7697864	9182664	9408712	4013320	3881416
192.168.1.115	224.0.0.251	IGMPv2										60
	225.1.0.0	UDP	2062	2062	2062	2062	2062	2062	2062	2062	2062	2062
	225.1.0.1	IGMPv2					60					
	225.2.0.15	IGMPv2						360				
		UDP	3081224	3863304	4728008	4153480	3979784	6935176	8109640	8929480	8421192	8447176
192.168.1.116	224.0.0.251	IGMPv2									60	
	225.1.0.0	UDP	2062	2062	1031	2062	2062	2062	2062	2062	2062	2062
	225.1.0.1	IGMPv2				60						
	225.2.0.9	IGMPv2	360								300	60
		UDP	139592	2858440	4633480	4024648	3843976	7747912	9074120	9474440	4050568	3903944

In this simplified example table, we can see a device with 0.0.0.0 IP address (marked red), sending IGMPv2 protocol messages to Multicast Group 224.0.0.1. This is a router device that should not be present in the system, as it causes Multicast Traffic management issues.

Sum of Length		Protocol	
Source	Destination	IGMPv2	UDP
0.0.0.0	224.0.0.1	60	
192.168.1.100	230.76.87.82	2040	
192.168.1.112	224.0.0.2	120	
	224.0.0.251	300	
	225.1.0.0	240	137123
	225.1.0.1	300	168625
	225.2.0.4	540	27404
192.168.1.113	224.0.0.2	120	
	224.0.0.251	240	
	225.1.0.0	300	136092
	225.1.0.1	300	
	225.2.0.4	2940	4643212
192.168.1.114	224.0.0.2	120	
	224.0.0.251	300	
	225.1.0.0	240	136092
	225.1.0.1	240	
	225.2.0.7	2880	
192.168.1.115	224.0.0.2	120	
	224.0.0.251	300	
	225.1.0.0	240	136092
	225.1.0.1	300	
	225.2.0.15	2880	
192.168.1.116	224.0.0.2	120	
	224.0.0.251	360	
	225.1.0.0	300	137123
	225.1.0.1	240	
	225.2.0.9	2880	

The four devices (marked light red) are still present, but this time none of those are sending significant traffic, because there is no video signal on those devices. This indicates that there are no issues in the system at the moment, however, this will not be a permanent condition. Any time when those devices receive a video signal, they will most likely impact the traffic and can potentially overload the trunk line and cause signal quality issues later.

5.2. Step by Step Instructions

The following description is about the monitoring and analysis of the network traffic among VINX devices. The mentioned tools and methods help to see potentially incorrect settings of a VINX network.

5.2.1. Preparations

You will need the following softwares:

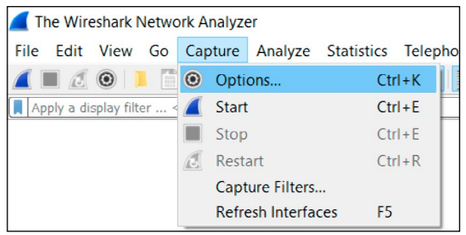
- Wireshark Network Analyzer (v3.4.1 is used in the examples) – download from here,
- Microsoft Office Excel (MS Office 365 is used in the examples).

Install the softwares above on a PC/laptop and make sure you are connected to the same network as the VINX devices.

