ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

Optimization of Network Infrastructures Through the use of Cloud Solutions

Banza Mudinga Arsène [1]; Luyembi Tshiniama Honoré [2]

[1],[2]Higher Technical Pedagogical Institute of Kinshasa (Ispt-Kin) in the Democratic Republic of Congo

Publication Date: 2025/02/04

Abstract: The proper functioning of companies today relies on the quality of their network infrastructures. A good quality network therefore allows for a good user experience and better productivity.

In this article, we propose a solution for optimizing business network infrastructures, based on the cloud. This approach provides global visibility and centralized control of network equipment; wired and wireless, while significantly reducing the cost and complexity of traditional controllers.

The Cloud solution is best suited, because it allows today's companies to maintain infrastructures in operational condition and ensure high availability and allows administrators to deploy scalable and secure networks that comply with confidentiality regulations with complete peace of mind.

To illustrate our points, in this project we will present a practical case of configuring an optimization solution based on the Cloud solution from the manufacturer Cisco: CISCO Meraki.

Keywords*: Optimization, Cloud, Lan, Wan, Stp, Rpc, Dashboard, Cisco Meraki, Zero Touch Deployment.*

How to Cite: Banza Mudinga Arsène ; Luyembi Tshiniama Honoré (2025). Optimization of Network Infrastructures Through the use of Cloud Solutions. *International Journal of Innovative Science and Research Technology*, 10(1), 1619-1638. https://doi.org/10.5281/zenodo.14792223.

I. INTRODUCTION

The agility of the evolution of Internet technologies has enabled the deployment of dynamic network infrastructures using highly decentralized architectures and whose services are organized independently, thus creating the need for a centralized network architecture on the cloud for management. simple network infrastructures. This constitutes a major challenge for equipment manufacturers who must adapt to this development in order to remain competitive in the market and continue to offer services that meet customer needs.

➢ *Problematic*

The functioning of companies today relies on the quality of their network infrastructures, namely LAN, WIFI, WAN. A good quality network therefore allows for a good user experience and better provision of different services.

Some companies today have network equipment from different manufacturers in their infrastructures. The management and support of this equipment becomes more and more difficult when the size of the network or the number of sites increases.

The administration and management of the IT equipment then becomes complex because the administrator needs:

- A VPN connection to diagnose an incident (if the admin is outside the network);
- To reassure yourself that the management server on which monitoring is based is physically in service;

A poorly designed architecture could lead to the absence of certain alarms, hence the need to have a solution allowing it to:

- Manage this equipment from a centralized platform;

[1] Teacher and researcher at the Higher Technical Pedagogical Institute of Kinshasa (ISPT-KIN) in the Democratic Republic of Congo

[2] Teacher and researcher at the National Pedagogical University (UPN) in the Democratic Republic of Congo

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

- Manage and administer your network regardless of where it is located;
- And also a solution that will allow it to reduce the cost of WAN links.

II. METHODOLOGY

In this article we invite companies to opt for a cloud solution in order to optimize their network infrastructures. To do this we will start by presenting the current architecture; the most popular, the one that does not use cloud solutions. Its components as well as its mode of operation; while nothing the flaws and limits of this architecture.

Next we will present our optimized cloud-based architecture; its components, its mode of operation and configuration, while placing particular emphasis on the advantages it presents for business network architectures.
To illustrate our points, we will take a practical case of typical configuration of a cloud-based optimization solution, we will configure the Cisco cloud solution step by step; CISCO MERAKI.

And we will finally present the advantages and performances of such a cloud-based architecture compared to a traditional architecture.

❖ *Current Architecture*

We will present the standard architecture diagram commonly deployed in most companies. The reasons are often diverse:

- Lack of Budget;
- Lack of Competent Engineer;
- Lack of Cloud skills;
- Etc…

A. Current Architecture Diagram

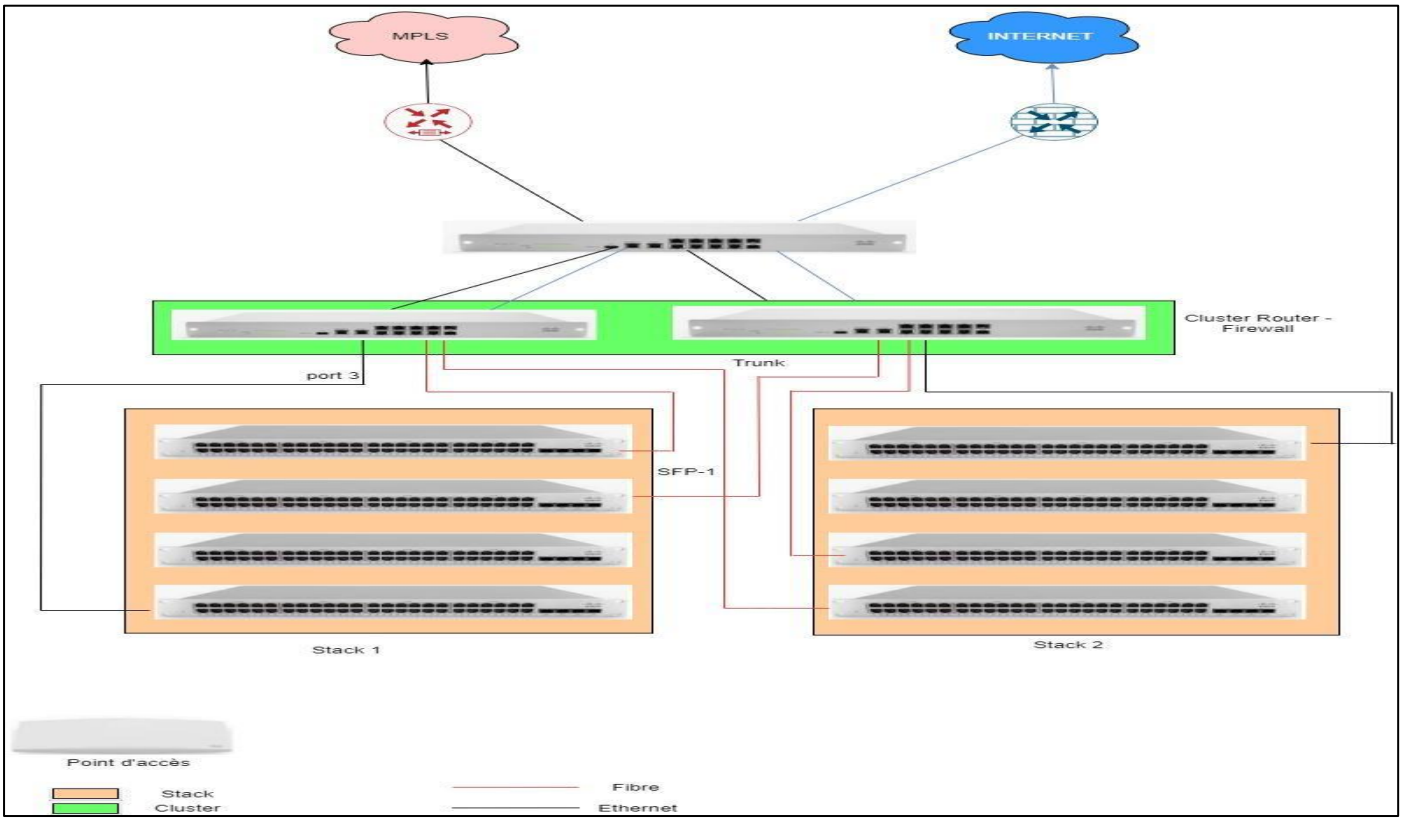

Fig 1 Current Architecture Diagram

B. The Components of the Current Architecture

The elements constituting the current architecture are:

➢ *The MPLS Router*

This is the equipment of the access provider, which aims to provide services such as:

- Extended VPN connections;
- Telephony;
- The Messaging;
- Etc.….

➢ *The Internet Router*

It is also the property of the provider, its role is to provide the Internet service.

➢ *Switch Interconnexion*

These are switches which allow the creation of transit VLANs between the internet network and the supplier equipment.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

➢ *Routers/Firewalls*

They allow the creation of different networks by giving users the possibility of accessing the following services:

- Telephony;
- Messaging;
- Internet ;
- Filtering (in the case of a firewall);
- Etc...

➢ *Access switches*

Access switches are equipment to which computers, access points, printers, telephones, etc. are connected. They can be arranged in a stack.

C. L'OAM (Operation Administration and Maintenance)

Operation and maintenance activities generally consist of the implementation of:

➢ *From A Supervision Server;*

- To configure protocols such as SNMP, Syslog etc. ;
- The presence of a network administrator who will be responsible for monitoring alerts and intervening if necessary.

*D. The Limits of this Architecture***.**

➢ *Redundancy*

- To ensure high availability of a network, it is recommended to use 2 switches to route transit VLANs.
- In the above architecture, the failure of the interco switch will result in the automatic loss of all internet and MPLS services.

➢ *OAM*

- Most alerts are reported to the central server. This is generally installed at the LAN level. This requires the administrator to be on site to ensure maintenance, support and diagnosis in the event of a breakdown.
- It should be noted that it is possible to configure the sending of an alert by email to the administrator but it will always be necessary for the latter to connect to the server and to the equipment concerned in order to be able to carry out the resolution of the incident.

➢ *This therefore implies:*

- Either a physical presence of the administrator on site;
- Or a VPN connection to the company LAN if this is set up (client VPN configuration on the administrator's PC).

III. OUR OPTIMIZATION SOLUTION

In order to optimize the quality of a network, it is essential to ensure that the architecture implemented has been optimally designed.

This point aims to present the architecture deployed in companies where the quality of the network has a strong impact on the company's production.

The section below presents the concept of optimized architecture

❖ *Target Architecture*

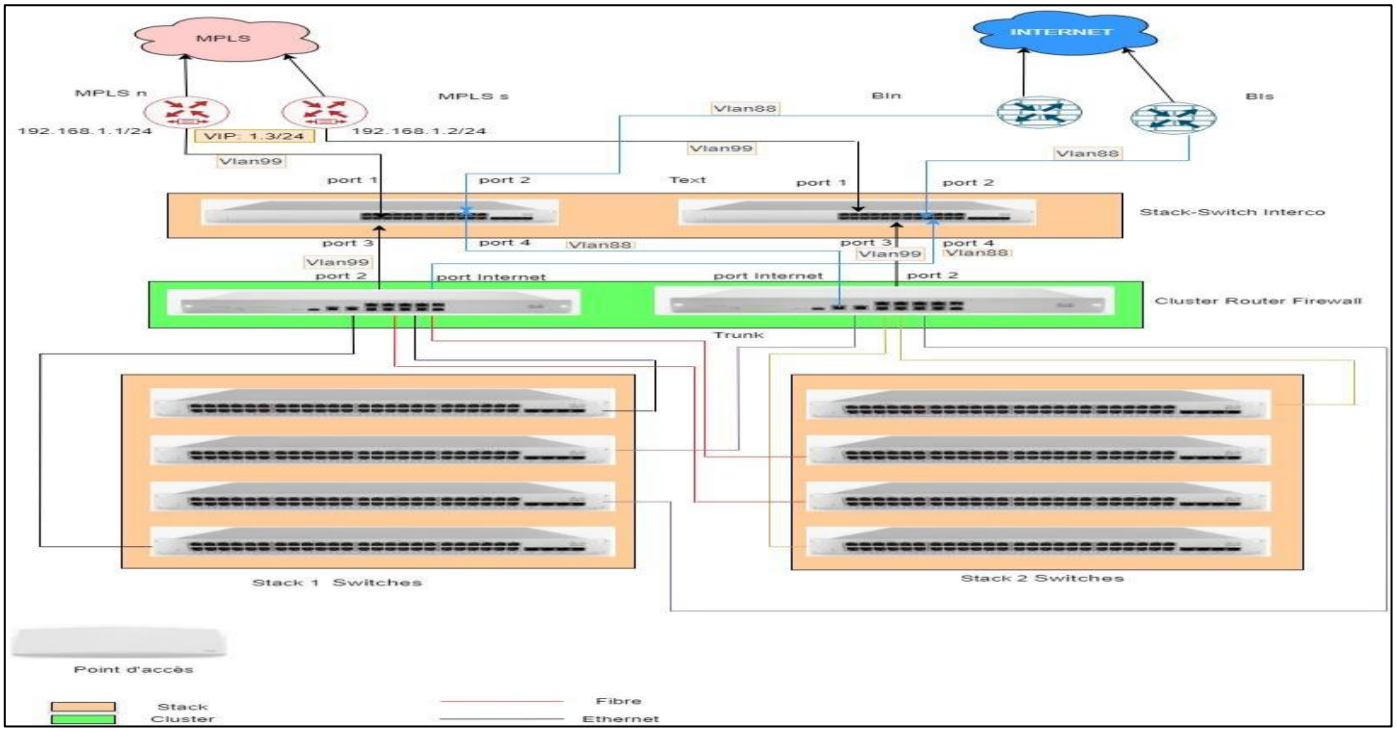

Fig 2 Target Architecture Diagram

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

A. Overview of Components

- The elements making up the target architecture are the same as those used in the existing architecture with the only difference that we will increase the equipment to ensure high availability.

