

Aatu Korhonen

UPDATING ISP CUSTOMER CONNECTIONS FROM COAXIAL CABLE TO FIBER

Bachelor's thesis
Bachelor of Engineering
Information Technology

2023



South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Aatu Korhonen
Thesis title	Updating ISP customer connections from coaxial cable to fiber
Commissioned by	MPY Telecom Oyj
Year	2023
Pages	35 pages
Supervisor(s)	Matti Juutilainen

ABSTRACT

Renewing network connections from old technologies to newer ones is a continuous process. As the internet is continuously growing larger and merging with our day to day lives. We are in demand of faster and more reliable connectivity. The objective of this thesis was to clarify the technical process of deploying new network connectivity technologies and what different steps are taking place in the process.

MPY is already providing network connections for customers via older cable connections and newer fiber optics. However, the idea is to expand and switch old technologies from the already existing customer base to the newer fiber optics technology.

In the deployment process there were many questions that needed answers. What is the deployment location, is the location fiber ready, is there old technology in use, how many possible customers etc.? This data is important because it guides in the process of choosing a switch device to the location. Switches come with different port amounts. Therefore, it is the best practice to choose a switch with port amount that is close, but not under the forecasted customer amount.

Careful documentation to network register is needed about the network connections and routes for each new deployment. Port information and descriptions about the switches on the installation location are also documented. Removing and unauthorizing old customer devices from databases. Setting up the new Milegate G.fast switches for deployment with updating firmware and configurations.

Keywords: ISP, telecom, G.fast, Last mile, networking

CONTENTS

1	INTRODUCTION	6
2	TELECOMMUNICATIONS	6
2.1	Wired technologies	7
2.1.1	Telephone lines	7
2.1.2	Ethernet	7
2.1.3	Cable networks	8
2.1.4	Fiber-optics networks	8
2.2	Advantages of switching to fiber-optics from older technologies	9
3	DATA FLOW FROM CUSTOMER TO THE INTERNET	9
3.1	Different devices in the network	10
3.1.1	Hosts	10
3.1.2	Switches	10
3.1.3	Routers	11
3.1.4	Firewalls	11
4	THE PROJECT	11
4.1	Defining the overall picture of the project	11
4.2	Mapping	12
4.3	Data analysis	13
4.4	Sales	13
4.5	Network register	13
4.6	Telecommunications team	14
4.7	Installers	14
5	DEVICE CONFIGURATIONS	14
5.1	Physical installment	14
5.1.1	Power cable	15

5.1.2	Optical transceiver module	17
5.1.3	Connecting cables	17
5.2	Switch configuration.....	18
5.2.1	Opening connection through console port	18
5.2.2	Basic configurations.....	20
5.2.3	Management configuration	22
5.2.4	Configuring customer access VLAN and DHCP	26
5.2.5	DHCP configurations	28
5.2.6	G.fast configurations.....	29
5.2.7	SNMP configurations	31
5.2.8	Configuration conclusion.....	32
6	CONCLUSIONS	32
	REFERENCES	33

1 INTRODUCTION

This thesis is about, MPY Telecom Oyj. It is a division of Mikkelin Puhelinyhdistys, a telecommunications company found in 1888 and based in Mikkeli, Finland. The company has two divisions, MPY Telecom Oyj and MPY Yrityspalvelut Oyj.

MPY Telecom Oyj is focused on providing modern and reliable telecommunications services to its customers, while MPY Yrityspalvelut Oyj help companies with their IT related problems. I have worked with MPY Telecom Oyj and am writing this thesis in relation to that.

I was part of a project aimed at futurizing telecommunications in Mikkeli and the surrounding regions, in which my role was to configure G.fast switches for the telecommunication premises of customer buildings to provide high-speed internet connections. The fiber connection in the telecommunication premises provided a foundation for future upgrades to the network and gave the building the flexibility to upgrade to newer technologies in the future.

My work was an important part of the company's ongoing efforts to improve and modernize the telecommunications infrastructure in Mikkeli and surrounding regions.

2 TELECOMMUNICATIONS

Telecommunications also known as Telecom is a term that is often heard, and it is used to describe many different types of communication technologies. Some examples of telecommunication technologies include the following:

- Wireless
- Wired
- Broadcasting
- Internet
- Emerging

I will be writing about wired networks, since it is closest to my thesis's topic. As a last mile provider, MPY provides the final part of communication service delivery to a customer. Which means that they are the ones who provide high quality network connections to customers.

2.1 Wired technologies

According to GeeksforGeeks(<https://www.geeksforgeeks.org/types-transmission-media/>). Transmission media is a definition of the physical infrastructure that is being used in Telecommunications. Different types of transmission medias are:

- Telephone lines
- Ethernet
- Cable networks (coaxial)
- Fiber-Optics networks

2.1.1 Telephone lines

Telephone lines use copper wires to transmit voice signals. This is considered legacy technology nowadays, since it is not implemented on new constructions, but it is still in use in older buildings.

Telephone lines downsides are that it offers limited bandwidth, so it isn't suitable for current fast internet requirements. They are sensitive to signal degradation and interference, which can affect the quality of the connection.

2.1.2 Ethernet

Ethernet is a local area network (LAN) technology that utilizes twisted-pair or fiber-optics cables for data transmitting between devices. It is one of the best ways to implement a LAN network, as it supports fast connections and isn't too expensive.

Ethernet's downside is that one cable can be only few hundred meters or less, otherwise, there will be signal attenuation, which means that the signal will get

weakened. Ethernet can be disrupted by other electrical devices, which can be prevented by using Shielded Twisted-Pair cables, which are expensive though.

2.1.3 Cable networks

Cable networks use coaxial cables for delivering broadband internet and cable television services to customers. At one point of time this was heavily used in city areas, because a cable TV was provided, so it was easy to just give internet connection using the same cabling.

Downsides for cable networks are that they have bandwidth limitations and the connection can be unreliable. There are also a lot of situations where there is only one cable providers in an area, which leads to a situation where they can decide the price for the service, since there is no competition or other providers to choose from.

2.1.4 Fiber-optics networks

Fiber-optic networks use glass or plastic fibers to transmit data using light signals. They can provide much faster and more reliable communication services compared to traditional copper wires.

Unidirectional fiber cable offers data transmission to longer distances but can only send data to one direction at a time. Unidirectional fiber cable is constructed in a way that it has only one fiber transmitting data inside the cable.

Bidirectional fiber cable is the opposite of unidirectional fiber cable. It offers data transmission to shorter distances but can transmit data to two directions simultaneously. Bidirectional fiber cable is constructed in a way that it has two fibres transmitting data inside the cable.

Although fiber optic networks present many advantages, there are also some disadvantages to take into consideration. These include physical damage, cost

considerations, structure, and the possibility of a fiber fuse(Nation, <https://fieldnation.com/resources/pros-and-cons-of-fiber-optics>).

2.2 Advantages of switching to fiber-optics from older technologies

Renewing and improving network connections is very important and the fast technological advancements of the modern day are making the telecommunications data transmission speeds faster.

The main reasons for switching from older technologies to fiber-optics are:

- better network bandwidth and capacity
- more reliable with less signal attenuation
- not affected by electromagnetic interference

Installing fiber-optics is expensive, but it is worth it in the long run. Reason being that the fiber-optics fulfil future needs for faster connections.

3 DATA FLOW FROM CUSTOMER TO THE INTERNET

Data flows from customer to the internet through an ISP. ISP provides the customer with a route to the internet. A brief summary of what happens when a customer browses the internet:

1. Customers host device verifies connectivity between itself and an ISP router
2. Customers router sends request to the internet websites web server; which is listening to ports 80(http)/443(https)
3. The request will be first routed by the customers home router (Default gateway) to the ISP router; which will then route the request to the internet
4. Once the request is received by the webserver it will respond with a HTTP response
5. Response will be delivered back to the customer

This will be explained in more detail at a device level in the following sub-chapters.