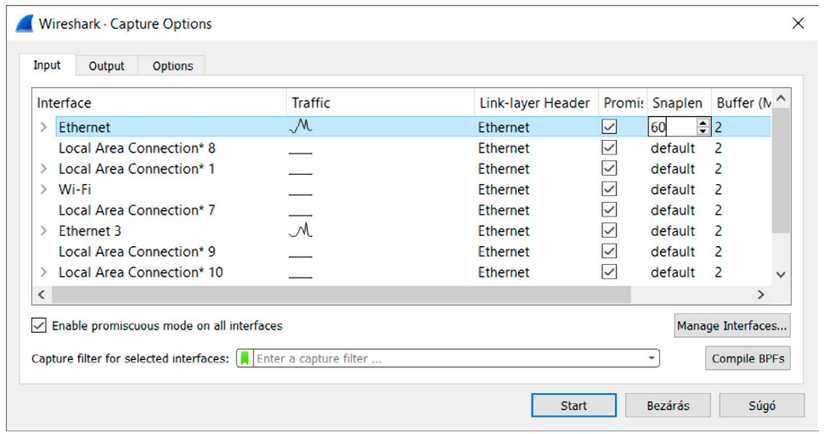
5.2.2. Data Collection

Step 1 – Interface Settings

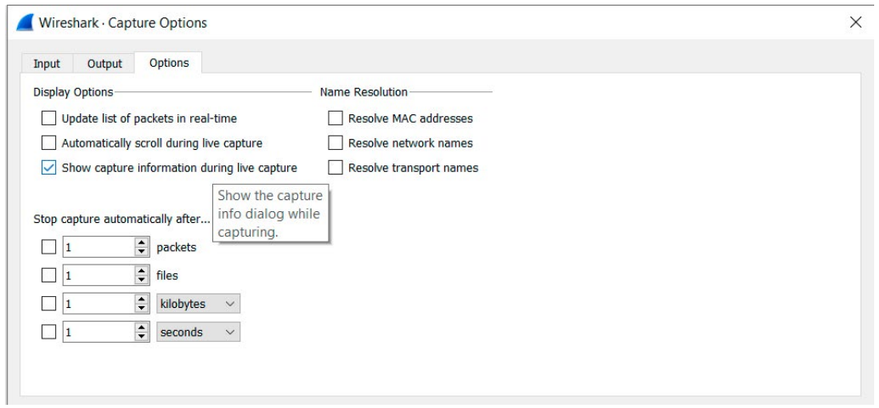
Start Wireshark and go to **Capture > Options** submenu and select the **Input** tab.



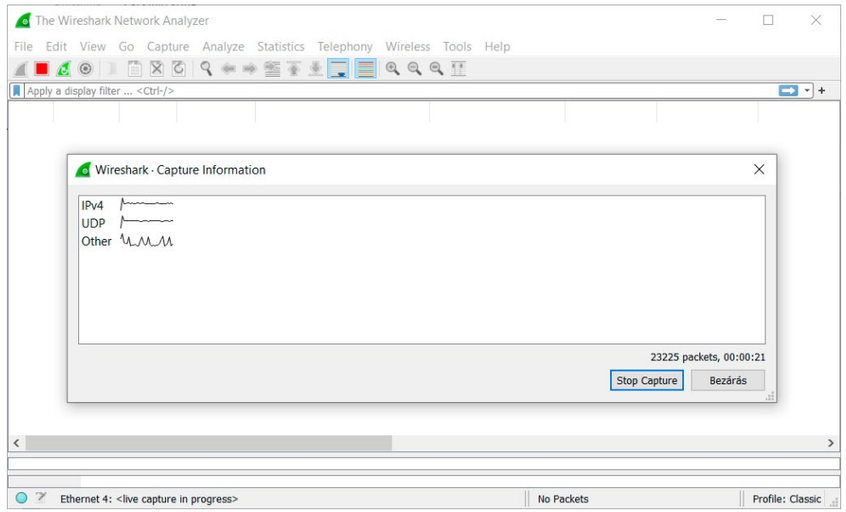
To reduce the size of the capture file, it is preferred to reduce the maximum amount of data that the software would store for each captured packet. For optimal analysis we recommend to capture the IP header data, but not the content of the IP payload. Check and take note of the interface that shows communication. Select the interface and double click on the **Snaplen** value (standard value is "default"), set it to 60 (60 bytes).



Optional: On the **Options** tab you can enable display of the capture information on the screen in real time in a separate window. This can help if the real-time updating of packets slows down the computer's response when capturing very high traffic data (e.g. 1080p or higher resolution video stream). If the computer you use has a very slow response during capture, this is most likely because of the the screen refreshing. In this case, you can turn off the **Update list of packets in real-time** and the **Automatically scroll during live capture** options.



