softcream

Funded by
the European Union

A Short guidebook for school network administrators

in the SAT4EDU Project

SoftCream Software Sp. z o. o.
Grójecka 194/19
02-390 Warszawa
Poland
tel. +48 22 867 80 00
biuro@softcream.pl

This document was prepared within the framework of the SAT4EDU Project:
Pilot Project – Satellite Broadband Internet Access for Educational Multimedia Contents to Unconnected Schools (BBSat4Edu – 2019).

Author: Tomasz Kulisiewicz
Editor: Laurence Taylor
DTP & Graphics: SoftCream Software

1. Preface

Despite extensive efforts in Next Generation Access (NGA) broadband access for all – meaning all citizens, entrepreneurs, public administration, and educational institutions – there are, in the EU, still so called *white areas*, where no provider of broadband access services currently operates, and no such provider is expected within the near future. Formally, investors in such areas may obtain public support if no NGA access is expected within a three year period, but in many cases these areas may remain permanently *white* due to the sparse density of housing, and demographic or geographic factors (i.e., small islands, or small villages in the mountains).

But even in these areas of digital divide, there are still citizens' rights, and a demand for appropriate education, especially in the area of primary education in schools. This is so even in small schools in remote areas where there is not only insufficient demand for deploying a network (even with the support of public funds), but also not enough to keep its operation profitable for private investors and providers of broadband access. For such schools satellite access may be a solution.

The European Commission decided to launch a pilot project that investigates the practical aspects of satellite access for such schools, and to assess its viability. The pilot project consists of the deployment of satellite broadband access to chosen schools that are in permanently white areas. These schools are in Greece, Italy, and Poland.

2. The SAT4EDU Project's school network

The aim of the SAT4EDU project is to provide those schools participating in the project with broadband access that has speeds adequate for using the educational multimedia that can be found on educational websites and other educational services. The schools are provided with hardware (satellite dish and a modem/router) that connects the school's local network to the Internet. This is a two-way connection, which allows schools to share the content created by its pupils with other schools.

Depending on geographical location, each school received one set of devices, which were supplied by one of two satellite access suppliers cooperating with the project; but for the school administrator, there is no difference in the access between the two suppliers.

The school network is connected to the Internet via the SAT4EDU connectivity set, which consists of:

A satellite dish and converter (

- Figure 1),
- A satellite modem (Figure 2),

A Cisco Meraki MX64 SAT4EDU Security Gateway

(

- Figure 3).

There are additional elements such as connecting cables, power supply units, and fitting and supporting elements, which are also included in the set.

Within the framework of the project, the SAT4EDU connectivity set is supplied, installed, and configured by SAT4EDU support personnel free of charge, and does not need any special cooperation from the school network administrators.

Figure 1. Satellite dish with signal converter

Figure 2. Satellite modem

Figure 3. Meraki MX SAT4EDU Security Gateway

2.1. Installation of the SAT4EDU satellite connectivity set

Videos showing how to install the SAT4EDU satellite connectivity set can be viewed by clicking on the following links:

- Polish version - Tooway KA-SAT Instrukcja instalacji
- English version - Tooway KA Sat installation video

To properly positioning the satellite dish during installation, or to adjust its position if it has changed, there is a dedicated webservice at the following address:

http://finder.tooway-instal.com/fixe/pages/index.html

There are two Android apps available on Google Play that can also be used to position the dish:

- KA-SAT Finder

  https://play.google.com/store/apps/details?id=com.eutelsat.kasatfindr&hl=pl&gl=US