3.1 Different devices in the network

There are four main devices in the network that need to be covered. These devices are routers, switches, hosts and firewalls. All of these devices have their own purpose in the network functionality.

3.1.1 Hosts

Hosts are typically end user PC's or servers. Hosts have IP address and a MAC-address. Hosts communicate with MAC-addresses inside a LAN. Hosts have an ARP-table that includes other hosts with their matching IP address and MAC-address.

Hosts need the IP address to figure out who to send the packet to; host checks the destination IP and checks if it lays in the same network. If the destination IP lays in the same network, then the host sends an ARP request (which has the destination IP) through every port to the LAN network and waits for response from the destination host. Destination host then responds to the ARP request with its MAC-address and now the hosts can communicate with each other. If, however the destination IP doesn't lay on the same network, then the host will send the packet to the default gateway (router) which will then route the packet forward.

3.1.2 Switches

Switches are transmitting packets inside a local area network (LAN). Switches operate on the data link layer (layer 2). Switches forward frames between hosts inside a LAN using MAC-addresses. Switches have a MAC address table containing mapping about ports to MAC-addresses. Switch learns MAC-addresses by receiving frames from ports and then mapping the source MAC-addresses to those ports.

3.1.3 Routers

Routers are responsible for routing packets from a network to another network. Routers operate on the network layer (layer 3). When router receives a packet it will check it's own routing table for any network match where it can forward the packet to. If there is no match, then the packet is discarded. Therefore, it is a common practice to always add 0.0.0.0/0 route to the router so that the packet is always forwarded at least to the next router.

3.1.4 Firewalls

Firewalls are configured on the edge of a network to provide filtering of packets from addresses that are not permitted. In simplicity firewalls can be configured to block packets from specific ip-addresses and ports, however there are different types of firewalls that use different reasoning for their filtering.

4 THE PROJECT

MPY is undergoing a project. The main driver for this project is to provide improved network connections for ISP customers. This is a big project and needs a lot of help from different departments inside MPY.

4.1 Defining the overall picture of the project

To reach the goal of this project, MPY needs to map the buildings around central Mikkeli. Information that is needed from the building mappings include:

- Is the building fiber optics ready?
- Is there electricity in the telecommunications premise?
- What kind of internal network the building possesses?

After this information is mapped and the data transferred to SharePoint the data can be analysed. Then the Sales department can take action and start marketing to the buildings residents and companies. Network register will be documenting and informing telecommunications team about the switch sizes that are suitable

for that building. The size of the switch depends on; how many current customers there are in the building or if condominium solution has been negotiated.

Telecommunications team will then configure the switch that is the right size port amount wise. After switches are configured they are handed out for Etelä-Savon Teleasennus (ESTA); which is a third-party company doing physical instalments for MPY.

4.2 Mapping

Mapping of the buildings is being done by a team of local vocational school students. This team consists of four pairs so the teams total size is eight members. Each pair is given a smartphone, master key, MPY-badges and additional old ABLOY keys in case the telecommunication premises door is behind an older ABLOY lock.

Every pair will pick a location which they are going to map. After the decision the pair moves to that location and look for a key-stash on the building; which is usually located near the entrance door of the building. Key-stash will be opened with the master key. Key that is inside the key-stash will allow access to the building.

Once inside the building the pair will use their smartphone and take pictures. In the lobby of the building the pair is taking pictures of the residence list and the noticeboard. These pictures help the later steps of this big project, giving the information about amount of apartments in the building and also the property manager of the building.

After taking pictures in the lobby the pair will look for the telecommunications premise. This premise is typically behind a door that has MPY-plate or has a "switchboard" text on the door. The key-stash key usually fits the lock of this door.

Once inside the telecommunication premises the pair is instructed to take pictures of the following:

- cable connections
- cable-tv transformer
- power sockets
- racks
- fiber-panels

When all of this information is gathered from the building, the pair can leave the building, they are instructed to place the key-stash key back in it's original position when leaving the location. Next step for them is to upload the pictures to SharePoint and inform about it.

4.3 Data analysis

The mapping team will provide pictures and these pictures will be analyzed for data. I was doing this data analysis in cooperation with Network register team. We at MPY had an excel that we were all filling with different data.

4.4 Sales

Sales will market services for these mapped locations by using the data analyzed before as a reference. They will need current customer amount, current company customer amount and apartment amount to do their job efficiently.

Although it must be noted that apartment amount is only relevant if the condominium agrees to a solution that will include the whole condominium.

4.5 Network register

Network register will decide and document the routes and connections related to these network installations. It is important that the device location and cabling routes are well documented. Good documentation eases the future device maintenance and possible replacements.

4.6 Telecommunications team

Telecommunications team gives speed profiles to customers and helps with configurations. This team also guides the workflow to the installers and when there are devices available for installation. They acted as my mentors in case of emergency.

4.7 Installers

Installers are responsible for the physical installation of the devices. This includes the responsibility on making sure that the devices are in clean and secure rooms and that the wiring is carefully attached to the device.

5 DEVICE CONFIGURATIONS

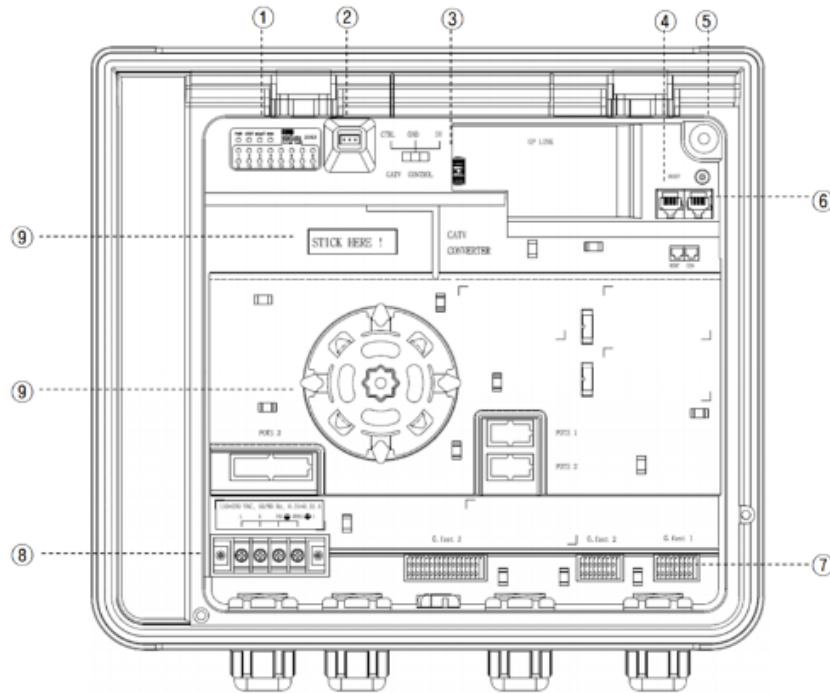
I was responsible for configuring the devices that are delivered to every buildings telecommunication premises. The devices I configured were DZS MileGate G.Fast devices. These devices come in three different port-amounts; which are:

- MileGate G.Fast MG2502 (8-port)
- MileGate G.Fast MG2503 (16-port)
- MileGate G.Fast MG2144 (24-port)

I had to add all the necessary routing information from MPY to the destination, and configure the ports on G.fast device facing the customers. Also physical installments like screwing in power cable, adding a fiber optics transceiver module and adding MPY- and the devices hostname stickers to each switch.