- This involves the use of several protocols such as VRRP, STP, etc.
- In this section we will present the optimization points provided.

B. Redundancy: VRRP Protocol

.

- The objective is to ensure the high availability of MPLS and internet services by implementing the VRRP protocol.
- The VRRP (Virtual Router Redundancy Protocol) protocol aims to create a virtual IP address which will be used by MPLS and Internet equipment.
- Indeed, the active router will use the virtual IP address which will be defined: in our case 192.168.1.3/24 for MPLS routers. If the primary MPLS router fails, the secondary MPLS router will become active and use the same virtual IP address to communicate with the LAN devices.
- The principle is the same for internet routers. It should be noted that the default routes to MPLS and Internet services are the respective virtual IP addresses.

*C. Redundancy: Transit switch***.**

- Setting up a stack of two switches for transit VLANs ensures high availability of services. The connections are distributed as follows:

- The nominal MPLS and nominal Internet Routers will be connected to switch 1 of the stack;
- The backup MPLS and backup Internet routers will be connected to Switch 2 of the stack.
- This ensures continuity of service in the event of failure of a switch member of the transit stack.

D. Redundancy: Cluster Routers.

The Routers will be configured in an Active/Passive cluster, in Uplink they will use a virtual IP address. The VRRP Protocol is used to monitor the status of the Active Router. “VRRP” packets are sent by the active router to the passive router over the LAN link. When the passive router stops receiving VRRP packets from the Active Router, it assumes that the latter is faulty and in turn switches from the Passive state to the Active state.

E. Redundancy: LAN.

- The objective is to ensure the maximum physical connection between Routers and Access Switches in order to maintain continuity of services and above all that this is transparent for users.

- *Physical connections are made as follows:*

- 4 trunk links carried by the routers, 2 of which arriving on each stack and on different switches.
- The objective of this connection is to ensure continuity of services in the event of failure of a switch member of a stack.

- *Spanning Tree Protocol* **:** In order to avoid loops in the network, the Protocol spanning tree is configured on the switch stacks and particularly on all the connection ports between the switches and the routers.

❖ *Target functional Architecture (Cloud solution)*

Today, having a cloud-based network infrastructure offers many cost and performance advantages to businesses that want to maintain high availability of their networks. To do this, you need to turn to a centralized, flexible and agile cloud solution at low cost.

- The cloud solution is a centralized management service that allows administrators to manage all their network equipment via a single, simple and secure platform.

- In this part, we will present a solution that offers a simple and secure centralized management platform for network infrastructures based on the cloud, accessible via the Internet with a dashboard for network management and administration.

- Thanks to this platform, customer network equipment is pre-registered and once connected can load their configurations directly from the cloud without the help of an administrator (ZTD: *zero touch deployment*) which constitutes an advantage in terms of infrastructure deployment.

- The cloud architecture we present provides global visibility and centralized control over wired and Wi-Fi network equipment without the cost and complexity of wireless controllers.

- This solution allows administrators to deploy scalable and secure networks that comply with privacy regulations with complete peace of mind.

Below is an illustration of the functional architecture of the solution.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

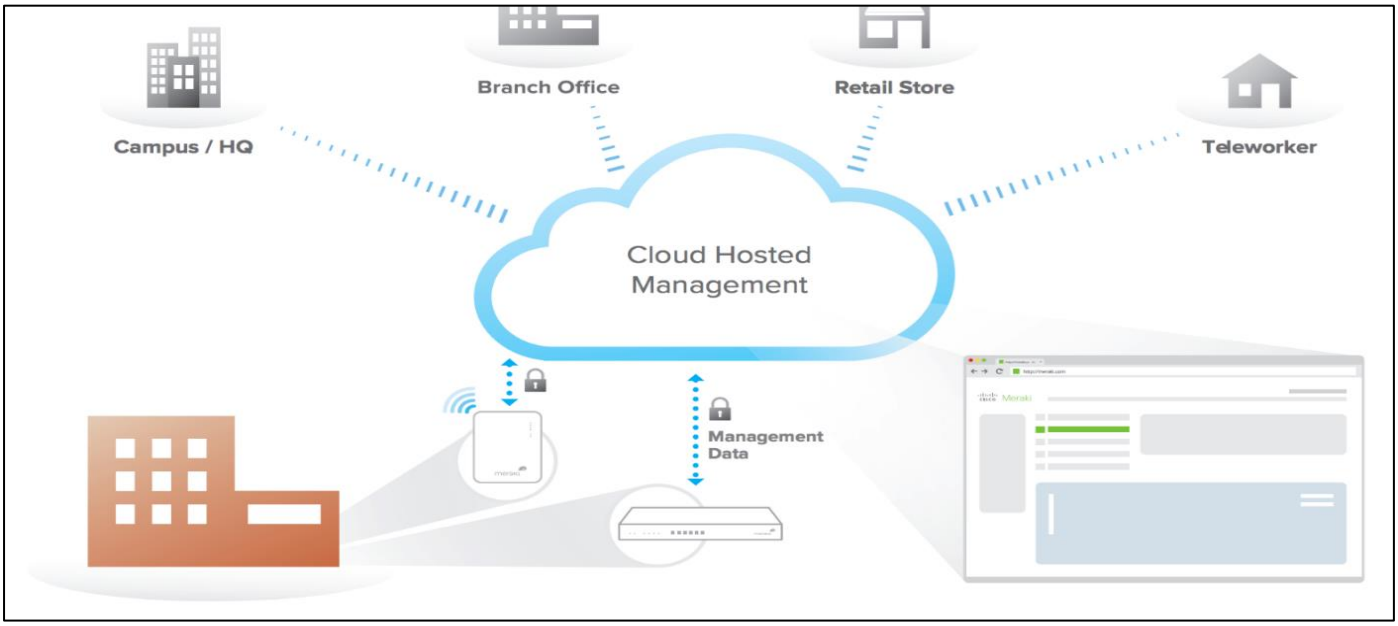

Fig 3 Target Functional Architecture

Administrators have the ability to configure, deploy and monitor their equipment remotely via the dashboard web interface (also called Dashboard or centralized management platform) in the Cloud or via API (Programming Interface). Once an administrator makes a configuration change, the change request is sent directly to the cloud server, then transmitted from the cloud to the affected client devices.

Below is the overview presenting the OAM process of the cloud solution.

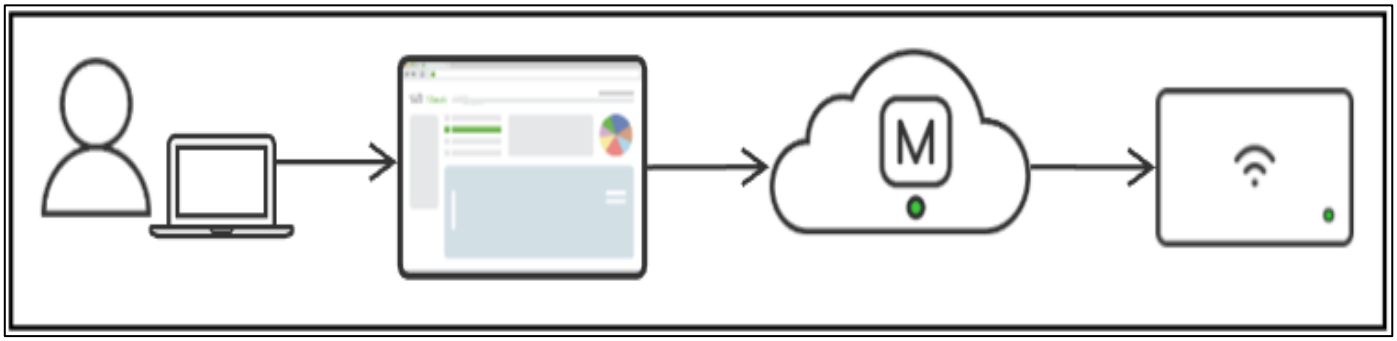

Fig 4 OAM Process of the Cloud Solution

➢ *Logical Operation of the Solution*

This solution uses a logical container for a centrally managed set of customer devices and services. A user account allows the administrator to manage several networks of the same or different entities.

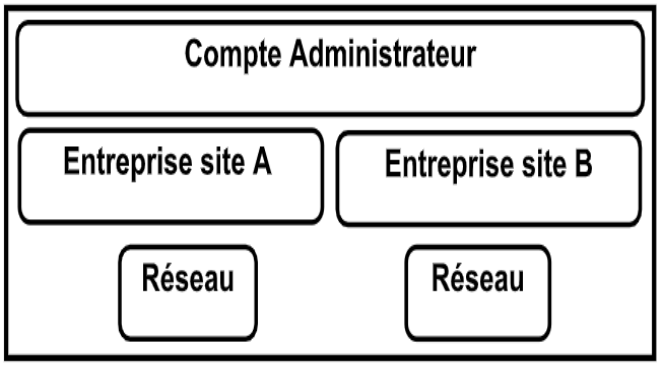

Fig 5 How a User Account Works Cloud

➢ *Data Management*

A separation of management flows and user flows is ensured by the control plane in a cloud solution.

Management data (e.g. configuration, statistics, monitoring, etc.) flows over network equipment (router, wireless access points, switches and firewalls) to the cloud via a secure Internet connection.

In order to ensure the security and confidentiality of information, management data passes over a secure Internet link and customer data does not go to the cloud.

- *User Data Management*

The data presented by a company's dashboard is hosted in data centers geographically close to it in order to reduce access time and ensure confidentiality in compliance with the SLA (Service Level Agreement) . All network-related management data, end-user traffic analysis data and location

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

analysis data are stored exclusively in these data centers in the region in which the customer is located

User data (web browsing, internal applications, etc.) does not go to the cloud, but travels directly to its destinations via the LAN or through the WAN network

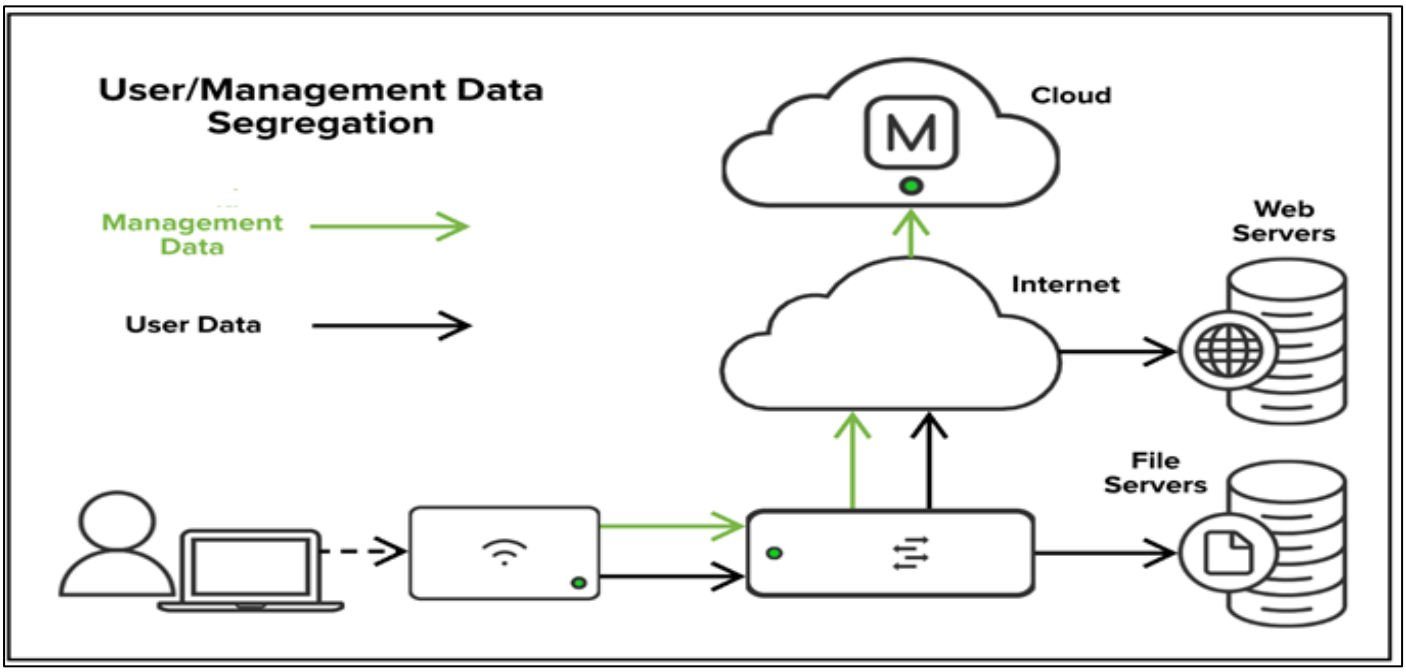

Fig 6 Management And User Data Management

➢ *Communication Between Devices and the Cloud*

Communication between the equipment, the dashboard in the cloud (management data) and the servers (user data) is ensured by an engine supporting the RPC (Remote Procedure Call) protocol.