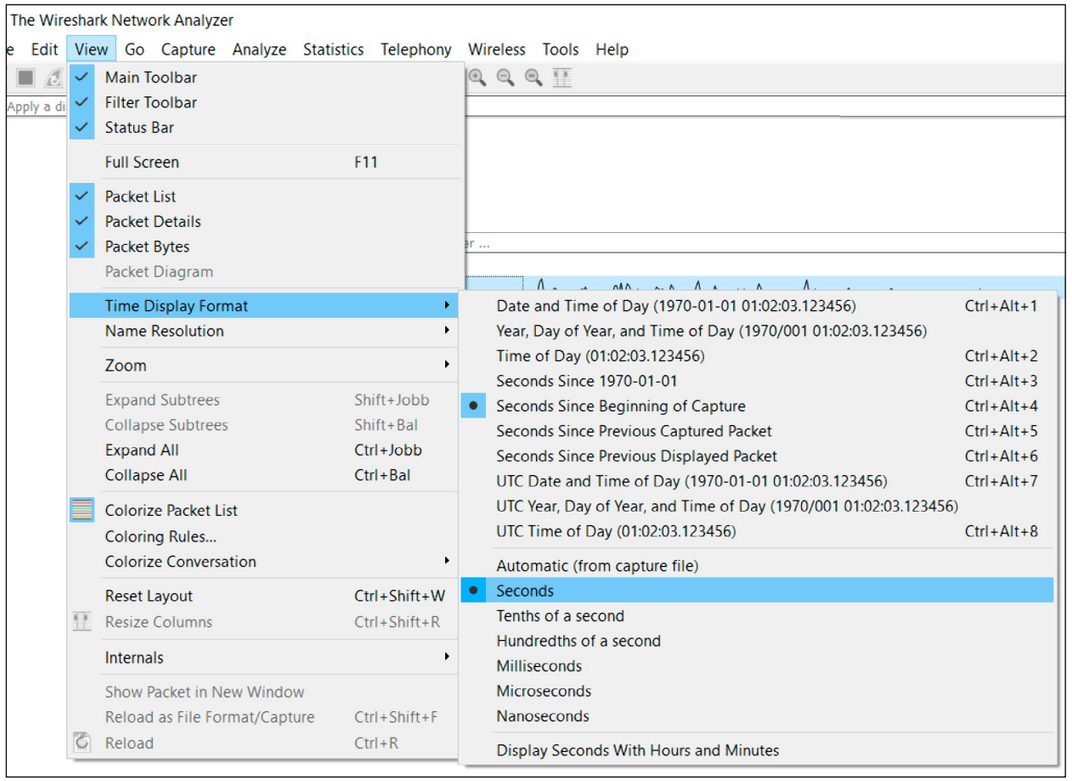
When the capture starts, the main screen will not show the captured traffic lines, instead the capture information window will show a simplified graph of the traffic details. This helps the computer's response to capture high traffic data.



INFO: When the real-time capture options mentioned above are disabled, you cannot use the I/O Graph function until the capture stops and the main window displays the captured data lines on the screen.

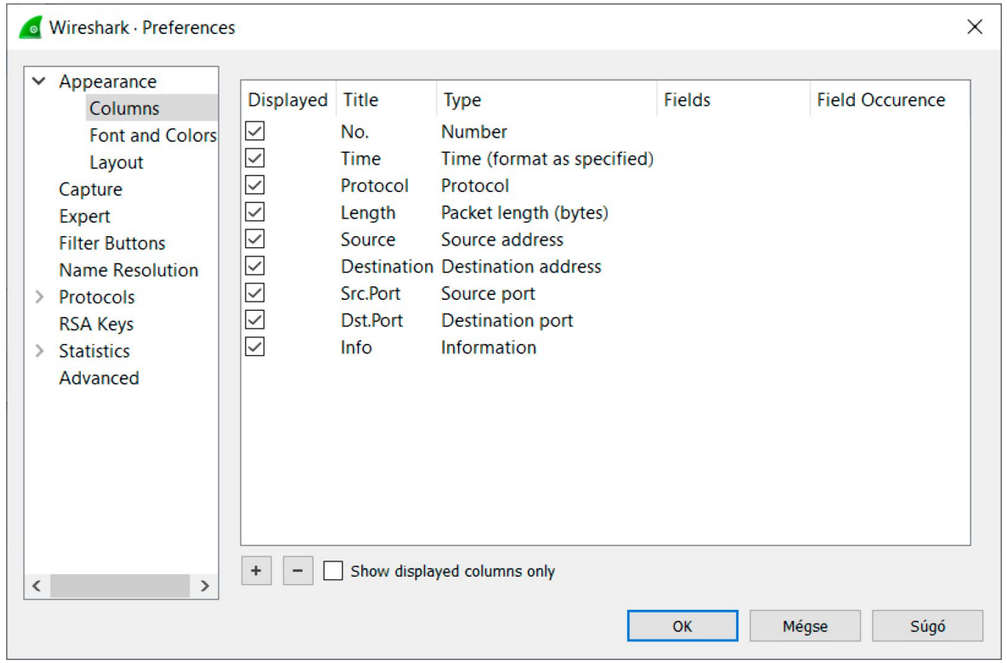
Step 2 – Time Display Settings

To change the capture screen's Time parameter, go to **View > Time Display Format**, and select the **Seconds Since Beginning of Capture** value and **Seconds** as unit. Seconds and Tenths of a second are preferred for Excel pivot, as Excel is currently limited to 16384 columns.