5.1 Physical installment

For physical installments I used a blueprint as a guide from the official documentation (DZS,2022). The blueprint has all the different physical modules and where they are located on the device.



① System LED	LEDs show status of system/G.fast operation.
② CATV connector	CATV connector to be connected to CATV converter
③ Uplink port	Uplink module can be inserted into the port
④ MGMT port	Equipment management port without effect to system performance.
⑤ Door button	The button monitor door open or intrusion.
⑥ Console port	Console terminal can be connected to equipment through this port.
⑦ G.fast(RJ21)	The ports to be connected to subscriber CPE.
⑧ Terminal Block	AC power input terminal
⑨ Fiber handling	Mechanical handling of optical fibre
⑩ CATV Converter fixation	CATV converter fixation location.

Figure 1. Physical blueprint

Above is a picture of the devices blueprint. Blueprint contains detailed information of the devices connections.

5.1.1 Power cable

First, I attached a power cable to the switch using a screwdriver. Attachments were made to position (8) **Terminal block** in the figure **x** above. The order of the wires were:

- Brown to **L**
- Blue to **N**

- Yellow/Green to **PE**

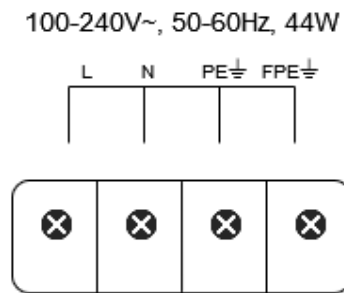


Figure 2. AC block.



Figure 3. AC-power cord.

Wiring order was done accordingly in reference to the figure 2. Cable used is displayed in figure 3.

5.1.2 Optical transceiver module

Then I attached a fiber optics transceiver module to the (3) **Uplink port** on figure 1 above. Transceiver module I attached to the switch, was a BCC-solutions NOK-SFP-10GB-B20-3327. This transceiver module is bi-directional so it can send and receive data at the same time. It has a 20km range of functionality.



Figure 4. Transceiver module

After I had attached transceiver module and the AC-cord I glued stickers to the devices exterior surface. I glued a MPY sticker with MPY's technical support phone number and a sticker that contained the devices hostname.

5.1.3 Connecting cables

I had to connect my PC to a console port that used RJ-45 connector on the switch, see the location (6) **Console port** figure 1 above. I needed a USB to console adapter for the connection. This console connection was needed to configure the switch. I used a command line interface called PuTTY to give configuration commands to the switch.

Next, I connected a fibre cable to the transceiver module I attached to the switch earlier, see the location of (3) **Uplink port** from figure 1 above. This fibre cable was connected to the same management network where we will be controlling

the devices when they are installed to their final locations. This was an important step, because it enabled me to test the management networks connectivity before giving the device for the installers.

Then I attached the power cord to a wall socket and turned the switches *I/O-switch* to position I; which means that the electricity can flow to the switches components now. Now the switch is ready for the actual software configuration.

5.2 Switch configuration

The switch was configured through a command line interface by giving it commands. When configuring the switch, I gave the switch different configurations:

- Basic configurations
- Management configurations
- DHCP configurations
- Bridge configurations
- G.fast configurations
- SNMP configurations

I will be going over the configuration in steps. First, I go through management configurations. Towards the end I will be going over more advanced configurations.

5.2.1 Opening connection through console port

Through my previously attached console cable connection from my PC to the switch I could connect to the switch using command line interface. I made the connection using PuTTY. I added needed parameters to PuTTY to establish a connection between my PC and the switch, the figure 5 shows the used parameters.