RPC is a network protocol allowing procedure calls to be made on remote equipment using an application server.

This protocol is used in the client-server model to ensure communication between the client, the server and any intermediaries.

The network equipment acts as a server because the communication is initiated by the dashboard in the cloud. Since the cloud infrastructure is the initiator, configurations can be executed in the cloud before the devices are actually online, or even physically deployed, by pre-registering the devices on the platform.

The figure below presents the concept of data exchange.

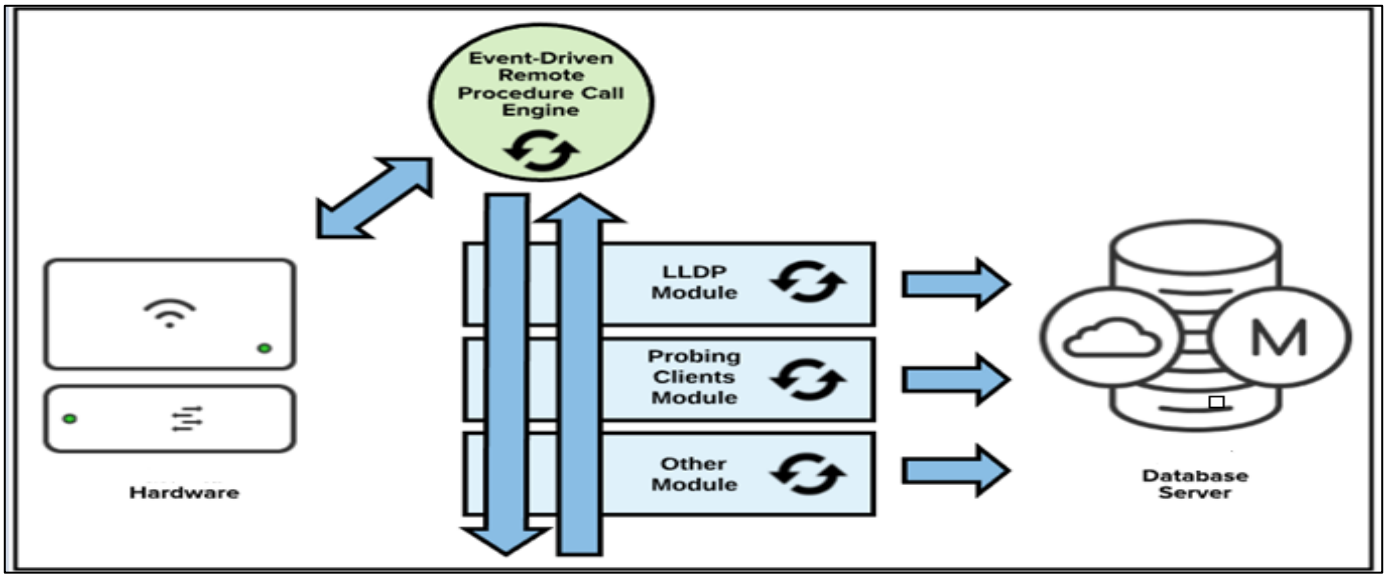

Fig 7 Concept of Data Exchange

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

➢ *Communication Process Between Equipment and Cloud Servers*

Even when offline, a network device will attempt to connect to the cloud until it gains connectivity.

Once online, it automatically receives the most recent configuration settings from the cloud.

In the event of configuration modifications by the administrator, the equipment receives and updates these modifications automatically.

Changes are sent to the device in seconds. However, a large amount of modification may take longer to reach their target devices. If no configuration changes are made by the administrator, the device continues to periodically check for updates to its configuration on its own.

Equipment that operates on the network will communicate its usage and network analytics to the cloud.

In the event of a connection break between network equipment and the cloud, the LAN will continue to function correctly with its existing configurations.

➢ *Configuration Containers*

Containers store equipment configurations in the platform. When the configuration of a device is modified by the administrator via the dashboard or the API, the container updates it then transmits it to the device with which it is associated, via a secure connection. The container also updates the cloud with its configuration change for failover and high availability.

Below is an illustrative diagram of how a container works.

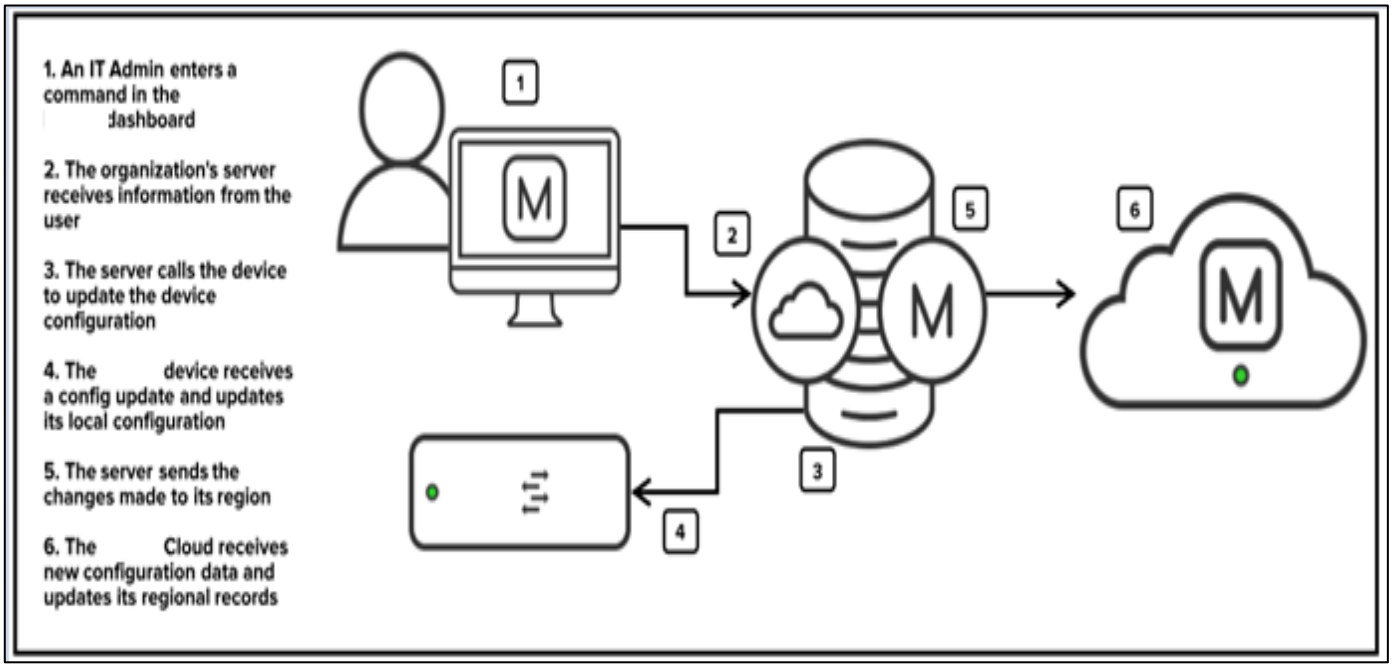

Fig 8 Container Configuration

➢ *Uses of APIs*

The APIs allow you to control the solution in a programmable way by making possible actions that may not be possible with the dashboard or require more granular control.

The use of APIs provides flexibility in configuring equipment at an advanced level, allowing more efficient and more powerful solutions to be implemented.

Using APIs, administrators can automate deployments, monitor their networks and create additional solutions on the dashboard.

The figure below presents the concept of management through the use of APIs

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

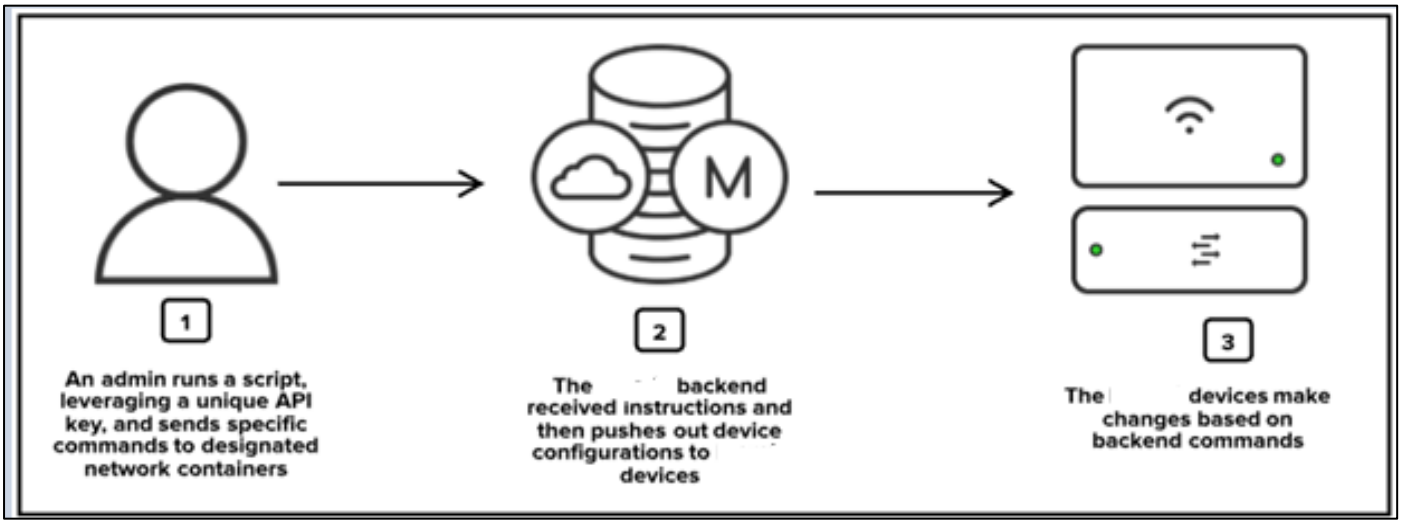

Fig 9 Using APIs

➢ *Security Aspect*

All data transported to and from equipment and servers is routed through a secure communications tunnel. Communication data is encrypted in transit through this tunnel. All customer management (dashboard/API) connections to the cloud have secure TLS encryption for all application traffic.

Transport Layer Security (**TLS**) is a protocols securing exchanges by Internet. It works in a mode client-server and ensures the following elements:

- L'authentication of the customer;
- L'authentication from the server;
- The confidentiality data exchanged;
- L'integrity data exchanged;

For network equipment to communicate with the cloud, they use a tunnel encrypted with AES256 while management data is in transit. In the tunnel itself, the system leverages HTTPS and protocol buffers for a secure and efficient solution.

➢ *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) is a algorithm of symmetric encryption. AES-256 – the key version of AES 256-bit – is the encryption algorithm used by the VPN.

The figure below presents the concept of secure communication.