- KA-SAT Pointer pour Tooway

  https://play.google.com/store/apps/details?id=com.eutelsat.kasatpointer

2.2. An example of a school network connected to the Internet via the SAT4EDU satellite connectivity set

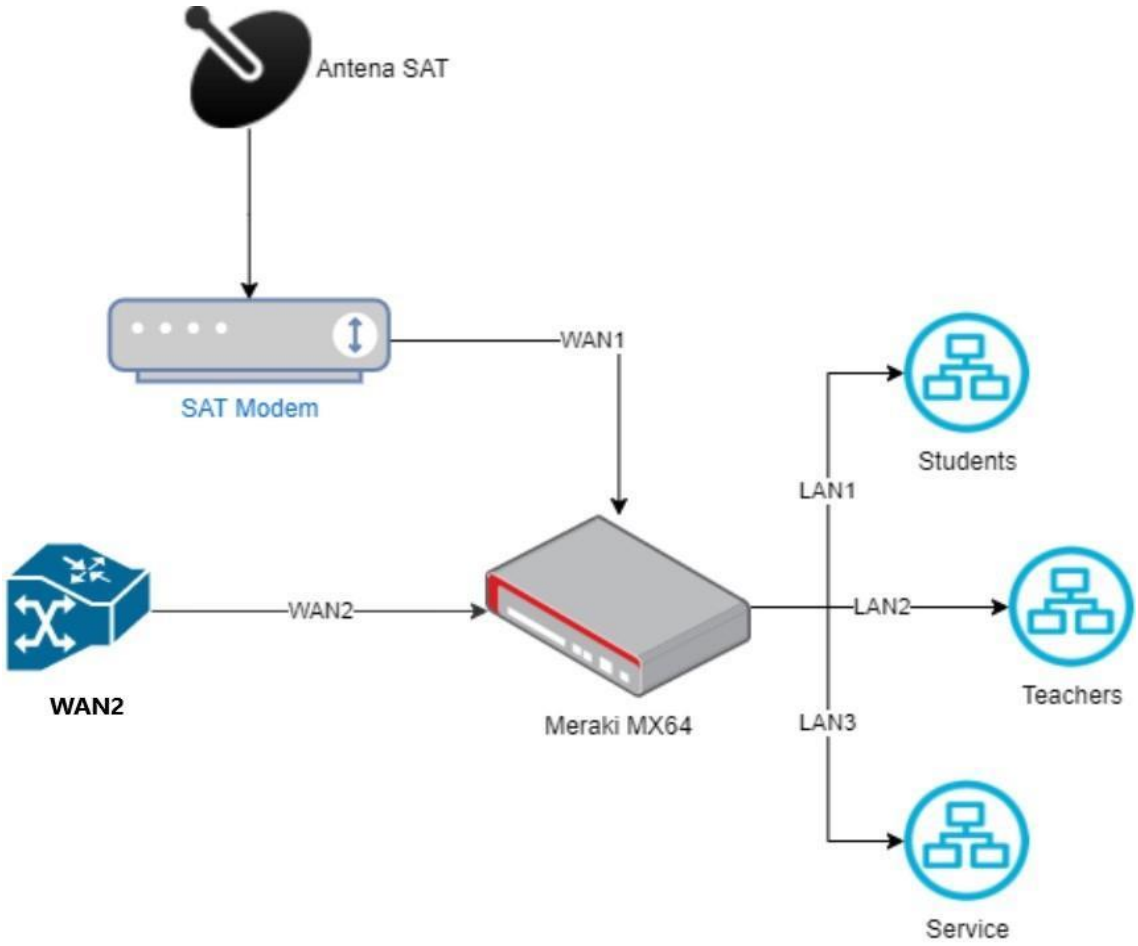

Figure 4.The school network connected to the Internet via the SAT4EDU satellite connectivity set

The school network is a part of school's infrastructure; it is not included in the equipment supplied within the framework of SAT4EDU project. A typical school network is shown in