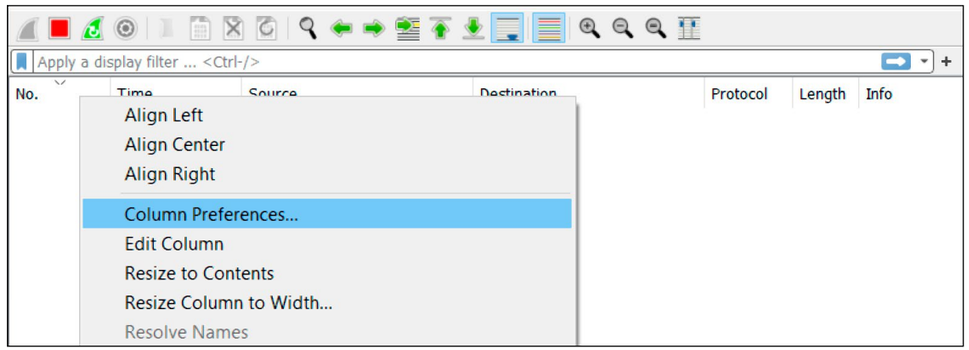


Step 3 – Column Settings

To change the columns shown (and later visible in Excel), go to **Edit> Preferences** and select **Appearance > Columns** option. You can add a column by clicking the **+** button in the lower left corner. To rename the column, double click on the **Title** cell, and edit the name (free text). To change the value of the column, double click on the **Type** cell, and select the preferred value. The preferred list of columns for AV over IP analysis are shown in the screenshot below:

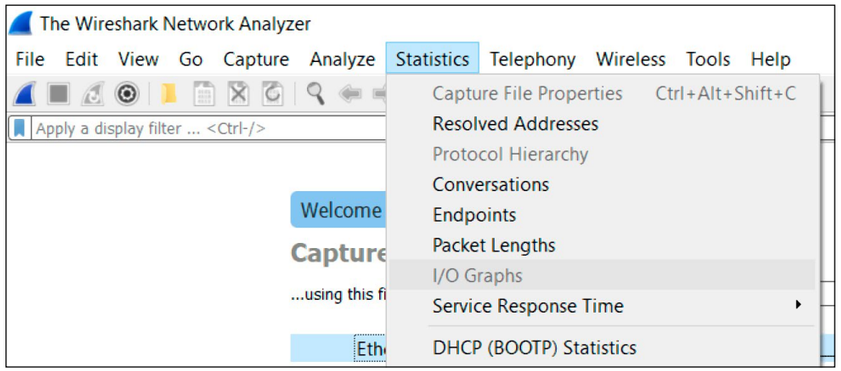


The same menu can be reached by right-clicking in the column title row cell in the capture window:

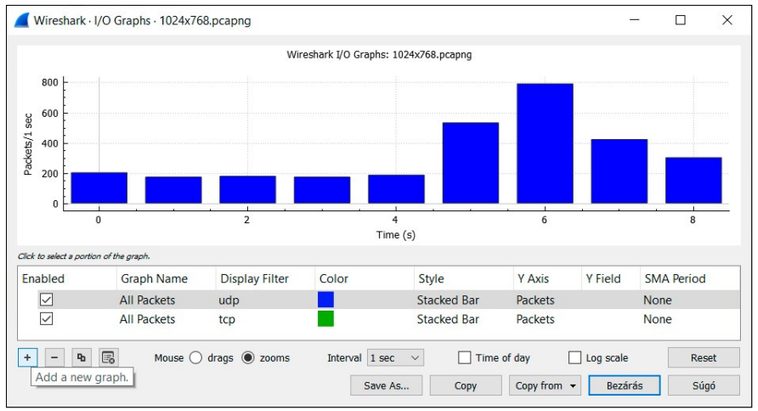


Step 4 – Graphical Settings

To configure the Graphical representation of the software during or after the capture process, go to **Statistics > I/O Graphs**.



At the I/O Graph screen select the Graph line you would like to change. E.g you can add a new Graph by clicking the + button:



Double click on the Display Filter cell to change the filter. When the cell's color is red, the entered filter is incorrect, when it is green, it is correct. When you start typing, the software will show the possible entries starting with the characters you enter.