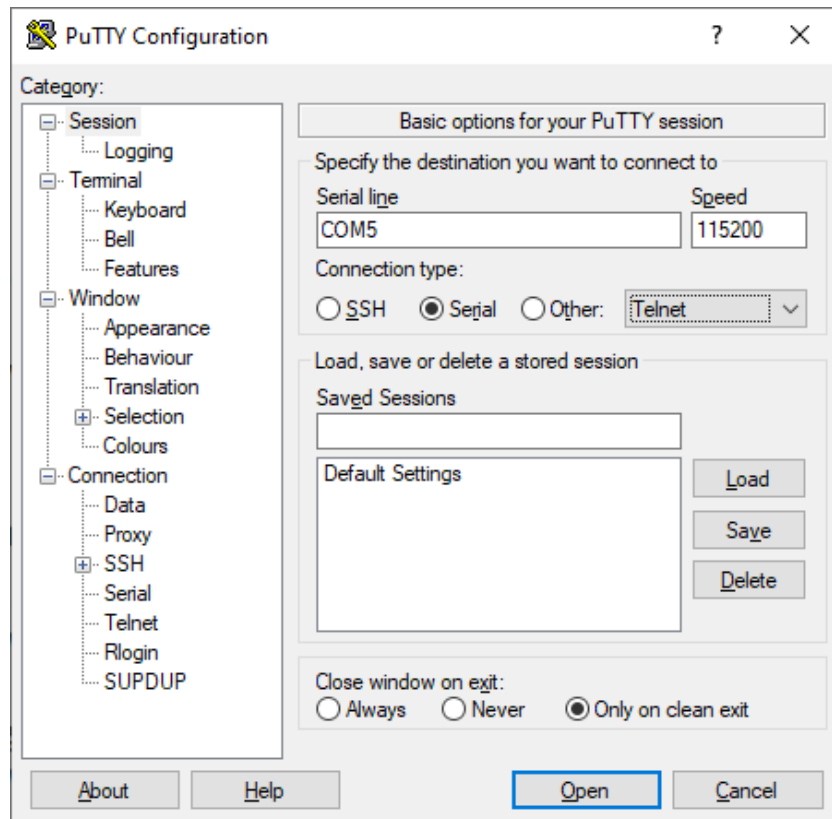


Figure 5. Putty configuration screen

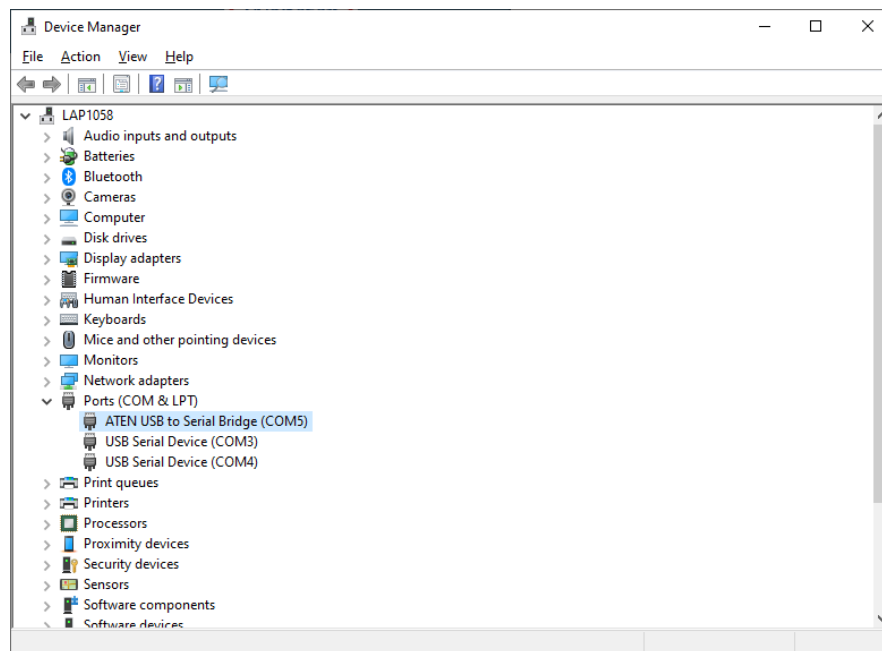
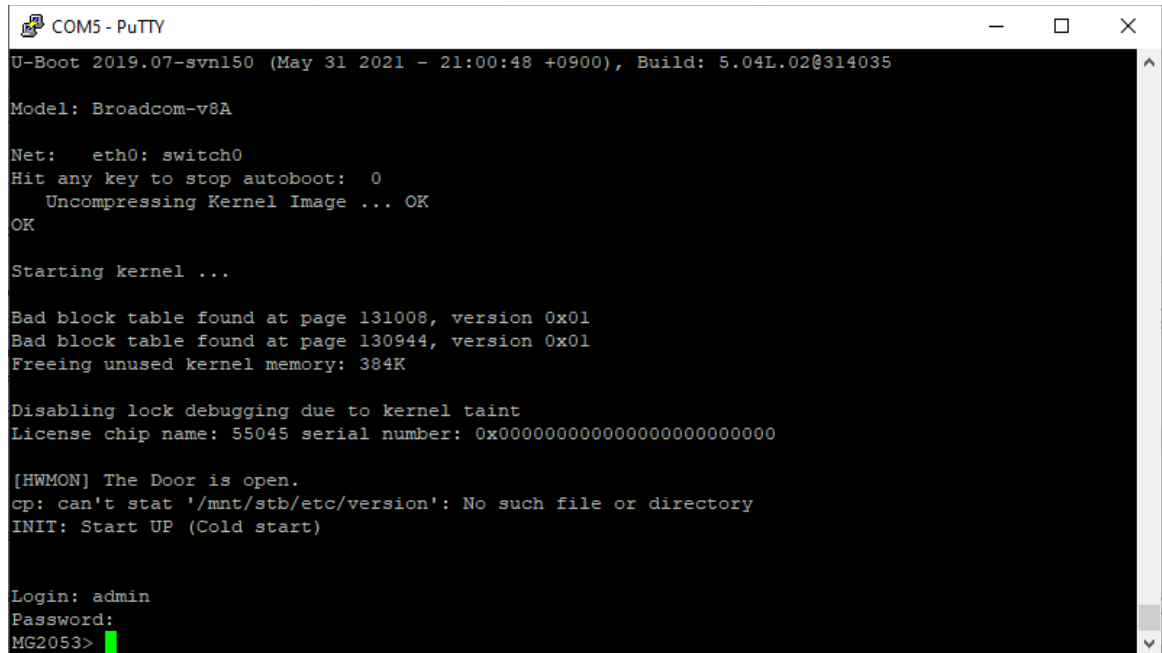


Figure 6. COM port check from device manager

The *ATEN USB to Serial Bridge (COM5)* in the figure 6 is the adapter I am using, so I can see that the serial line I have to use for this connection to work is *COM5*.

Speed parameter; which is *115200* is given in the DZS documentations (DZS, 2022). Then choosing connection type *Serial* and clicking *Open* will open a connection from PuTTY command line interface through COM5 to the switch.



```
COM5 - PuTTY
U-Boot 2019.07-svn150 (May 31 2021 - 21:00:48 +0900), Build: 5.04L.02@314035
Model: Broadcom-v8A
Net: eth0: switch0
Hit any key to stop autoboot: 0
Uncompressing Kernel Image ... OK
OK
Starting kernel ...

Bad block table found at page 131008, version 0x01
Bad block table found at page 130944, version 0x01
Freeing unused kernel memory: 384K

Disabling lock debugging due to kernel taint
License chip name: 55045 serial number: 0x000000000000000000000000

[HWMON] The Door is open.
cp: can't stat '/mnt/stb/etc/version': No such file or directory
INIT: Start UP (Cold start)

Login: admin
Password:
MG2053>
```

Figure 7. Fresh first boot

After opening connection using PuTTY you are asked for Login and password. They are both just **admin**. Now the device and connection, is ready for configurations.

5.2.2 Basic configurations

Basic configurations include eg. hostname, ntp, time-zone, syslog and banner. These were given to the switch as console line commands, first entering **enable** mode and then **configure terminal**, which is the global configuration mode:

Then I gave the switch its hostname **MLI0000-jokukatu12-ad1.mik** which was constructed from different parameters telling information about the location and connections through the network. The first parameter **MLI000** is the distribution identifier; each device in the private network has their own distribution identifier, this information is important because it is used as an ID in different applications

through the whole company. The second parameter **jokukatu12** is the address where the device is installed and running at. The third parameter **ad1** defines the mother device. Fourth, which is the last parameter defines the city **.mik**, where the network distribution device is located at. Also changing the admin password from the default one **passwd admin Gfast123**.

Next, I moved on to giving ntp server command for the switch **ntp 82.197.31.5**, ntp protocol gives time for the switch and is therefore important that every networking device is connected to the same ntp server, so that the time stamps on logs are synchronous. I also specified the time-zone for the switch **time-zone GMT+2**.

Syslog's were configured next which are responsible for logging commands and logins on the switch. In this case we had it stored locally

syslog output info local volatile

syslog output info local non-volatile

and externally. External logging was done by sending the logs to a remote server

syslog output debug remote 82.197.31.5. Logs are important for inspecting

login data and what commands were used with what login.

Next up banners.

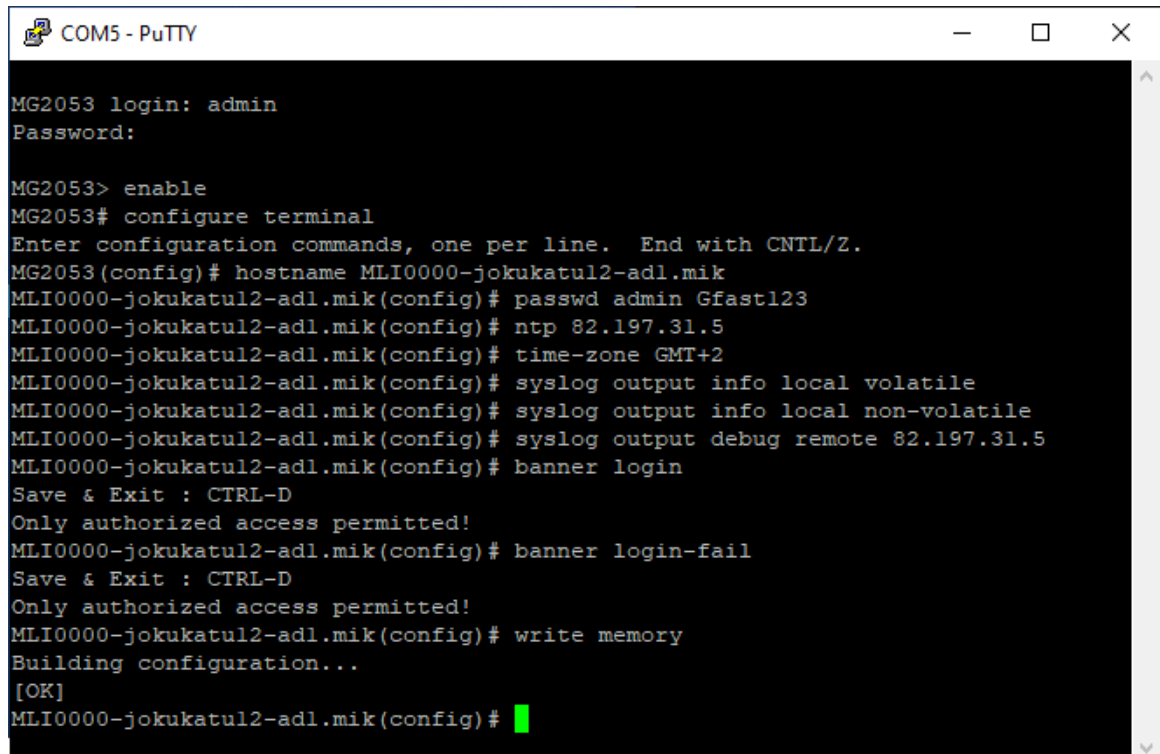
banner login

banner login-fail

Banners give the user a prompt on successful or unsuccessful logins. It is a common standard to use banners to let the user know that they are accessing a sensitive device.