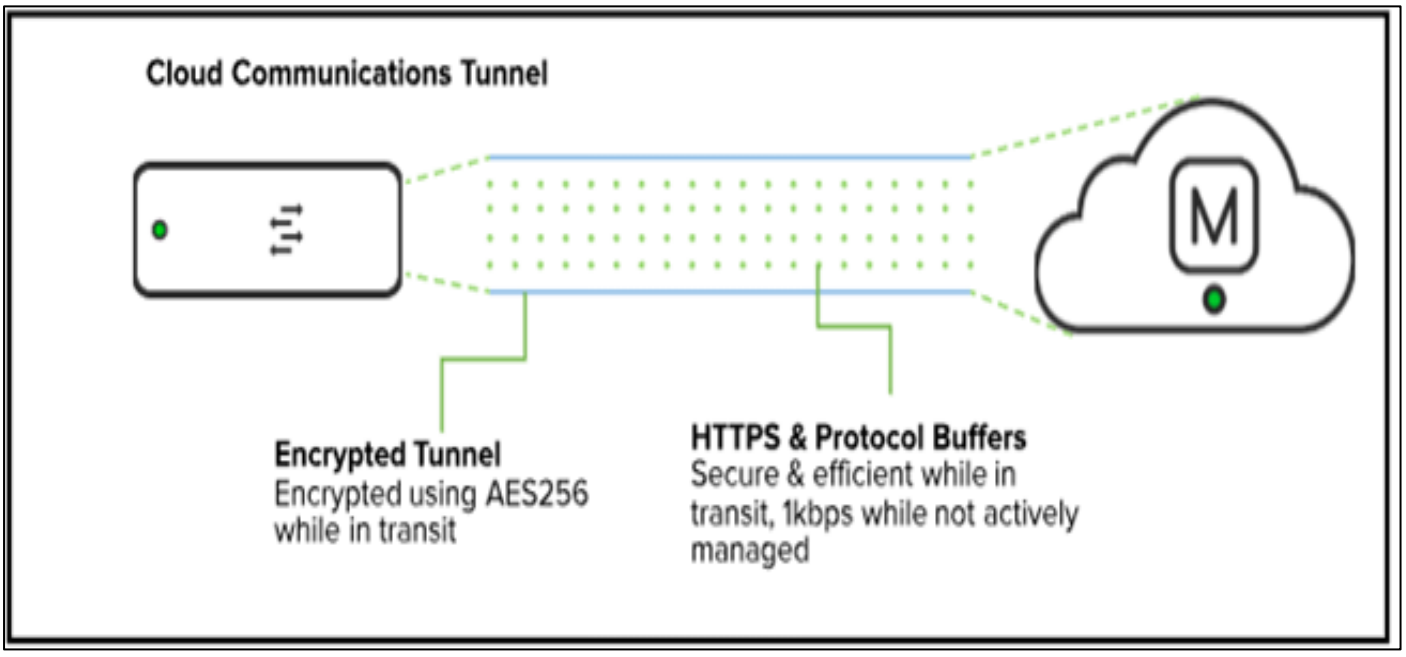

Fig 10 Secure Communication Concept

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

IV. PRACTICAL CASE OF DEPLOYMENT OF THE SOLUTION

In this part we will present a practical case of deploying a centralized Cloud-based optimization solution. As part of this project, we will use the solution from the manufacturer Cisco: *CISCO Meraki.*

This equipment offers the possibility of being administered, configured and monitored via a centralized platform in the Cloud called Dashboard.

❖ *Deployment Principle*

This section presents the steps for deploying the solution in a LAN (company network) environment.

➢ *Creation of the Dashboard*

The Dashboard is presented in the form of a web interface allowing you to supervise and administer network equipment. An organization in the Dashboard represents a customer or a company which has several networks and which contain devices such as access points, switches or MXs.

Within an organization, multiple networks can be created containing equipment from different sites and locations; multiple organizations can be linked together under a single connection using the same username and password when connecting. creating a new account/organization.

In this part we will explain the method of creating a new account/organization in the Dashboard, the steps are given as follows:

Go to http://dashboard.meraki.com/. Recommended browsers are Google Chrome and Mozilla Firefox.

Click on ***Create an account***.

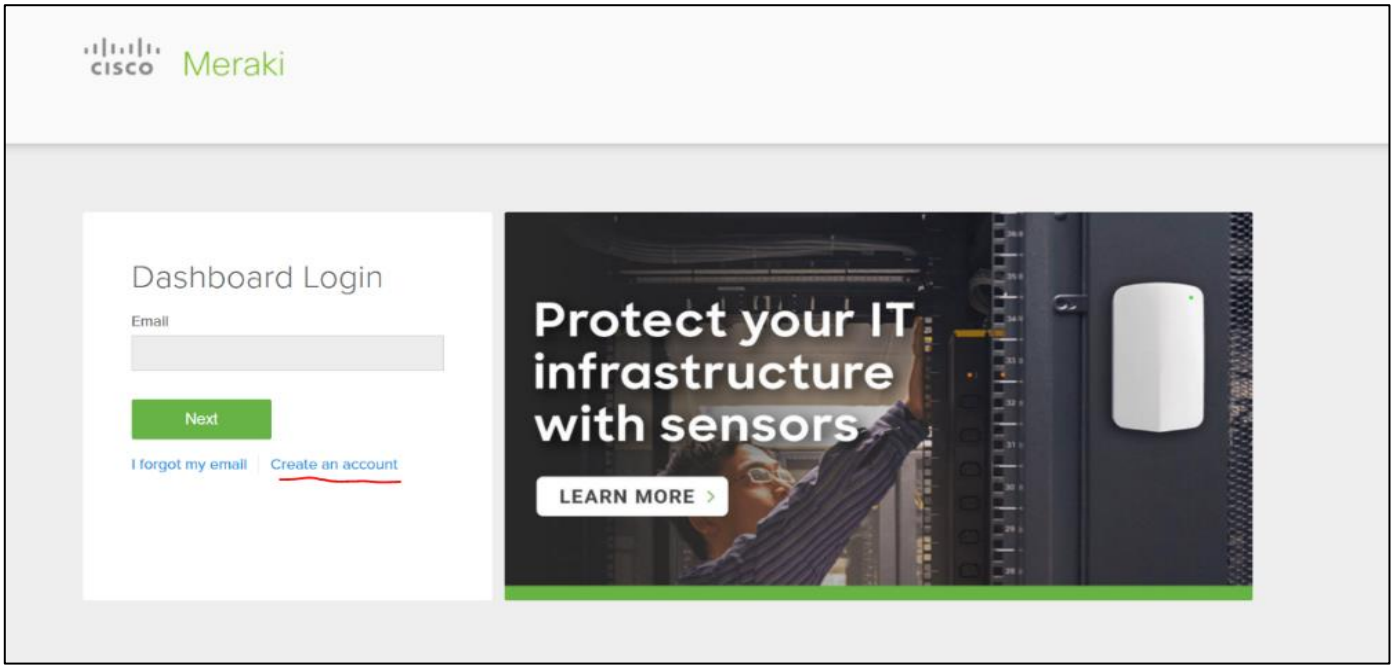

Fig 11 User Account Creation Interface

Select the region in which your new organization is located. This will determine where your company's LAN is hosted

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

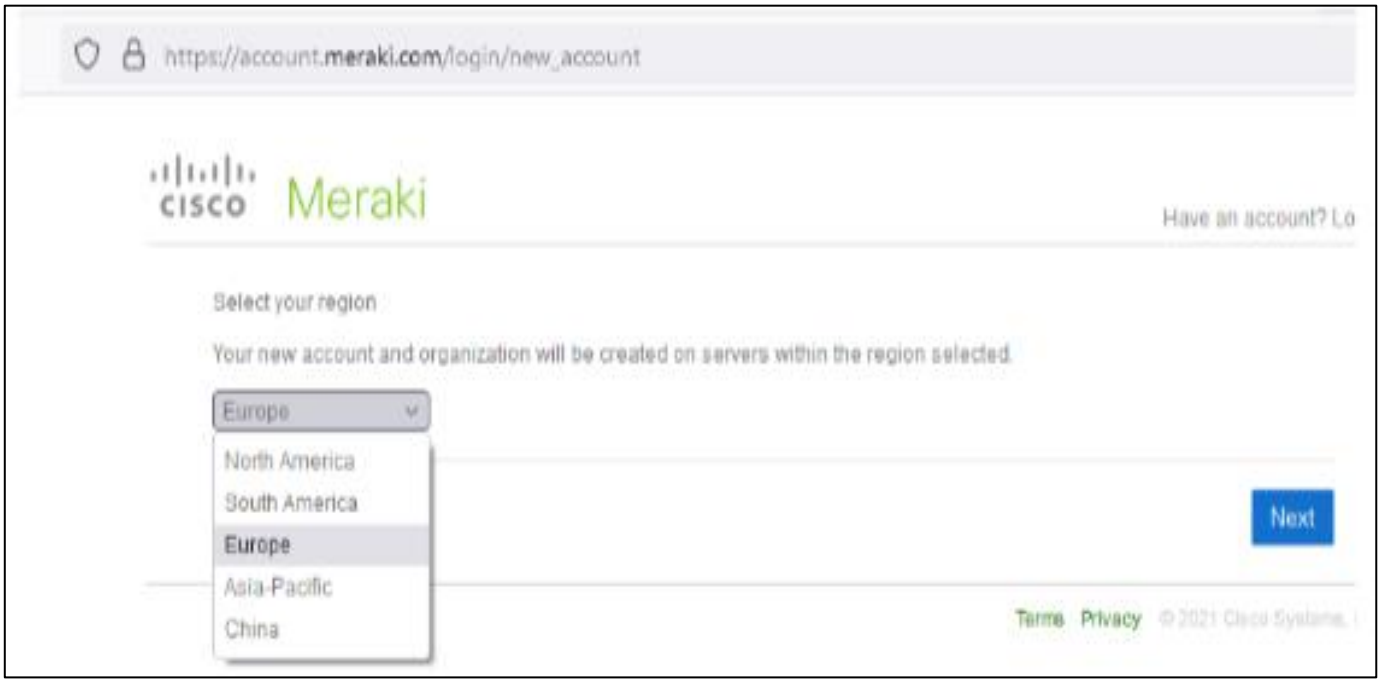

Fig 12 Selection of the geographic area of the company

Complete the fields presented below with your organization's information.

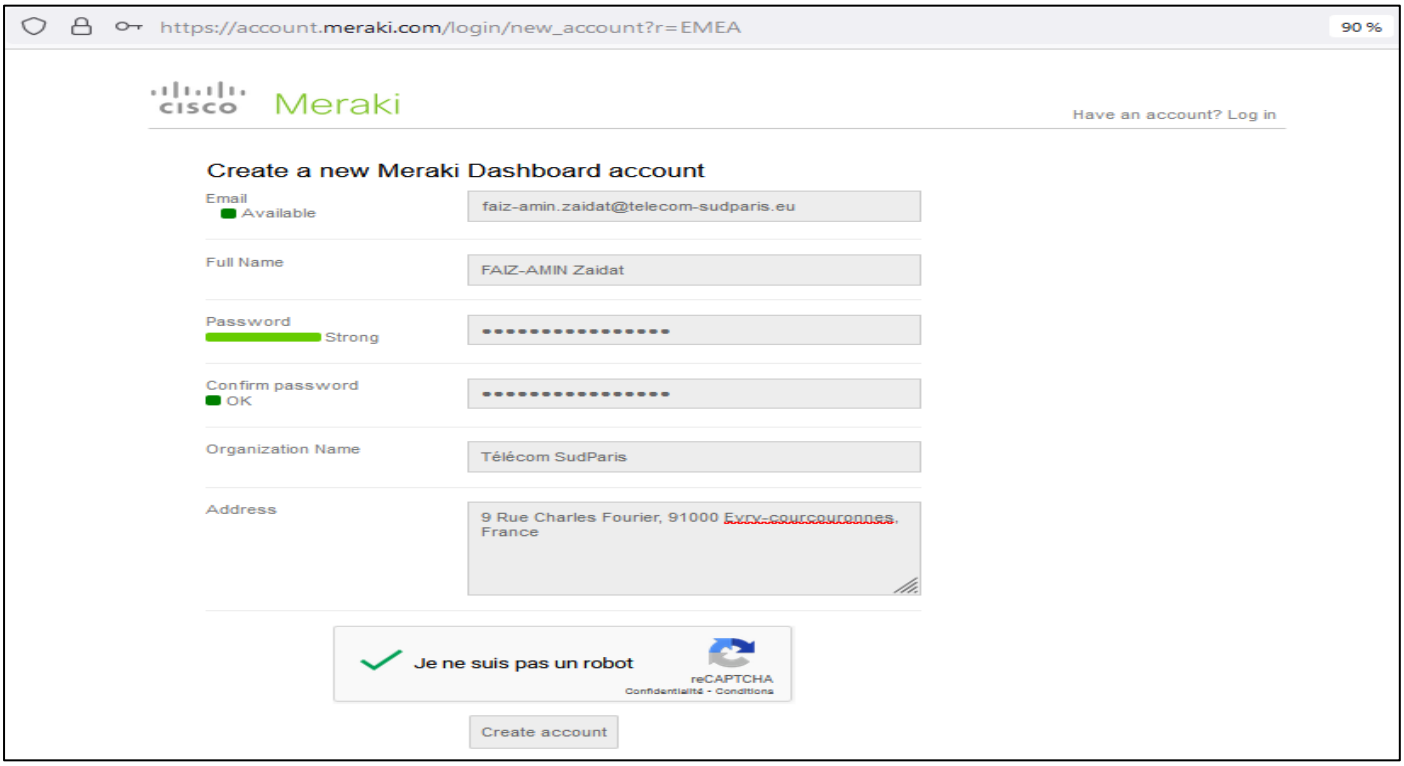

Fig 13 Creating a Company

➢ *User Account*

Click on the button *"Create an account"* once all required information is correctly entered.