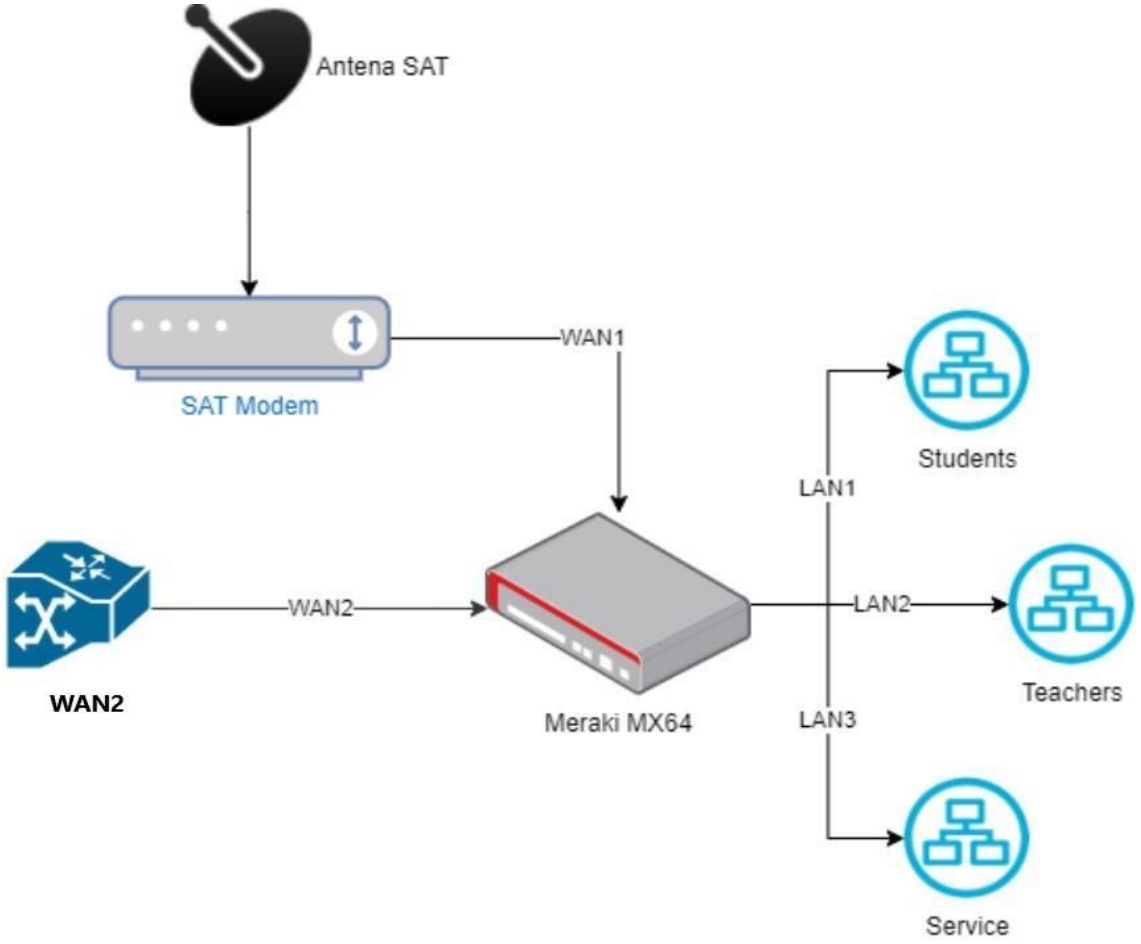

Figure 4, and consists of:

- teachers' computers (optional: a separate computer for the school network administrator),
- pupils' computers, supplementary equipment: other devices connected to the school network (file server, print server, networked printers),
- router (with optional Wi-Fi access point) – connected to the SAT4EDU connectivity set by an Ethernet cable, additional routers or switches (depending on the architecture and the number of computers connected to the school network),
- SAT4EDU diagnostic device (not shown in this guidebook).

The school network is connected to the dedicated ports in the Cisco Meraki MX64 SAT4EDU security gateway, as shown in Figure 5.