Typically used filters: udp, tcp, icmp, igmp, arp

Filters also helpful for AV over IP products:

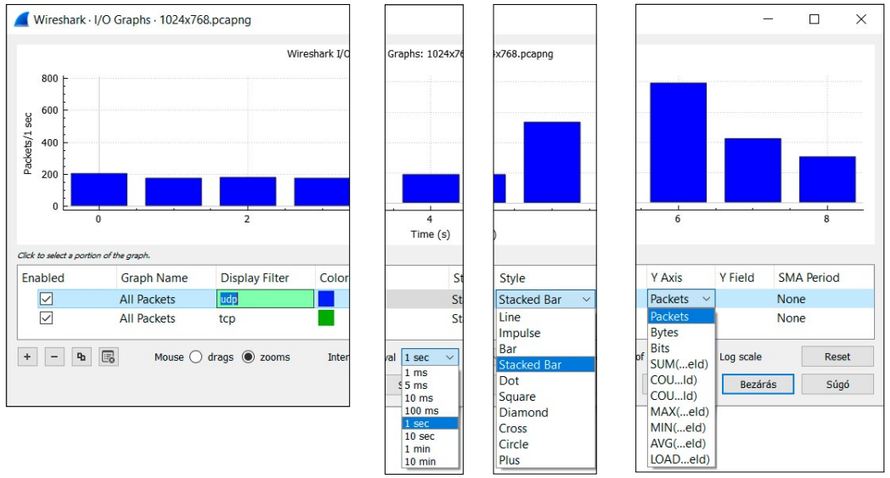
- **ip.addr==xxx.xxx.xxx.xxx** (e.g. a known multicast group address 225.2.0.1)
  - shows all packets sent to this group
- **ip.src==xxx.xxx.xxx.xxx** (e.g. a known VINX product IP address: 192.168.1.50)
  - shows all packets from this IP address

Double click on the **Color** tab to open the default windows color palette to select the preferred color of the graph.

Double click on the **Style** cell to change the graph style. Stacked Bar is preferred for such a graph.

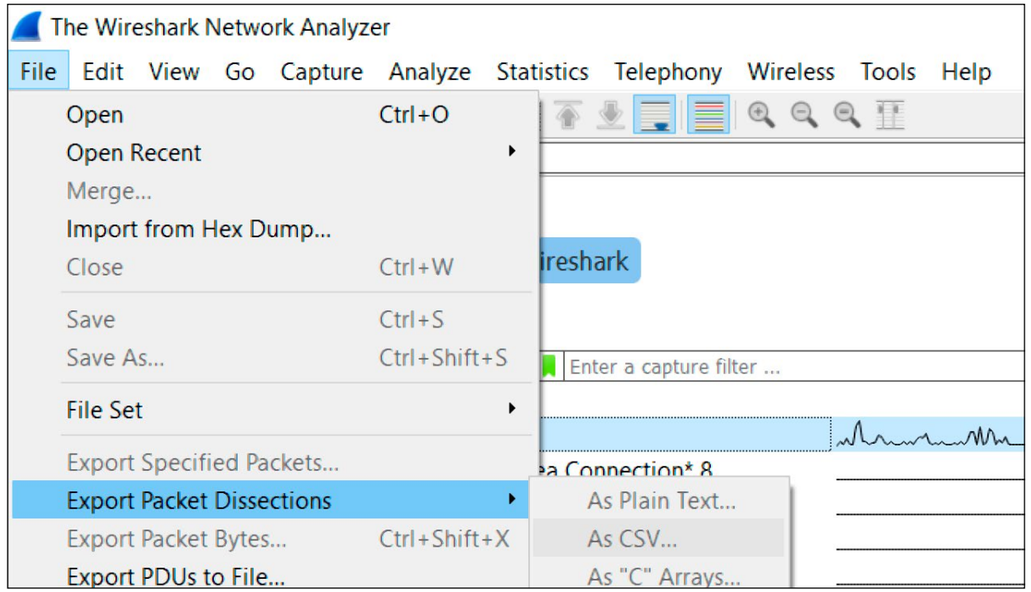
Double click on the **Y Axis** cell to change the data value shown. Preferred values for AV over IP are Bytes (total bytes captured) or Packets (number of packets captured).

It is possible to change the **X Axis** time interval by selecting the preferred value.