All of these commands above are saved on the running configuration at this point, which means that if the switch loses power or is rebooted it will lose those configurations. Therefore, I used **write memory**. Write memory command writes the running configuration to the startup configuration.

The list of commands for basic configurations is shown in figure 8.



```
COM5 - PuTTY
MG2053 login: admin
Password:

MG2053> enable
MG2053# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MG2053(config)# hostname MLI0000-jokukatul2-adl.mik
MLI0000-jokukatul2-adl.mik(config)# passwd admin Gfast123
MLI0000-jokukatul2-adl.mik(config)# ntp 82.197.31.5
MLI0000-jokukatul2-adl.mik(config)# time-zone GMT+2
MLI0000-jokukatul2-adl.mik(config)# syslog output info local volatile
MLI0000-jokukatul2-adl.mik(config)# syslog output info local non-volatile
MLI0000-jokukatul2-adl.mik(config)# syslog output debug remote 82.197.31.5
MLI0000-jokukatul2-adl.mik(config)# banner login
Save & Exit : CTRL-D
Only authorized access permitted!
MLI0000-jokukatul2-adl.mik(config)# banner login-fail
Save & Exit : CTRL-D
Only authorized access permitted!
MLI0000-jokukatul2-adl.mik(config)# write memory
Building configuration...
[OK]
MLI0000-jokukatul2-adl.mik(config)#
```

Figure 8. Basic configurations

Basic configuration is the first important step in the configuration process of a switch.

5.2.3 Management configuration

In this section I will be configuring the part that is needed for the switches remote management after the switch is installed to its final location and firmware update because default firmware version **1.10_0001** is old . In management configuration I configured:

- Management VLAN
- Management interface with IP
- Default IP route
- Updating latest firmware version *1.14_0001*

This step of configuration will start the same way as the basic configurations, by first logging in to the switch, then switching to **enable** mode and then entering to **configure terminal** mode.

Then I configured management VLAN for the switch by passing in command **bridge** to enter the bridge configuration mode and then creating a management vlan for the device **vlan create 2**. Then adding the VLAN to a port **vlan add 2 25**. Then tagging the VLAN **vlan tagged 2 us**. Tagged VLAN ports are also referred as “Trunk ports” these ports expect VLAN tags inside of the frames. When VLAN port is tagged it can deliver and receive packets from many different VLANS using a single port. The tag will contain information about the VLAN the frame is part of.

Next up I configured the bridge interface matching the management VLAN by exiting **exit** the bridge configuration and using **interface br2** in the global configuration mode. After entering the interface configuration I gave the interface an IP-address **ip address 10.120.1.4/24** and made opened the interface with **no shutdown**.

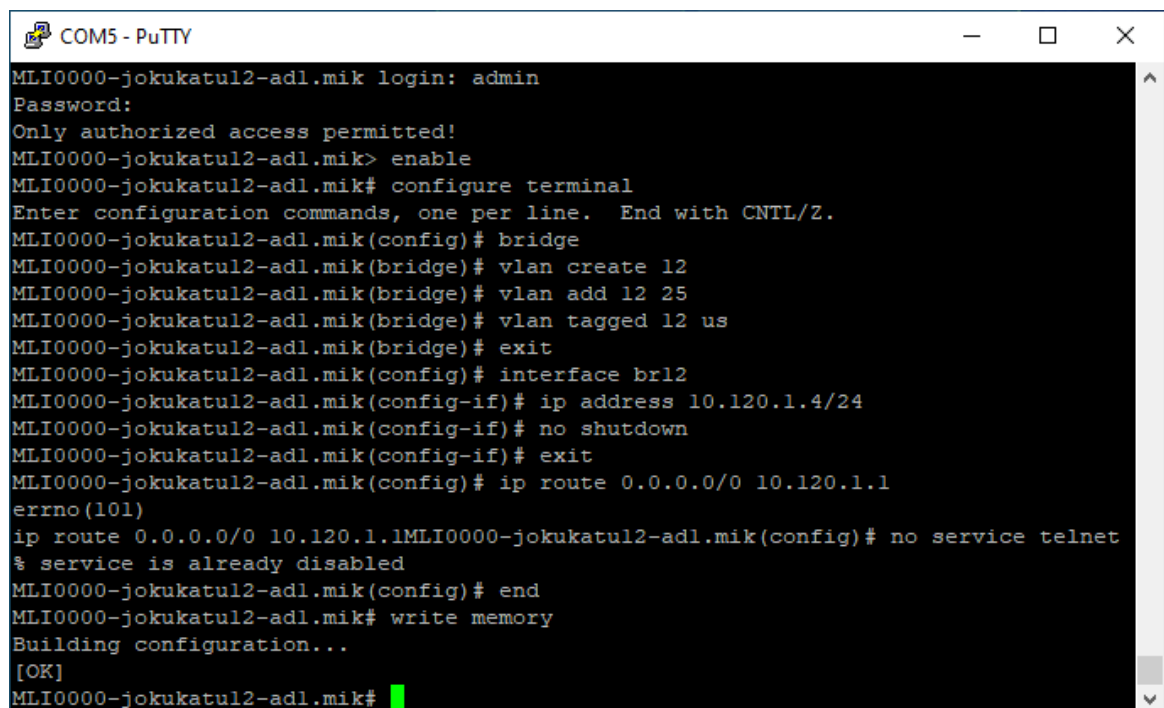
After this I gave the switch a default route. I had to exit the interface configuration for br2 by using **exit** and then in the global configuration mode used command **ip route 0.0.0.0/0 10.120.1.1**. In this command the **0.0.0.0/0** address is the default destination route for packets. **0.0.0.0/0** covers all the IP-addresses in the IPv4 address space, which means that the destination route is going to be the first “gateway” match the switch can sense in the network. The **10.120.1.1** address is the default gateway address. This address is the main device that connects this switch to the world wide web.

There is two types of remote connection protocols on this device by default: Telnet and SSH and they are both enabled by default. Telnet is very old and has no encryption, all the data it sends and receives is in plaintext. If someone is eavesdropping the connection, one can easily see the data that is being transmitted over that connection, only if they are in the same network of course. SSH is the better version of Telnet, since it offers password encryption and connection authentication using Asymmetric keys. So, I disabled Telnet by using

no service telnet. We don't want to have telnet enabled since there is the possibility to use SSH which is way more secure.

Now that management parameters were configured, I saved everything to the startup configuration once again using **write memory.**

The list of commands used for management configurations is shown in figure 9.