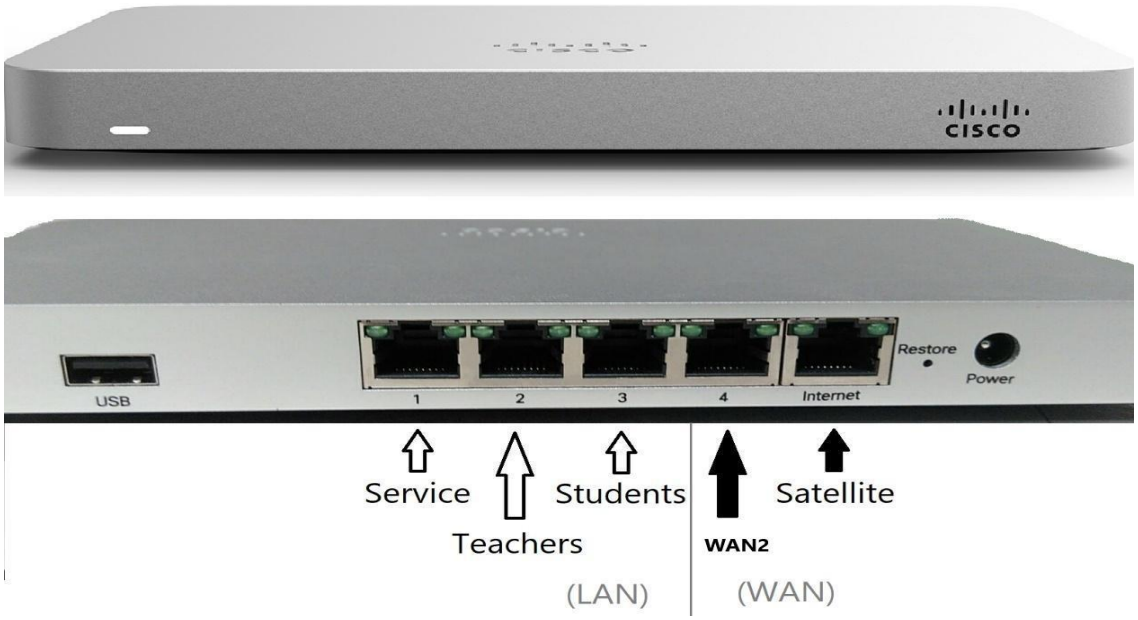

Figure 5. Ports in the Cisco Meraki MX64 SAT4EDU Security Gateway

For the typical configuration of a school network, the WLAN/LAN/VLAN ports of the Cisco Meraki MX64 SAT4EDU Security Gateway are used as shown in Figure 5:

1. The satellite modem is connected to the ***Satellite*** port (one of the ports in WAN zone marked INTERNET on the device),
2. The teachers' computers and the school network administrator's computer (if there is a dedicated admin computer) are connected to the ***Teachers*** port (one of the LAN ports marked 1–3 on the device),
3. The pupils' computers (or the school's local network router/switch for connecting pupils' computers) are connected to the ***Students*** port (one of the LAN ports marked 1–3 on the device),
4. The SAT4EDU diagnostic device (not shown in this guide) is connected to the ***Service*** port (one of the LAN ports marked 1–3 on the device),
5. An alternative, additional access device/connection (acting as a fallback, e.g. 3G/4G cellular network modem or a DSL modem on a fixed telephone line) is connected to the ***WAN2*** port (one of ports in the WAN zone, marked 4 on the device).

The USB port is used for optional local firmware upgrades of the Cisco Meraki MX64 SAT4EDU Security Gateway, which can only be done by SAT4EDU support personnel.

Additional SAT4EDU diagnostic devices (not shown in this guide) are accessed remotely only by SAT4EDU support personnel and cannot be switched off or removed by the school network administrator.

In some school networks, the network traffic on the **WAN2** and **Satellite** ports has to be additionally configured for proper load balancing. Configuring the load balancing and its parameters can only be done by SAT4EDU support personnel. School network administrators should not reconfigure this on their own. If it does not seem to work properly, they should contact SAT4EDU support personnel using the dedicated SAT4EDU technical support form (see Point 0).

In some cases, the entire school network may be connected to the ***Teachers*** port, but it should be noted that in the typical configuration, all the pupils' computers connected to the ***Students*** port will be protected by the Meraki security system, including advanced protection against malware and harmful content. The teachers and administrators' computers connected to the ***Teachers*** port are protected only by a basic firewall against external attacks. This protection setup is configured remotely by SAT4EDU support personnel, who can be contacted if the configuration needs changing.

3. The role and responsibility of the school network administrator

The role of school network administrator is as follows:

- managing the correct operation of the satellite connection,
- acting in order to restore operations in the case of failure,
- reporting problems and/or failures to the SAT4EDU support system.

It would be useful if the administrator was present during the installation of the satellite connectivity set, in order to see how to position the satellite antenna using the dedicated app or web-service mentioned in Point 2.