➢ *Equipment Registration*

- Adding equipment to the Dashboard can be done by two methods:
- Addition of serial numbers and licenses for each equipment;
- Importation of the PO (purchase order) which presents the equipment purchase number.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

- Below are the screenshots showing the steps to follow for adding network equipment:

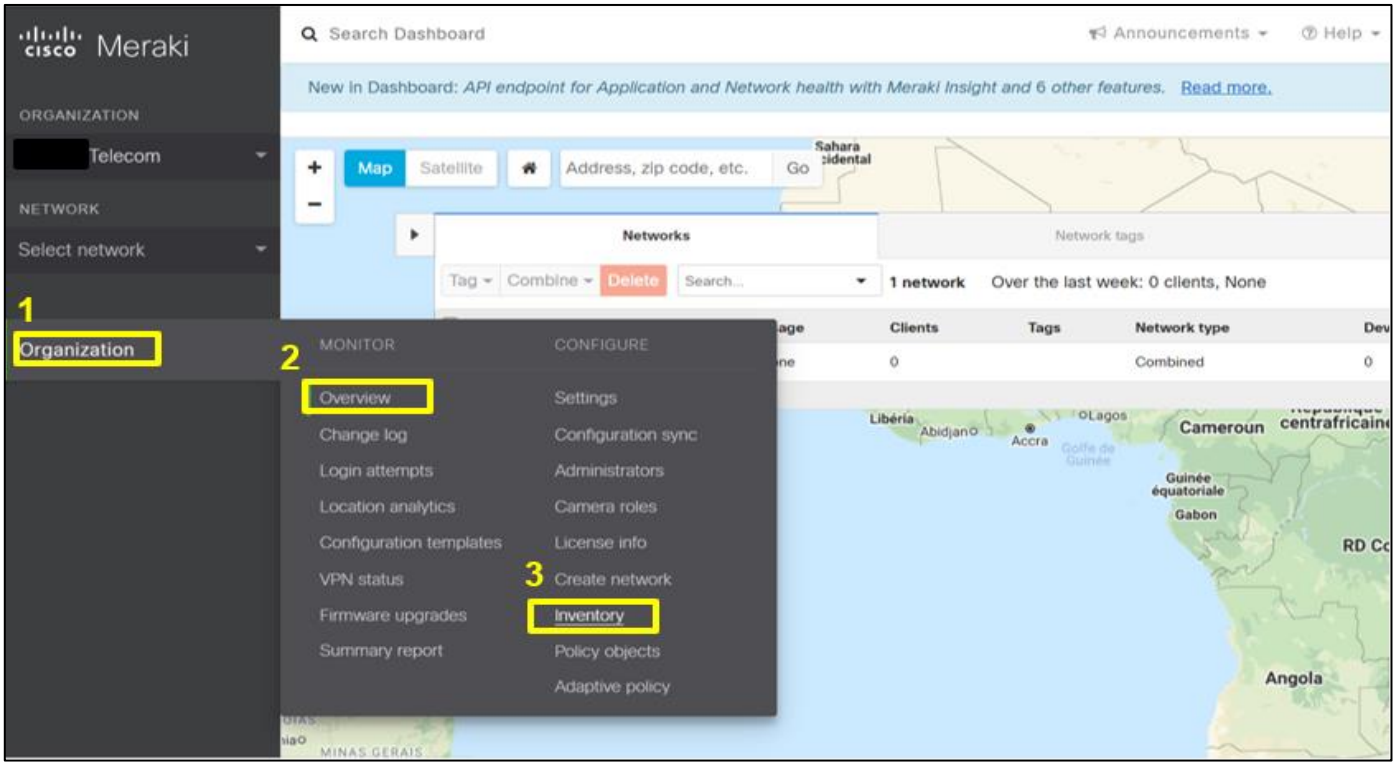

Fig 14 Adding Network Equipment

Then we put the serial/PO numbers on the reserved part as shown below

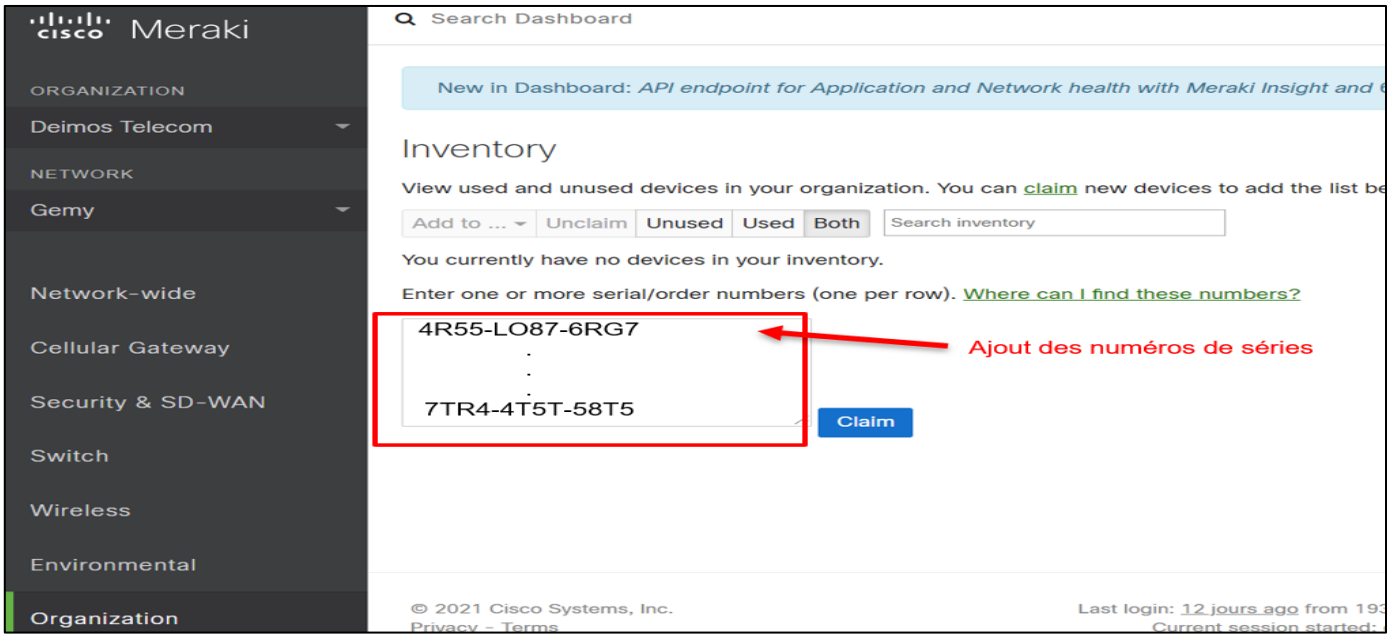

Fig 15 Adding the Serial Number

➢ *Configurations Des Switche*

In this part we list the steps for configuring the switches used in our company's network.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