Step 5 – Data Export

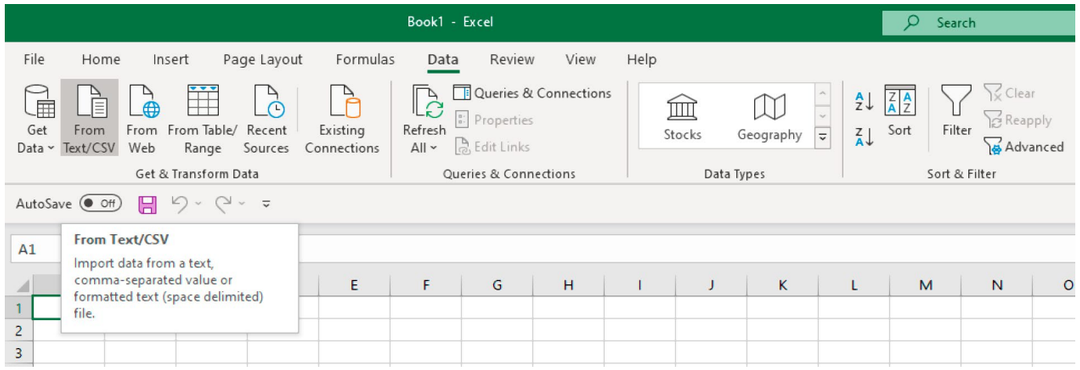
To export a capture stream into Comma Separated Values (CSV) file extension, go to **File > Export Packet Dissections > As CSV...**



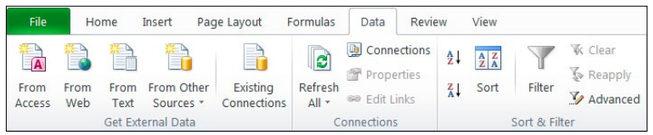
5.2.3. Deep Analysis with MS Excel

Step 1 – Import Data

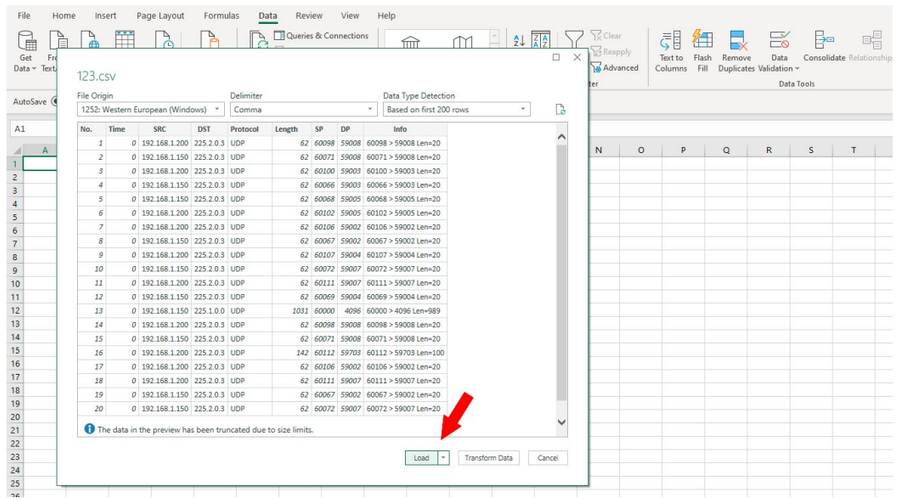
Start Microsoft© Office© 365 Excel and open a blank workbook. Go to **Data**, select "**From Text/CSV**", and select the .csv file containing the capture from Wireshark.



In MS Excel 2010, this step can be found in **Data > From Text**:



When the file is loaded, click on **Load** in the pop-up window:

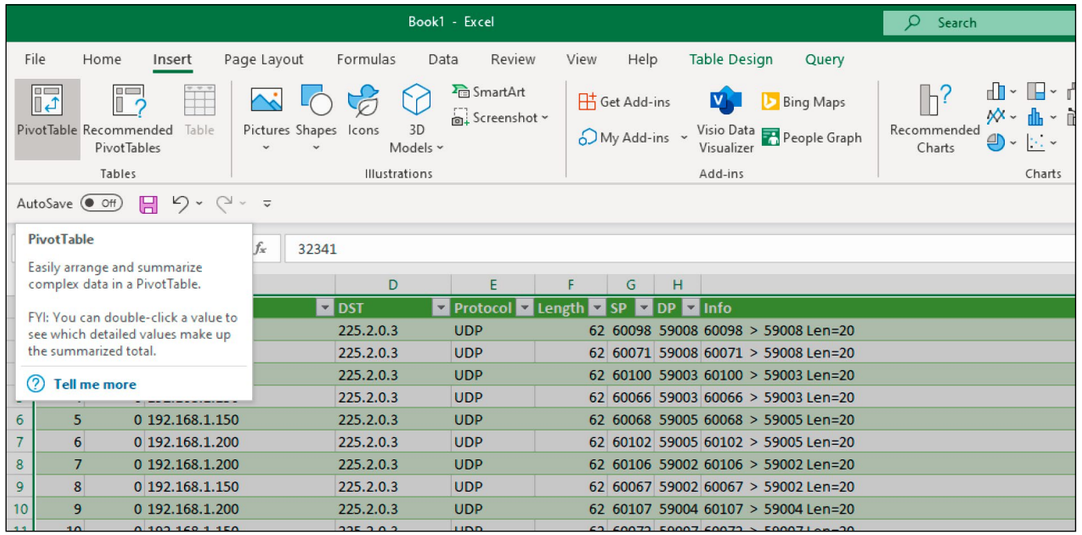


Step 2 – Create a Pivot Table

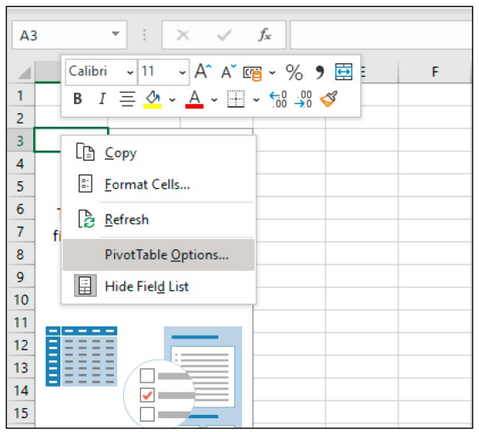
When the data table is loaded, select the entire table.

> TIPS AND TRICKS: Hotkey sequence with A1 cell selected:
> 1. Ctrl + <arrow down>
> 2. Ctrl + Shift + <arrow up>
> 3. Ctrl + Shift + <arrow right>

Go to **Insert**, and click on the **PivotTable** icon to create a pivot table report. It is preferred to select "New Worksheet" in the pop-up window to select where the pivot table will be placed.

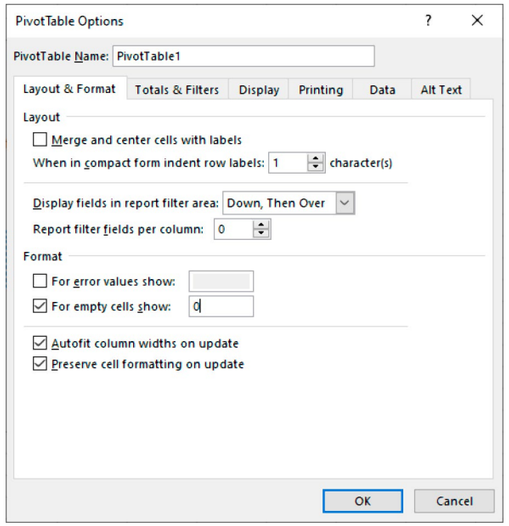


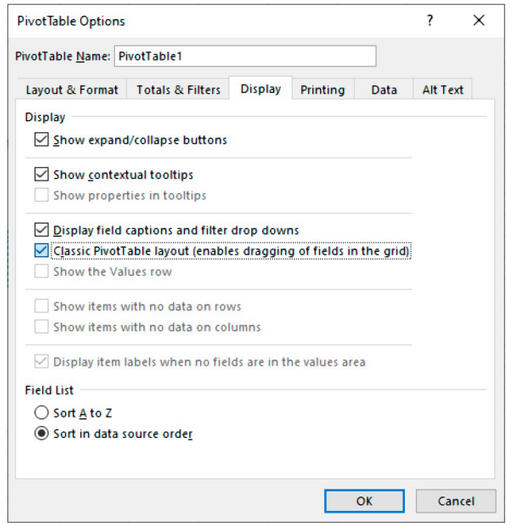
> TIPS AND TRICKS: Once the pivot table is created, right click inside the pivot table area and select **Pivot Table Options.**