3.1. Access failures

The operation of the satellite connection is continuously monitored by SAT4EDU support personnel using diagnostic devices connected to the Meraki Security Gateway. In the simplest case, the school network administrator can try to act before the SAT4EDU support personnel start their own actions. The first thing to do in such cases is to check the status of satellite access displayed by the LEDs on the satellite modem

(

Figure 6).

Figure 6. The display (LED ring) that indicates the state of the modem and connection

The status of the modem and connection are indicated by the color and state of the LEDs on the display ring (see Table 1).

Display	*Meaning*
No display	Power off
White constant	Initialization procedure
White blinking	Starting connection
Blue constant	Connected
Blue blinking	Upgrading software/firmware
Orange blinking	Installing
Red constant	Modem reset needed (switching the power supply off and on). If this state (red constant) is displayed for more than 5 minutes, SAT4EDU support should be contacted.
Red blinking	Device/system failure. SAT4EDU support personnel should be contacted immediately.

Table 1. Types of LED display on the satellite modem

In practice the two most frequent cases of failures are:

- No power (No display on the satellite modem – see **Błąd! Nie można odnaleźć źródła odwołania.**)

After reinstating power there is no special action needed from the school network administrator, as the SAT4EDU connectivity set should resume its operation and broadband connection. If there is still no access, the administrator should reset (switching off and on) the modem, Meraki MX SAT4EDU Security Gateway, and the school network router.

- Failure of hardware elements (e.g. change in the position of the satellite dish, short circuit of the satellite converter caused by lightning discharge).

Such a failure will result in no Internet access, even if all devices are operational. The satellite modem's LED display will indicate this by displaying repeated attempts to connect to the Internet (i.e. white blinking then blue constant, white blinking again then red blinking or constant – see Table 1).

If there is fallback connectivity device (cellular modem or DSL modem on a fixed telephone line) connected it to port WAN2 on the Meraki MX SAT4EDU Security Gateway, and there is a satellite connection failure, the Meraki device will automatically switch the connection over to the fallback device. The WAN2 port and the fallback device are configured according to local circumstances by SAT4EDU support personnel during the installation of the satellite connectivity set.

If the circumstances suggest that the reason for the loss of broadband connection is because the antenna position has moved (e.g. as a result of strong winds), the administrator can try to reposition the antenna using the apps or webservice mentioned in Point 0. If the LED display on the satellite modem shows first white blinking then blue constant (see **Błąd! Nie można odnaleźć źródła odwołania.**) it means that antenna positioning has been reinstated correctly and the satellite connection is operating. If these actions do not deliver this result it may mean that the satellite converter has been destroyed, for example, by a short circuit caused by lightning; the administrator should report it immediately to the SAT4EDU support system.

3.2. Protecting the school network

All computer networks are subject to a range of external attacks. The main aim of such attacks is to steal data, block the operation of the network, or takeover the network. Usually there is no valuable data in school networks to be stolen (as there is in financial or industry networks). An attack that happens quite often is the so called DDoS (distributed denial-of-service) attack, which is a malicious attempt to disrupt the normal operation of a network by overwhelming it with a flood of Internet traffic. For school networks, the most dangerous attack is the network takeover, which results from planting malicious software in school computers, which will then attack the other networks, for example, by initiating a DDoS attack. In many cases, the network owners may not even notice that their network has been taken over and is being used as the source of an attack. The most common symptom of such an attack is extremely high traffic on the network, even when pupils and teachers are not using the network.

These types of dangerous situations are recognized by the Meraki MX SAT4EDU Security Gateway, which operates the SAT4EDU school protection system, and is monitored remotely by SAT4EDU support personnel. The system protects the school network and advanced software will additionally protect pupils' computers against accessing malicious content.

4. The SAT4EDU technical support system

Administrators should report network failures and problems by using the SAT4EDU technical support system. This service is for administrators who are registered in the SAT4EDU system (they are registered under their email addresses during the installation of the SAT4EDU connectivity set).

Administrators can make use of the system at the following address: https://www.softcream.pl/en/ai-research-projects/sat4edu/support-request/

A request for help or action is carried out by using the form that opens after clicking on "Report the problem." Further communication regarding the request for support or action is done by email communication between the registered address of the administrator and SAT4EDU support's email address (serwis@softcream.pl). The contact form is shown in Figure 7.