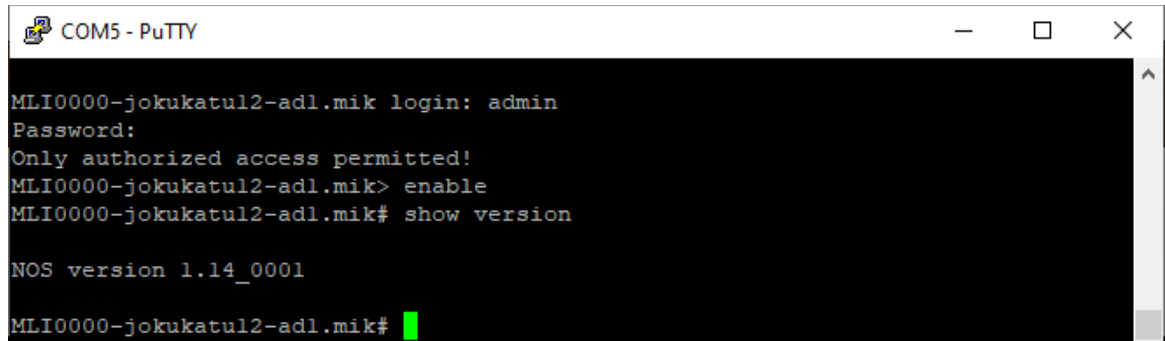


```
COM5 - PuTTY
MLI0000-jokukatul2-ad1.mik login: admin
Password:
Only authorized access permitted!
MLI0000-jokukatul2-ad1.mik> enable
MLI0000-jokukatul2-ad1.mik# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MLI0000-jokukatul2-ad1.mik(config)# bridge
MLI0000-jokukatul2-ad1.mik(bridge)# vlan create 12
MLI0000-jokukatul2-ad1.mik(bridge)# vlan add 12 25
MLI0000-jokukatul2-ad1.mik(bridge)# vlan tagged 12 us
MLI0000-jokukatul2-ad1.mik(bridge)# exit
MLI0000-jokukatul2-ad1.mik(config)# interface br12
MLI0000-jokukatul2-ad1.mik(config-if)# ip address 10.120.1.4/24
MLI0000-jokukatul2-ad1.mik(config-if)# no shutdown
MLI0000-jokukatul2-ad1.mik(config-if)# exit
MLI0000-jokukatul2-ad1.mik(config)# ip route 0.0.0.0/0 10.120.1.1
errno(101)
ip route 0.0.0.0/0 10.120.1.1MLI0000-jokukatul2-ad1.mik(config)# no service telnet
% service is already disabled
MLI0000-jokukatul2-ad1.mik(config)# end
MLI0000-jokukatul2-ad1.mik# write memory
Building configuration...
[OK]
MLI0000-jokukatul2-ad1.mik#
```

Figure 9. Management VLAN config

Updating the firmware to the latest version was done through an tftp call from the command line interface enable mode which meant I had to exit the global configuration mode using **exit.** Then I used **copy tftp os download os** to download the firmware this command asked for tftp servers IP-address **10.120.1.92** and the file name **MG2053.1.14_001-02_loader.x** to download. The firmware was loaded from a tftp server in MPY's internal network. After a little bit of waiting the firmware was downloaded from the tftp server, then I was able to set the new firmware as the running operating system **default-os os2.** Then I

Then I checked if the newest version is running on the switch using command **show version**. I could see that the newest version **1.14_0001** is running on the switch. Now I was able to move to the next step in the configuration.

A screenshot of a PuTTY terminal window titled 'COM5 - PuTTY'. The terminal shows a login sequence for 'admin' on a device named 'MLI0000-jokukatul2-ad1.mik'. After logging in, the user enters 'enable' to reach the privileged EXEC mode (indicated by '#'). Then, the user enters 'show version', and the output is 'NOS version 1.14_0001'. The prompt returns to 'MLI0000-jokukatul2-ad1.mik#'.

```
COM5 - PuTTY
MLI0000-jokukatul2-ad1.mik login: admin
Password:
Only authorized access permitted!
MLI0000-jokukatul2-ad1.mik> enable
MLI0000-jokukatul2-ad1.mik# show version

NOS version 1.14_0001

MLI0000-jokukatul2-ad1.mik#
```

Figure 11. New firmware running on the switch

Having the newest firmware is important on devices. It makes the device more secure.

5.2.4 Configuring customer access VLAN and DHCP

Configuring customer access VLAN is done through bridge interface, which can be accessed by first entering **enable** then entering **configure terminal** and then **bridge** to the command-line interface. For the access VLAN I configured:

- VLAN ID
- Customer ports and trunk port
- Storm-control
- DHCP-server-filter

VLAN ID was created by entering command **vlan create 111**, in this command string 111 defines the VLAN ID. Then I added customer ports and trunk port to this VLAN 111 by entering a command **vlan add 111 1-16,25**, in this command string 111 defines the VLAN we want to add, 1-16 defines the customer ports and 25 defines the trunk port. Making the VLAN 111 tagged with command **vlan tagged 111 us**.

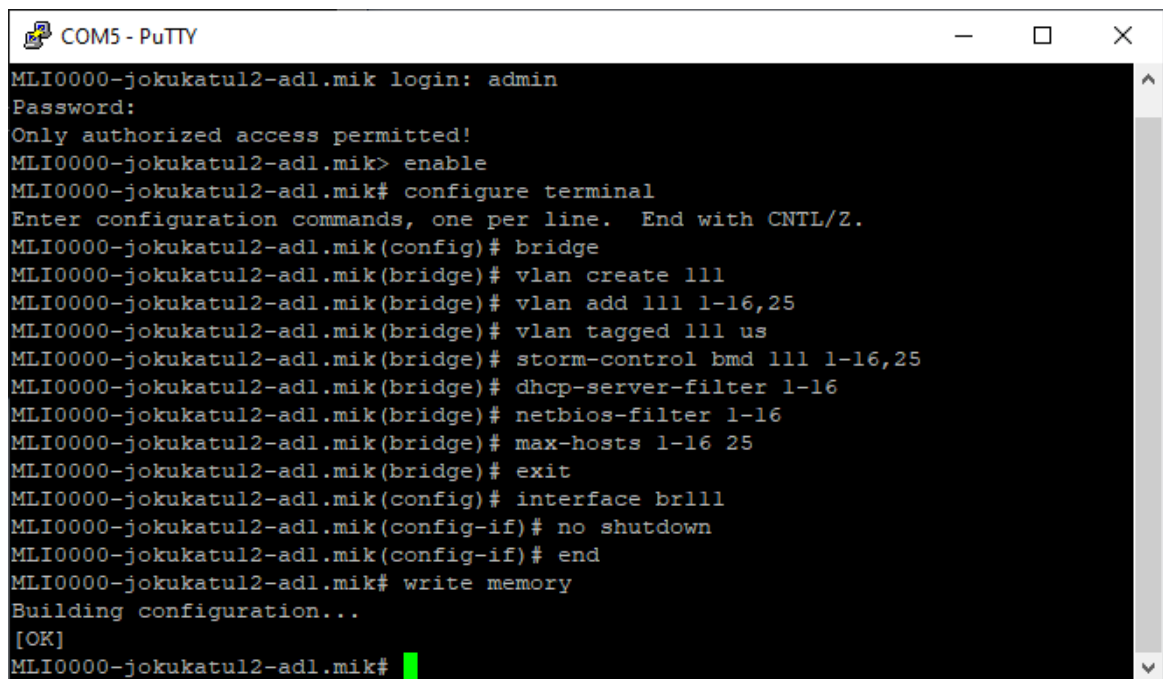
Next, I added storm control for all the interfaces. Storm-control was added by entering command **storm-control bmd 111 1-16,25**, this command adds storm-

control on ports 1-16 and 25 on VLAN 111 with bmd packet type. Then I added DHCP-server-filter and netbios-filter for ports 1-16 with commands **dhcp-server-filter 1-16** and **netbios-filter 1-16**. I also specified max-hosts 1-16 for port 25, by entering **max-hosts 1-16 25** which means that port 25 cannot handle more hosts simultaneously.