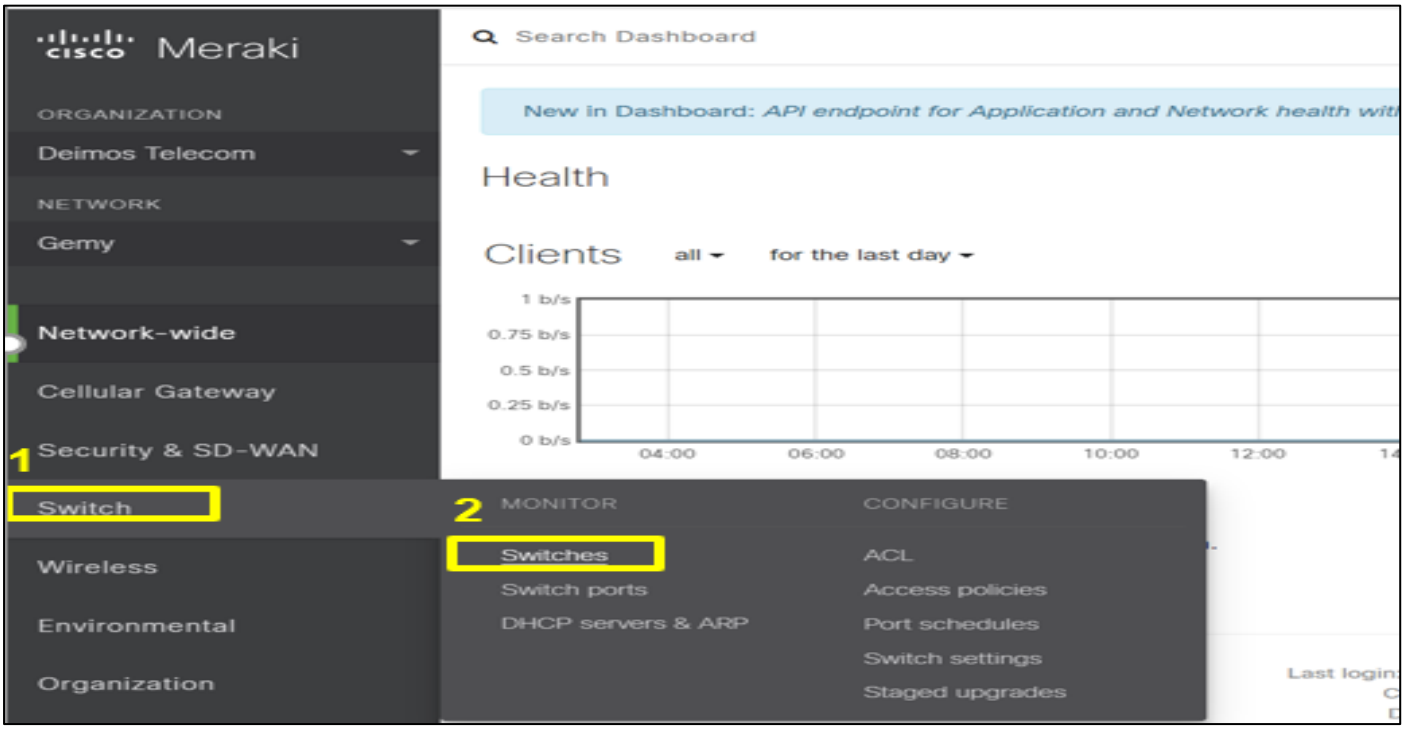

Fig 16 Switch Configuration

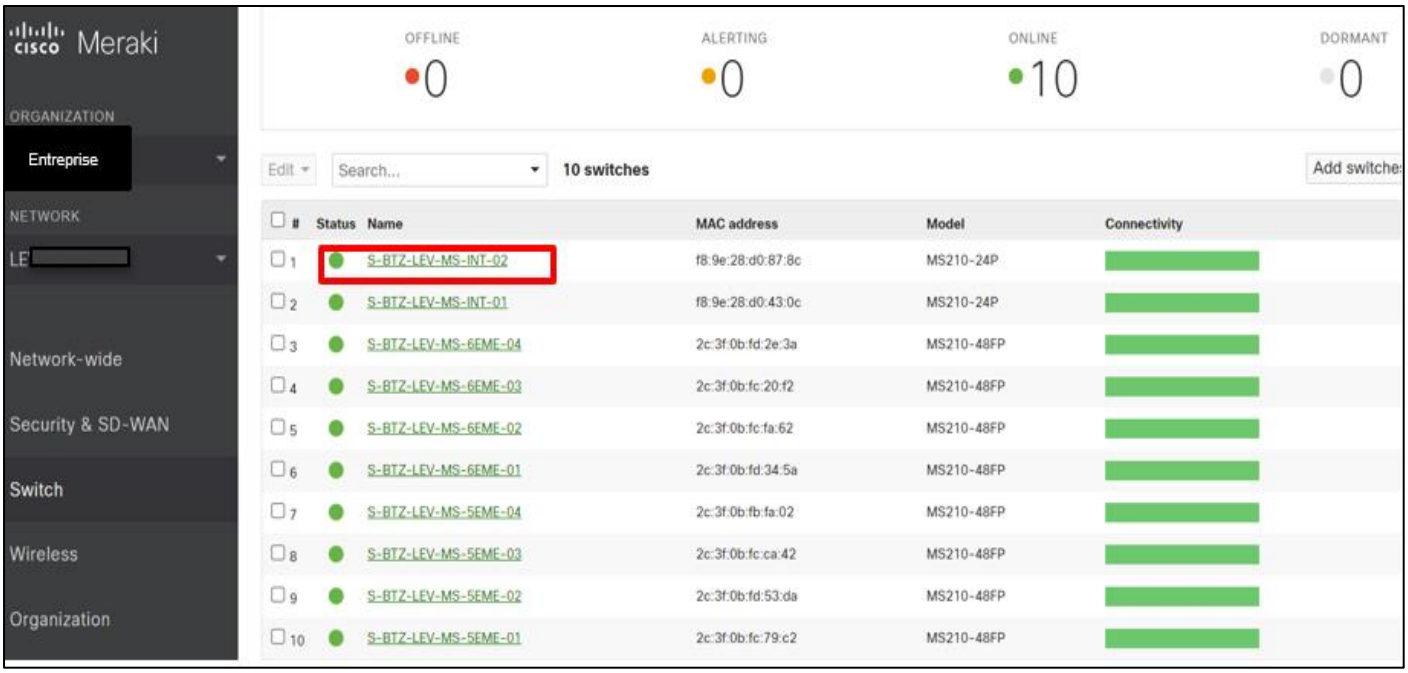

Fig 17 Identifying a Switch Using the Serial Number

By clicking on the serial number we open the window of the switch in question in order to make the configuration.

We proceed in the same way for the creation of VLANs on the switches in the " *Switch ports* » as shown below an illustration.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

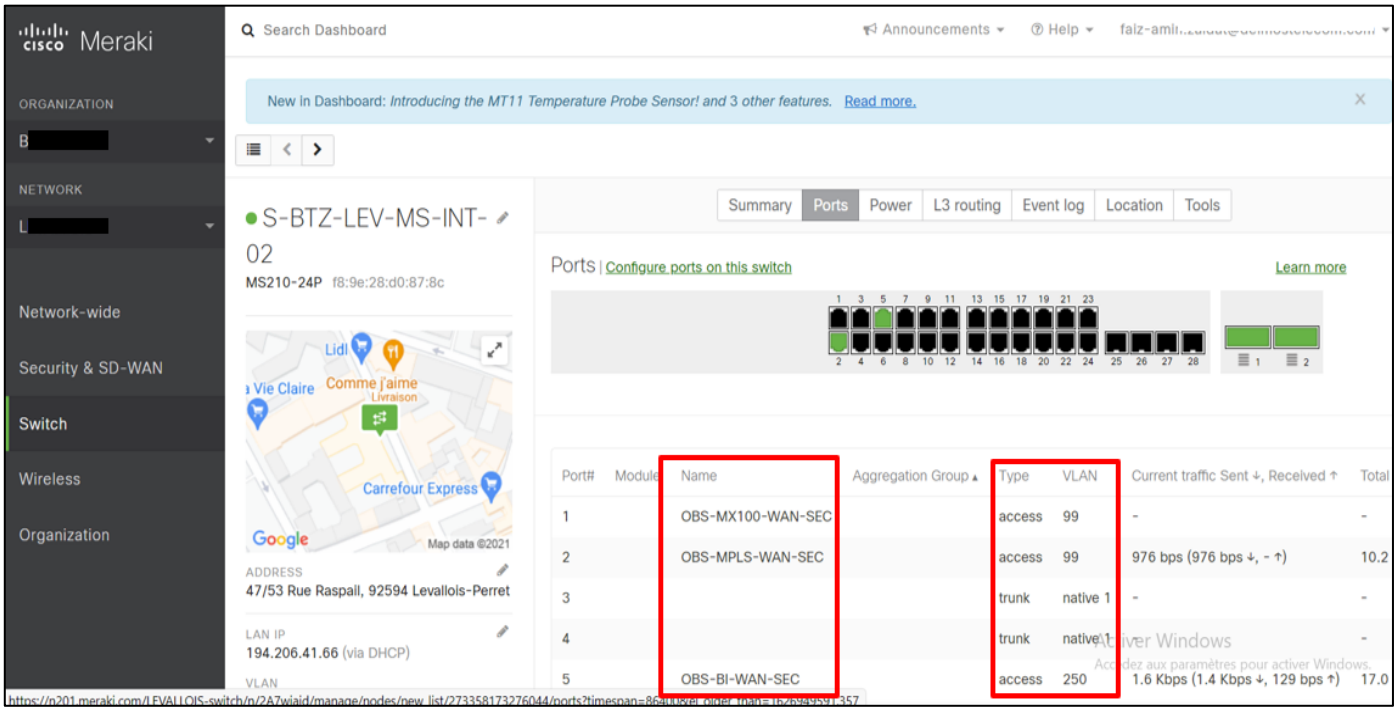

Fig 18 Verifying the Configuration

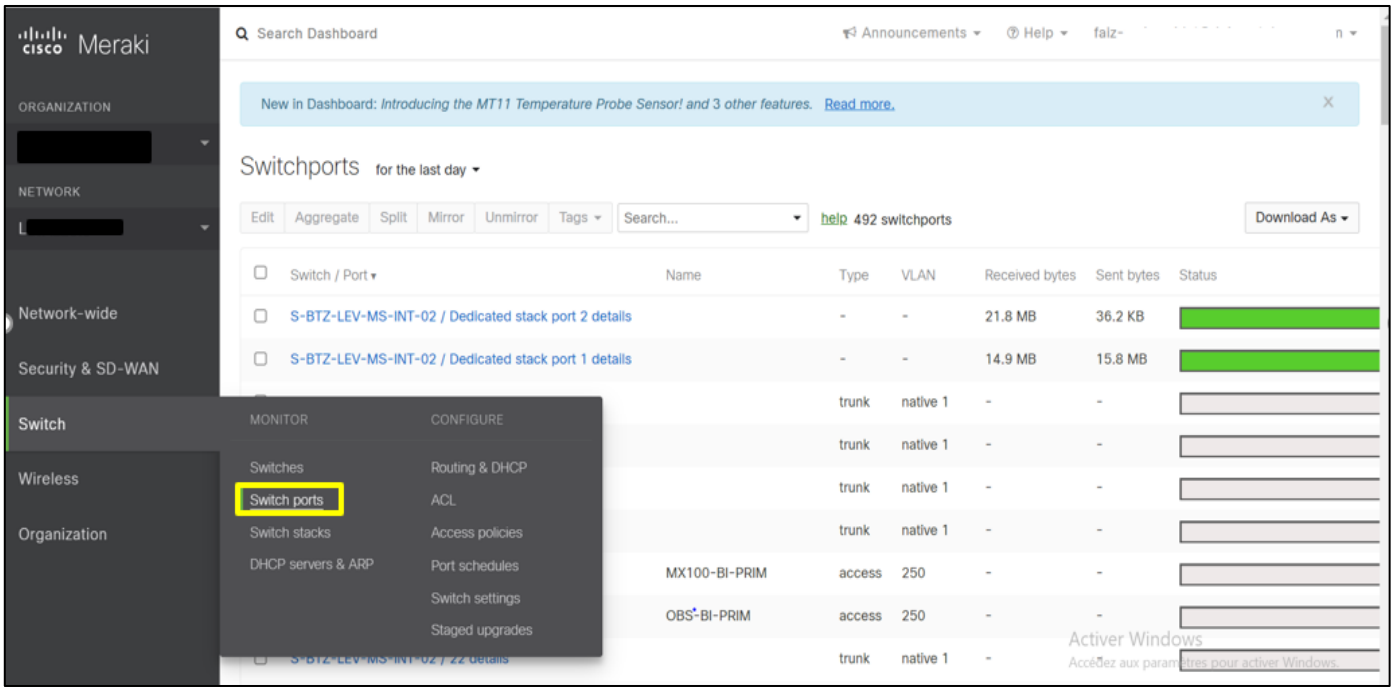

Fig 19 Creation of VLANs

Then we click on the name of the switch concerned to open the configuration window which includes the ports, port statuses, VLANs, RSTP configuration, etc...

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

The figure below shows an overview of the configuration of a switch port.

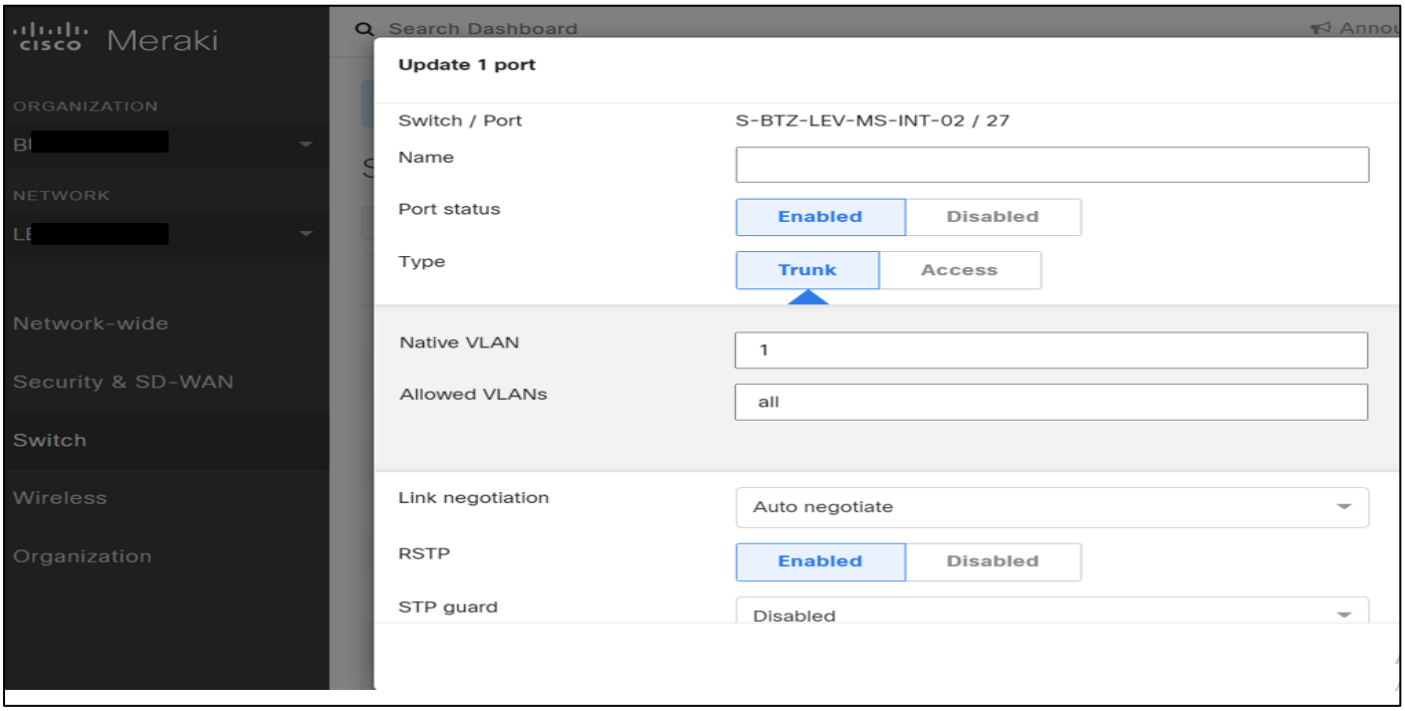

Fig 20 Configuring a Switch Port

Regarding the creation of stack switches that we often adopt for LAN architectures in order to have more ports for users, printers, servers and access points and to ensure optimal redundancy, the creation procedure and the same on the Switch part → Switch stack.