Once in the form, the type (topic) of problem/failure can be chosen from the list, or described manually after choosing "Other". When the description of the problem/failure has been entered and the privacy policy accepted, the person requesting support clicks on "Send." An email confirming the request for support will be sent to the administrator's registered email address.

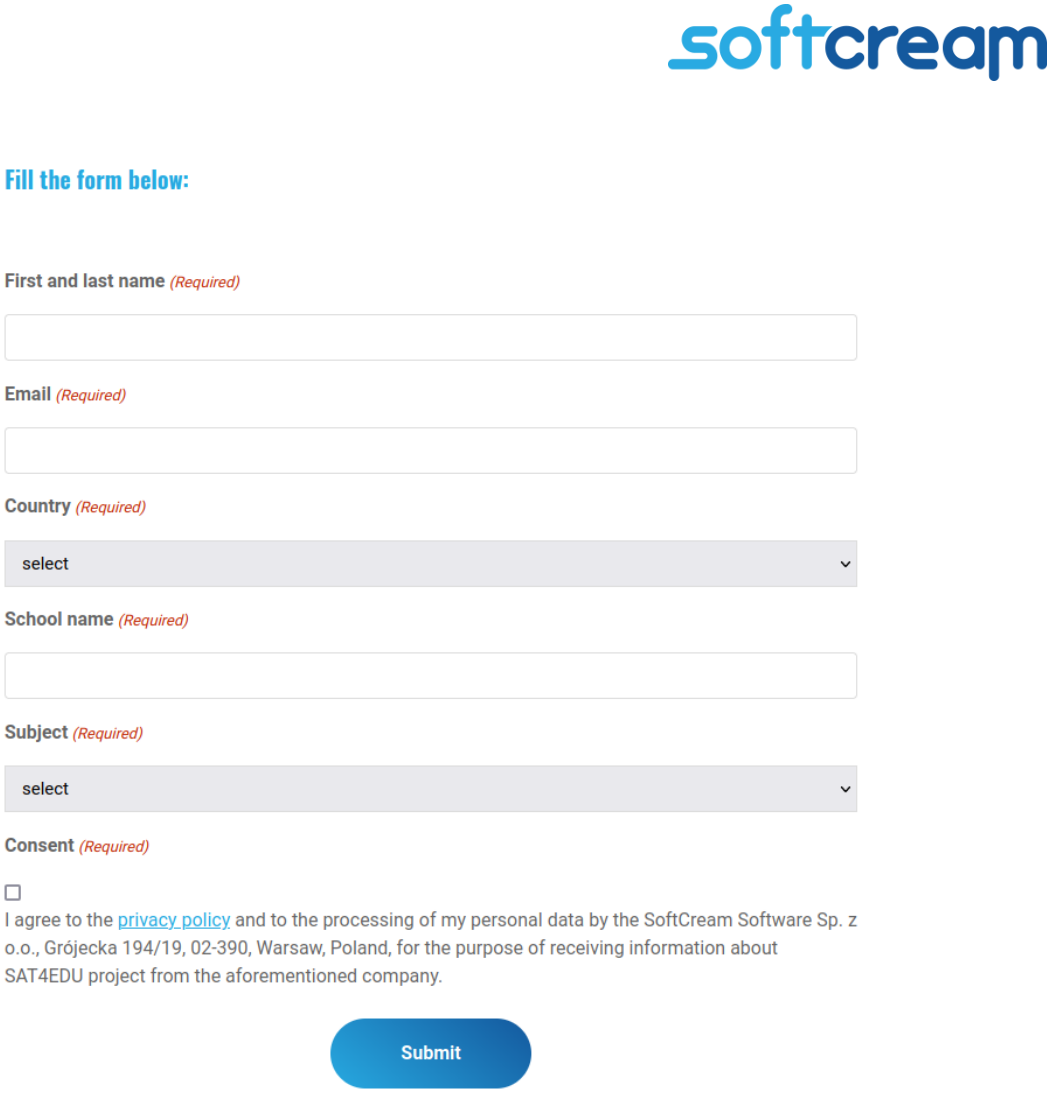

Figure 7. Request for support/report a problem form