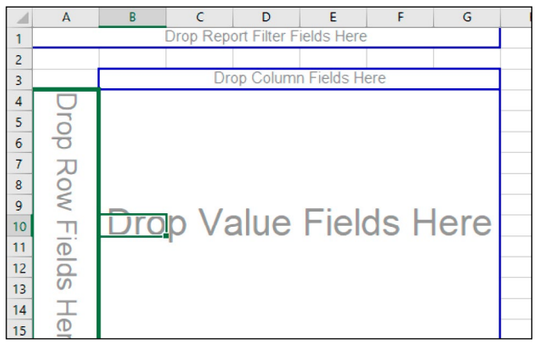
Step 3 – Pivot Table options

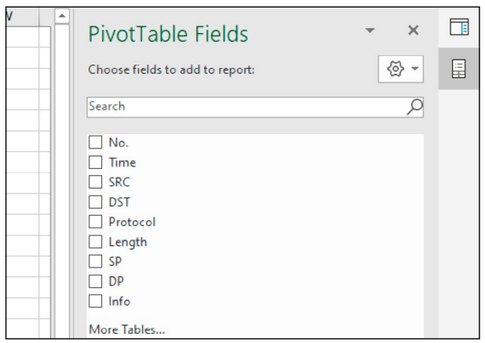
In the **Layout & Format** tab, in the cell next to the **"For empty cells show"** enter "**0**" to avoid empty cells and make sure the data is not skewed. In the **Display** tab, select the check box next to "**Classic Pivot Table layout**" to enable the drag & drop feature.





On the right side of the window the available Wireshark column names will appear. Drag and drop the values into the various cells of the pivot table to create the analysis table.



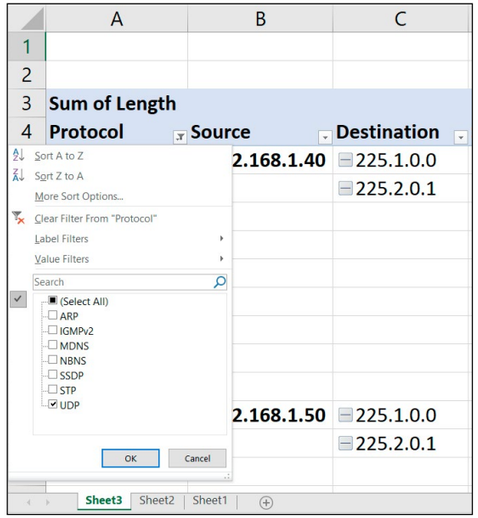


The preferred view is:

- In the Column Fields place the "**Time**" parameter (optional).
- In the Value Fields, place the "**Length**" parameter.
- In the Row Fields, place Protocol, Source address, Destination address, Source port, Destination port.

Step 4 – Example table

You can use the **filter** button ▼ in the column headline to enable/disable values, e.g. protocols.



Sum of Length					Time									
Protocol	Source	Destination	Src.Port	Dst.Port	0	1	2	3	4	5	6	7	8	Grand Total
UDP	192.168.1.40	225.1.0.0	60000	4096	4124	4124	4124	4124	4124	4124	4124	4124	2062	35054
		225.2.0.1	60262	59003	868	744	620	744	868	992	868	744	868	7316
			60264	59005	992	868	744	1116	992	744	496	992	496	7440
			60266	59004	868	496	1116	868	868	744	744	992	496	7192
			60267	59002	1116	992	868	744	868	868	620	744	496	7316
			60268	59008	1116	744	744	744	868	868	744	868	496	7192
			60269	59200	0	0	0	0	0	365224	680624	60960	46796	1153604
			60272	59801	180	0	0	0	0	0	0	0	0	180
			60273	59007	992	1240	1116	868	992	620	496	992	620	7936
	192.168.1.50	225.1.0.0	60479	4096	4124	4124	4124	4124	4124	4124	4124	4124	2062	35054
		225.2.0.1	60576	59003	868	744	620	744	868	992	868	744	868	7316
			60577	59004	868	496	1116	868	868	868	620	992	496	7192
			60579	59008	1116	744	744	744	868	868	744	868	496	7192
			60582	59002	1116	992	868	744	868	868	620	744	496	7316
			60583	59005	992	868	744	1116	992	744	496	992	496	7440
			60587	59201	0	0	0	0	0	124	0	0	0	124
			60588	59007	992	1240	1116	868	992	620	496	992	620	7936
			60589	59703	568	568	568	568	568	568	284	568	568	4828
Grand Total					20900	18984	19232	18984	19728	383960	696968	80440	58432	1317628