Finally, I enabled the port by entering interface configuration for vlan port 111 with **interface br111**. Then doing command **no shutdown** to enable the port.

Now that customer access VLAN parameters were configured, I saved everything to the startup configuration once again using **write memory**.

The list of commands used for access VLAN configurations is shown in figure 12.



```
COM5 - PuTTY
MLI0000-jokukatul2-adl.mik login: admin
Password:
Only authorized access permitted!
MLI0000-jokukatul2-adl.mik> enable
MLI0000-jokukatul2-adl.mik# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MLI0000-jokukatul2-adl.mik(config)# bridge
MLI0000-jokukatul2-adl.mik(config-bridge)# vlan create 111
MLI0000-jokukatul2-adl.mik(config-bridge)# vlan add 111 1-16,25
MLI0000-jokukatul2-adl.mik(config-bridge)# vlan tagged 111 us
MLI0000-jokukatul2-adl.mik(config-bridge)# storm-control bmd 111 1-16,25
MLI0000-jokukatul2-adl.mik(config-bridge)# dhcp-server-filter 1-16
MLI0000-jokukatul2-adl.mik(config-bridge)# netbios-filter 1-16
MLI0000-jokukatul2-adl.mik(config-bridge)# max-hosts 1-16 25
MLI0000-jokukatul2-adl.mik(config-bridge)# exit
MLI0000-jokukatul2-adl.mik(config)# interface br111
MLI0000-jokukatul2-adl.mik(config-if)# no shutdown
MLI0000-jokukatul2-adl.mik(config-if)# end
MLI0000-jokukatul2-adl.mik# write memory
Building configuration...
[OK]
MLI0000-jokukatul2-adl.mik#
```

Figure 12. Customer access VLAN configuration

VLAN configuration tells the switch what Virtual-LAN to use.

5.2.5 DHCP configurations

DHCP configuration commands were added from global configure mode, which was accessed through entering **enable** and then **configure terminal**. First I had to enable the DHCP service **service dhcp**. And then I activated DHCP snooping **ip dhcp snooping**. I added DHCP snooping for VLAN 111 **ip dhcp snooping vlan 111** and added limit rate of 15 on all customer ports **ip dhcp snooping limit-rate 1-16 15**. Limit rate 1-16 defines which ports the limit rate is added to and 15 defines how many DHCP packets per second can be transferred to each port. Then I added igmp snooping on VLAN 111 **ip igmp snooping VLAN 111**. “IGMP snooping prevents flooding of multicast traffic in L2 network environment.”(DZS, 2022).

Then I added settings for the DHCP, by entering IP DHCP option82 mode **ip dhcp option82**. After entering the DHCP options I added default policy for option82 packets **trust default permit** and then on port 25 I enabled all options82 packets on that port. Lastly I added a system circuit id to all customer ports **system-circuit-id x text MLI000-AD1-x**, this will be the defining factor for the switch to find speed and authorization for each customer port from RADIUS.

Now that DHCP configuration parameters were configured, I saved everything to the startup configuration once again using **write memory**.

The list of commands used for DHCP configurations is shown in figure 13.

```
COM5 - PuTTY
MLI0000-jokukatul2-adl.mik login: admin
Password:
Only authorized access permitted!
MLI0000-jokukatul2-adl.mik> enable
MLI0000-jokukatul2-adl.mik# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MLI0000-jokukatul2-adl.mik(config)# service dhcp
MLI0000-jokukatul2-adl.mik(config)# ip dhcp snooping
MLI0000-jokukatul2-adl.mik(config)# ip dhcp snooping vlan 111
MLI0000-jokukatul2-adl.mik(config)# ip dhcp snooping limit-rate 1-16 15
MLI0000-jokukatul2-adl.mik(config)# ip igmp snooping vlan 111
MLI0000-jokukatul2-adl.mik(config)# ip dhcp option82
MLI0000-jokukatul2-adl.mik(config-opt82)# trust default permit
MLI0000-jokukatul2-adl.mik(config-opt82)# trust port 25 all
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 1 text MLI0000-AD1-1
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 2 text MLI0000-AD1-2
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 3 text MLI0000-AD1-3
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 4 text MLI0000-AD1-4
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 5 text MLI0000-AD1-5
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 6 text MLI0000-AD1-6
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 7 text MLI0000-AD1-7
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 8 text MLI0000-AD1-8
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 9 text MLI0000-AD1-9
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 10 text MLI0000-AD1-10
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 11 text MLI0000-AD1-11
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 12 text MLI0000-AD1-12
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 13 text MLI0000-AD1-13
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 14 text MLI0000-AD1-14
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 15 text MLI0000-AD1-15
MLI0000-jokukatul2-adl.mik(config-opt82)# system-circuit-id 16 text MLI0000-AD1-16
MLI0000-jokukatul2-adl.mik(config-opt82)# end
MLI0000-jokukatul2-adl.mik# write memory
Building configuration...
[OK]
MLI0000-jokukatul2-adl.mik#
```

Figure 13. DHCP configurations

DHCP configurations enable the switch to use dynamic IP-addresses.

5.2.6 G.fast configurations

G.fast configurations were added by first entering enable mode **enable**. After that entering global configuration mode **configure terminal**. And lastly entering gfast mode **gfast**.

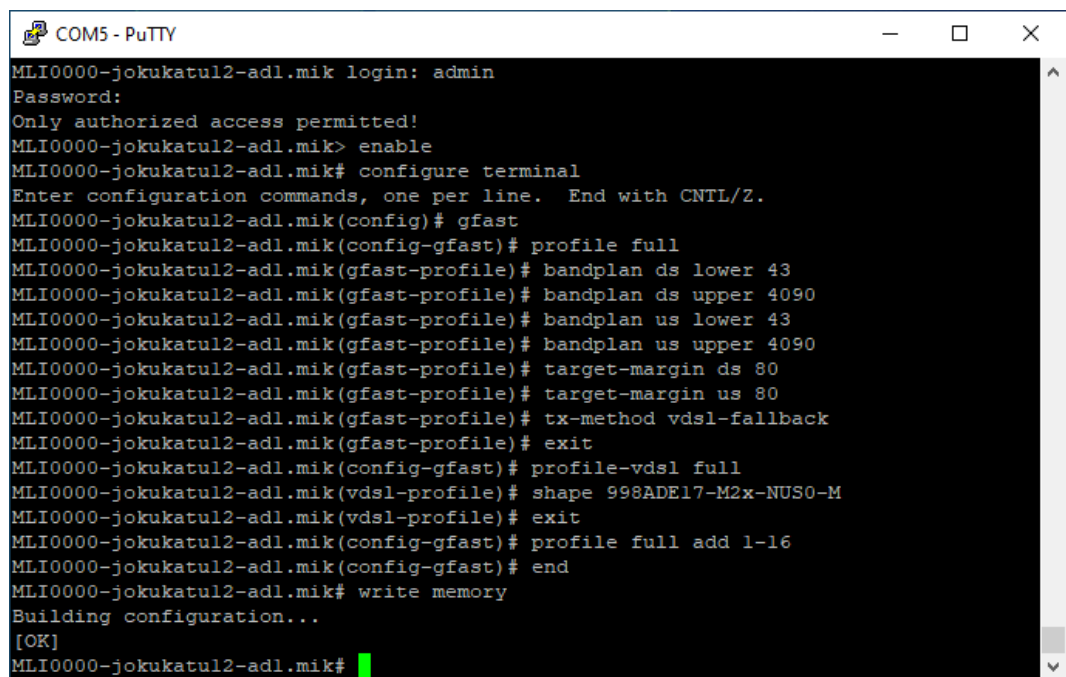
After entering gfast mode I defined a profile name with **profile full**. Then I added bandplan for upstream- and downstream dataflows. I specified sub-carrier downstream ranges with **bandplan ds lower 43** and **bandplan ds upper 4090**. Then I did the same for upstream sub-carrier ranges with **bandplan us lower 43** and **bandplan us upper 4090**.