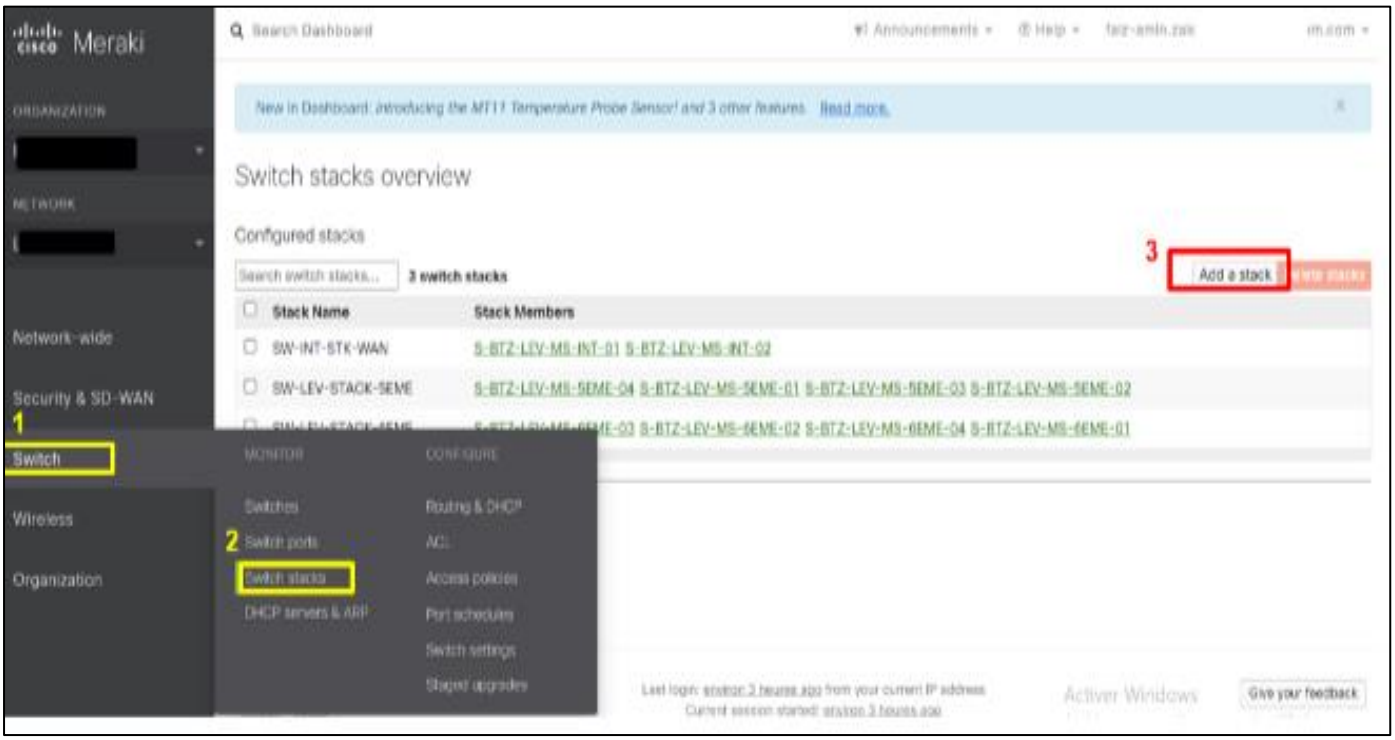

Fig 21 Creation of switches in stack

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

➢ *Configuring Routers*

This section defines how traffic will be routed at the MX between MPLS and INTERNET links. We will present the configuration steps.

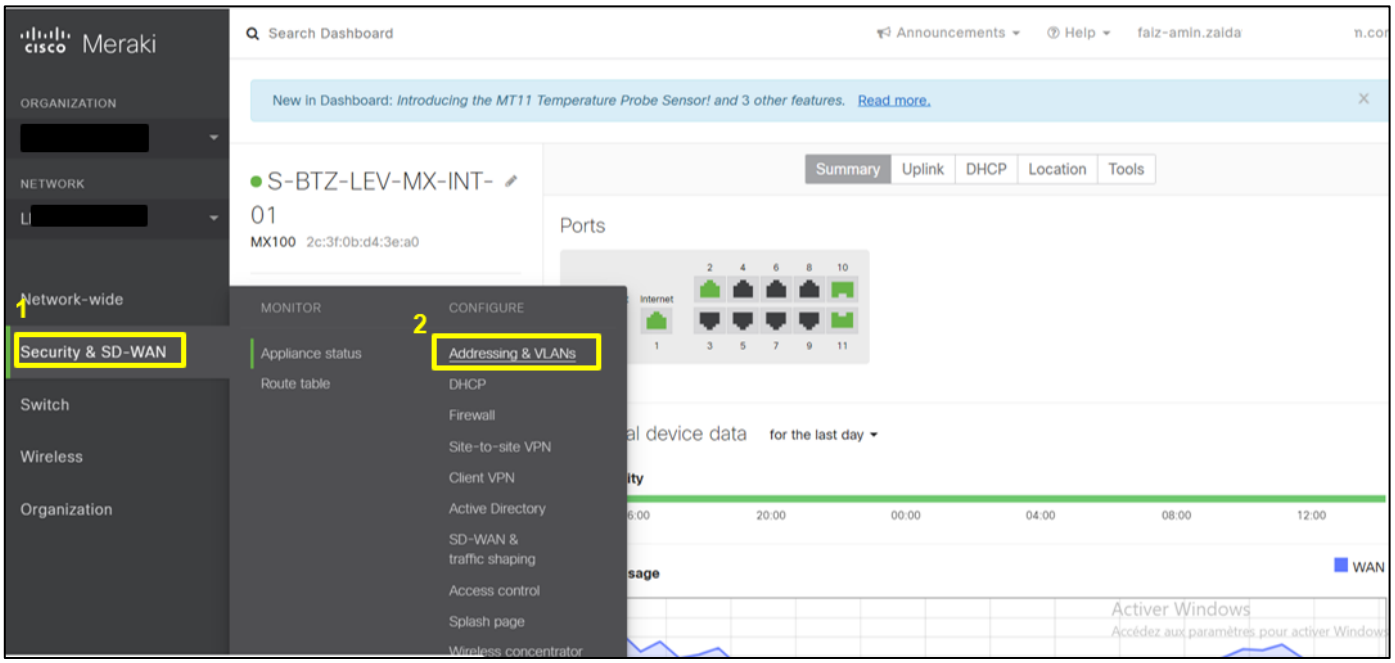

Fig 22 Routing Configuration

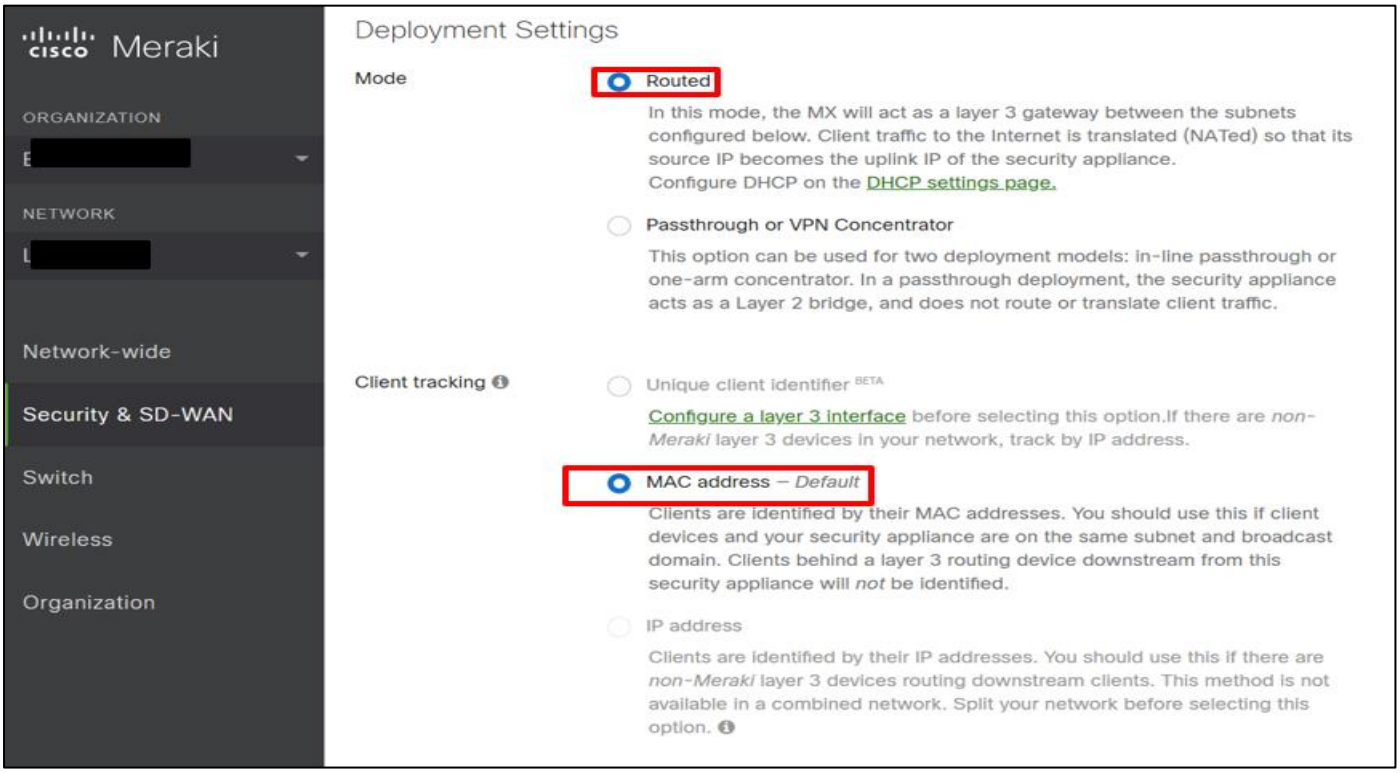

Fig 23 Selecting the Routing Option

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

Below is an illustration of network interface configuration.