I added target SNR margin of 8dB for upstream and downstream for Gfast line. SNR margins were added with **target-margin ds 80** and **target-margin us 80**. Then I specified that the G.fast line accepts only VDSL fallback protocol with **tx-method vdsl-fallback**. Then I exited profile full configuration to the G.fast root configuration with **exit**.

Now I added a VDSL profile to the G.fast line with **profile-vdsl full**. Added a standard VDSL PSD mask and bandplan to it with **shape 998ADE17-M2x-NUS0-M**. Now I exited to the G.fast root once again and added the profile full to all customer ports with **profile full add 1-16**.

Now that G.fast configuration parameters were configured, I saved everything to the startup configuration once again using **write memory**.

The list of commands used for G.fast configurations is shown in figure 14.



```
COM5 - PuTTY
MLI0000-jokukatul2-adl.mik login: admin
Password:
Only authorized access permitted!
MLI0000-jokukatul2-adl.mik> enable
MLI0000-jokukatul2-adl.mik# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MLI0000-jokukatul2-adl.mik(config)# gfast
MLI0000-jokukatul2-adl.mik(config-gfast)# profile full
MLI0000-jokukatul2-adl.mik(gfast-profile)# bandplan ds lower 43
MLI0000-jokukatul2-adl.mik(gfast-profile)# bandplan ds upper 4090
MLI0000-jokukatul2-adl.mik(gfast-profile)# bandplan us lower 43
MLI0000-jokukatul2-adl.mik(gfast-profile)# bandplan us upper 4090
MLI0000-jokukatul2-adl.mik(gfast-profile)# target-margin ds 80
MLI0000-jokukatul2-adl.mik(gfast-profile)# target-margin us 80
MLI0000-jokukatul2-adl.mik(gfast-profile)# tx-method vdsl-fallback
MLI0000-jokukatul2-adl.mik(gfast-profile)# exit
MLI0000-jokukatul2-adl.mik(config-gfast)# profile-vdsl full
MLI0000-jokukatul2-adl.mik(vdsl-profile)# shape 998ADE17-M2x-NUS0-M
MLI0000-jokukatul2-adl.mik(vdsl-profile)# exit
MLI0000-jokukatul2-adl.mik(config-gfast)# profile full add 1-16
MLI0000-jokukatul2-adl.mik(config-gfast)# end
MLI0000-jokukatul2-adl.mik# write memory
Building configuration...
[OK]
MLI0000-jokukatul2-adl.mik#
```

Figure 14. G.fast configurations

G.fast configurations tells the switch what kind of speed profiles are available for the switch to handle on each port.

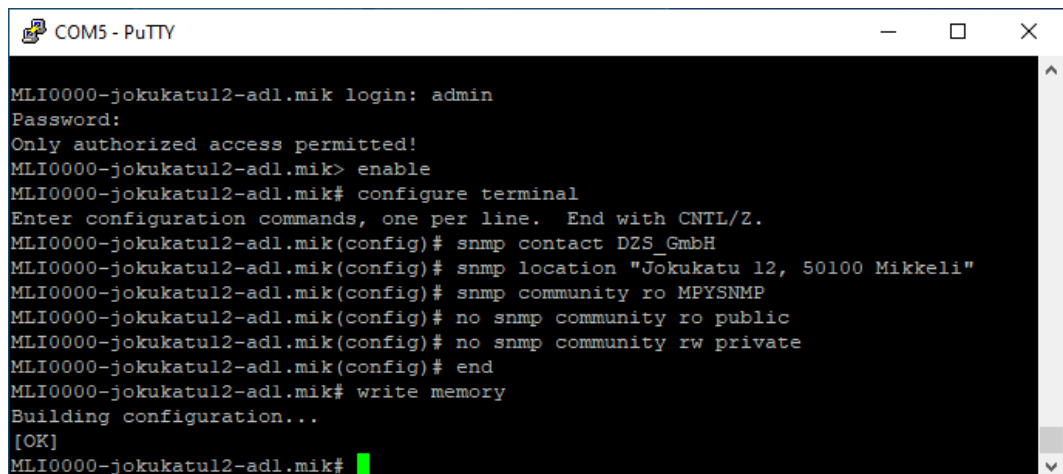
5.2.7 SNMP configurations

SNMP configurations were added from global configuration mode, by first accessing **enable** mode and then entering **configure terminal**. Then I added **snmp contact DZS_GmbH** this defines the manufacturer of the switch. Then I added **snmp location "Jokukatu 12, 50100 Mikkeli"** which defines the address where the switch will be operating at. Then I added **snmp community ro MPYSNMP**, ro means that it is read only and MPYSNMP defines the key SNMP manager and SNMP agent will use to share information.

Then I disabled two default SNMP configuration lines from the switch., because it is not a good practice to have default SNMP community configurations on the switch. I did **no snmp community ro public** and **no snmp community rw private**, to disable the two default community SNMP lines from the switch.

Now that SNMP configuration parameters were configured, I saved everything to the startup configuration once again using **write memory**.

The list of commands used for SNMP configurations is shown in figure 15.



```
COM5 - PuTTY
MLI0000-jokukatul2-adl.mik login: admin
Password:
Only authorized access permitted!
MLI0000-jokukatul2-adl.mik> enable
MLI0000-jokukatul2-adl.mik# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MLI0000-jokukatul2-adl.mik(config)# snmp contact DZS_GmbH
MLI0000-jokukatul2-adl.mik(config)# snmp location "Jokukatu 12, 50100 Mikkeli"
MLI0000-jokukatul2-adl.mik(config)# snmp community ro MPYSNMP
MLI0000-jokukatul2-adl.mik(config)# no snmp community ro public
MLI0000-jokukatul2-adl.mik(config)# no snmp community rw private
MLI0000-jokukatul2-adl.mik(config)# end
MLI0000-jokukatul2-adl.mik# write memory
Building configuration...
[OK]
MLI0000-jokukatul2-adl.mik#
```

SNMP configurations, Figure 15.

SNMP configurations make the switch more secure.

5.2.8 Configuration conclusion

Configuration was straightforward when understanding the purpose of these devices. The MileGate user manual was helpful and provided a lot of critical information, for the successful configurations.

6 CONCLUSIONS

Upgrading telecommunications to fiber optics in older buildings can be a big project, but it can be done with the help of G.fast. The Internet Service Provider (ISP) can deliver the fiber to the buildings premises which can then be converted to copper lining fitting technology with the help of G.fast. This makes the connection between the ISP and the customer very reliable and it eases future internal network updates in the buildings future.

I think that G.fast is good and easy to configure. I didn't get to see the end result (how G.fast actually worked on the customers end) because I didn't continue working with MPY for much longer.

The things that could be still investigated and measured is how well the systems actually work from the customers perspective. E.g. does the network deliver promised speeds? Is it reliable? Etc.

REFERENCES

GeeksforGeeks 28 February 2022. Types of Transmission Media. WWW document. Available at: <https://www.geeksforgeeks.org/types-transmission-media/>

DZS January 2022. MG205X User Manual. PDF document.

DZS December 2020. MileGate 2144 User Manual. PDF document.

Field Nation 12 March 2018. Pros and Cons of Fiber Optics. WWW document available at: <https://fieldnation.com/resources/pros-and-cons-of-fiber-optics>