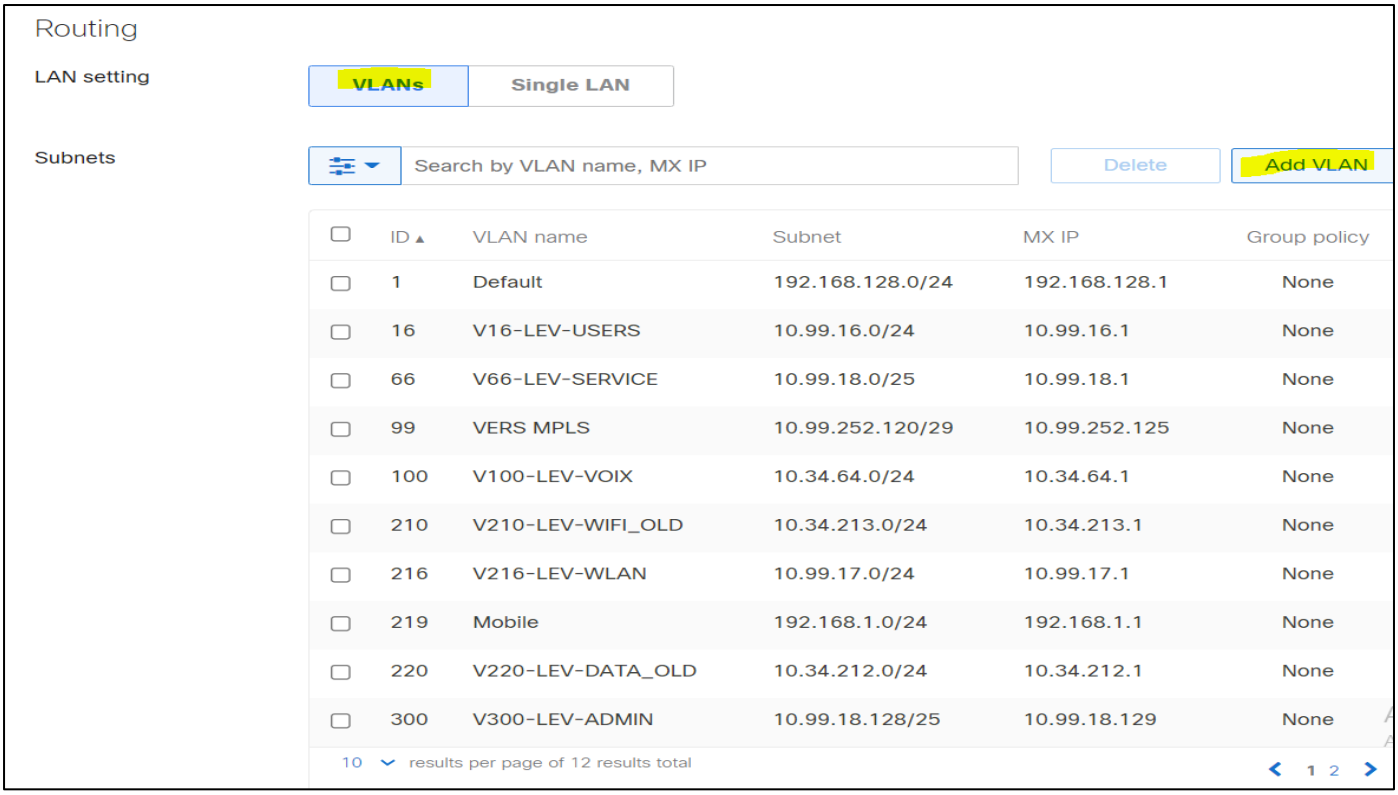

Fig 24 Configuration of Network Interfaces

The figure below shows a configuration applied to the different ports of the MX.

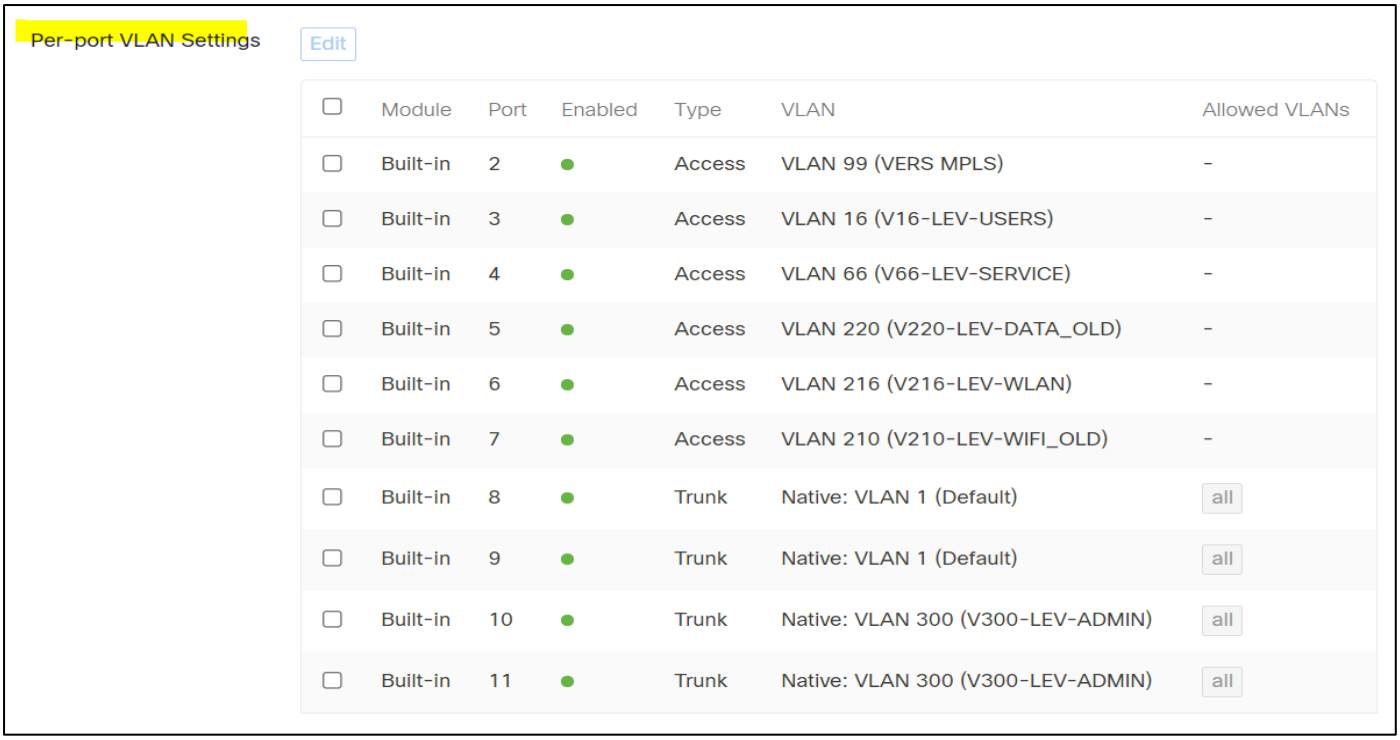

Fig 25 Configuration on MX Interfaces

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

The figure below shows a configuration of static routes.

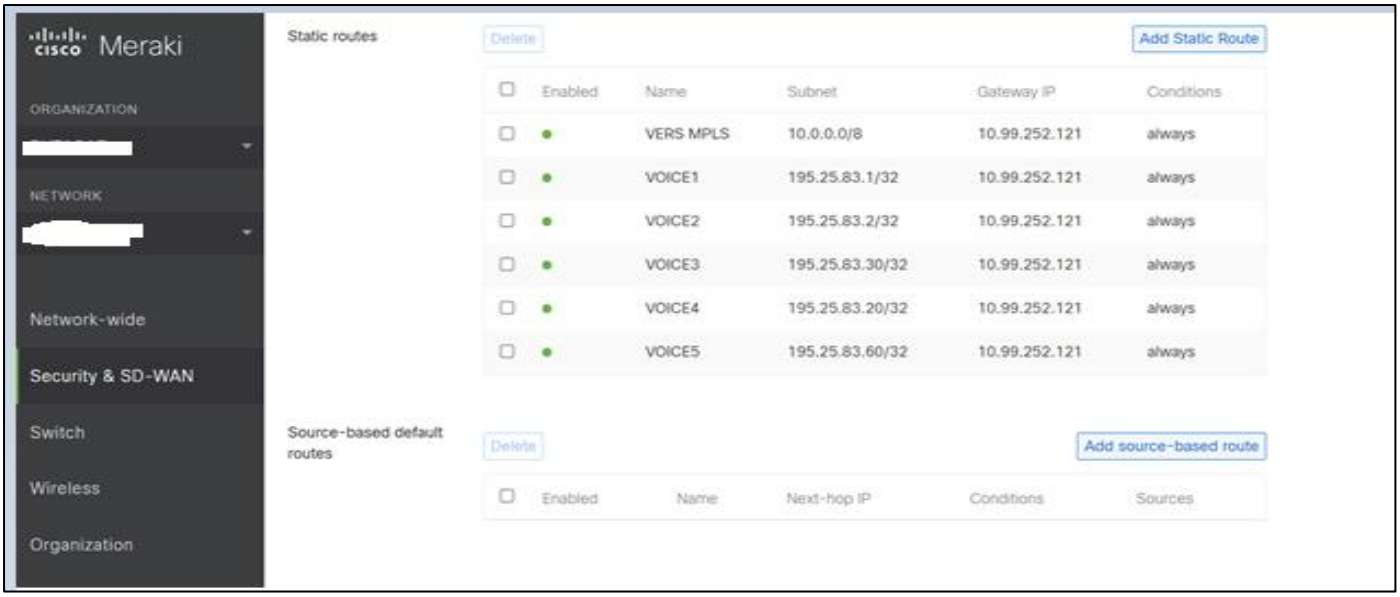

Fig 26 Configuring Static Routes

For creating firewall rules

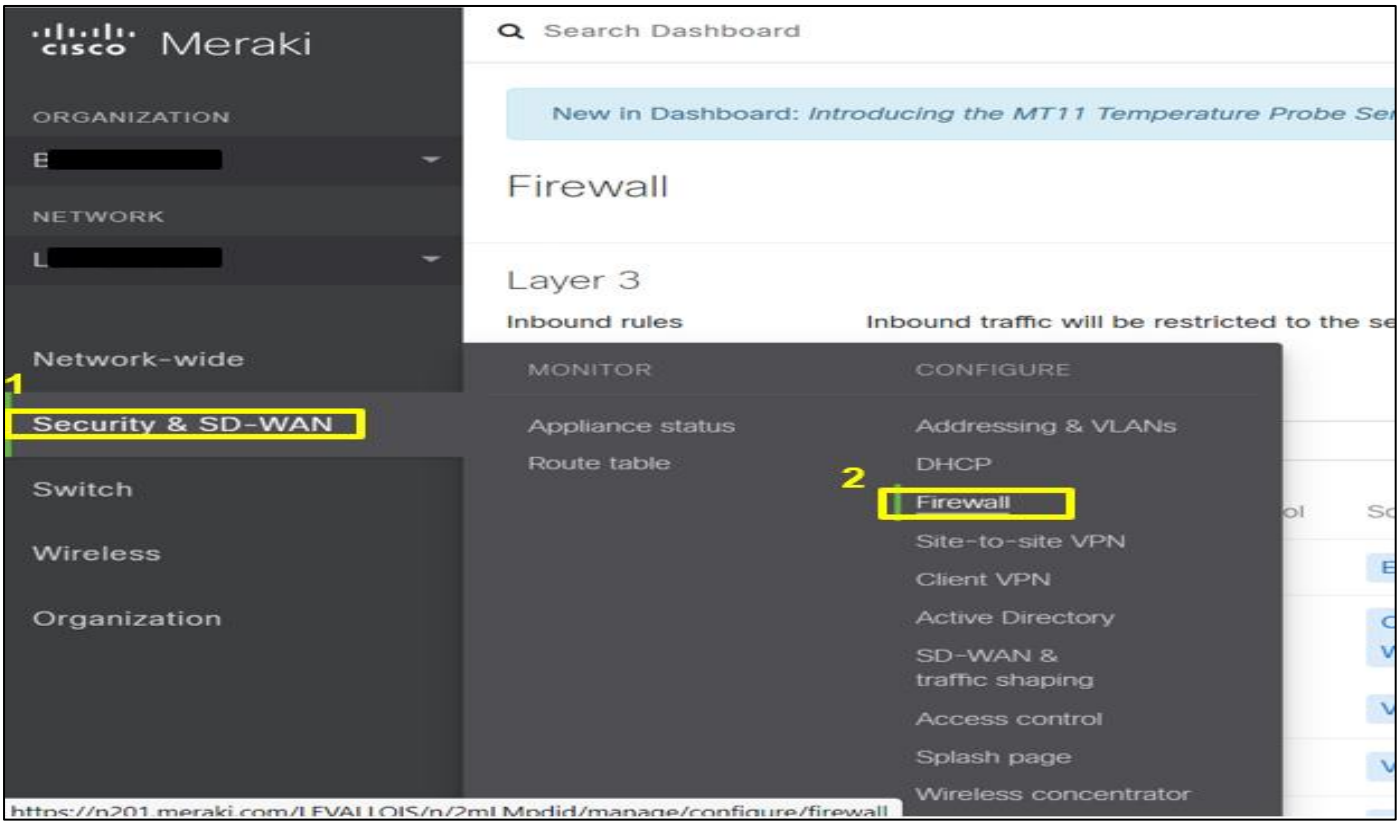

Fig 27 Creating Firewall Rules

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

Configuring access points

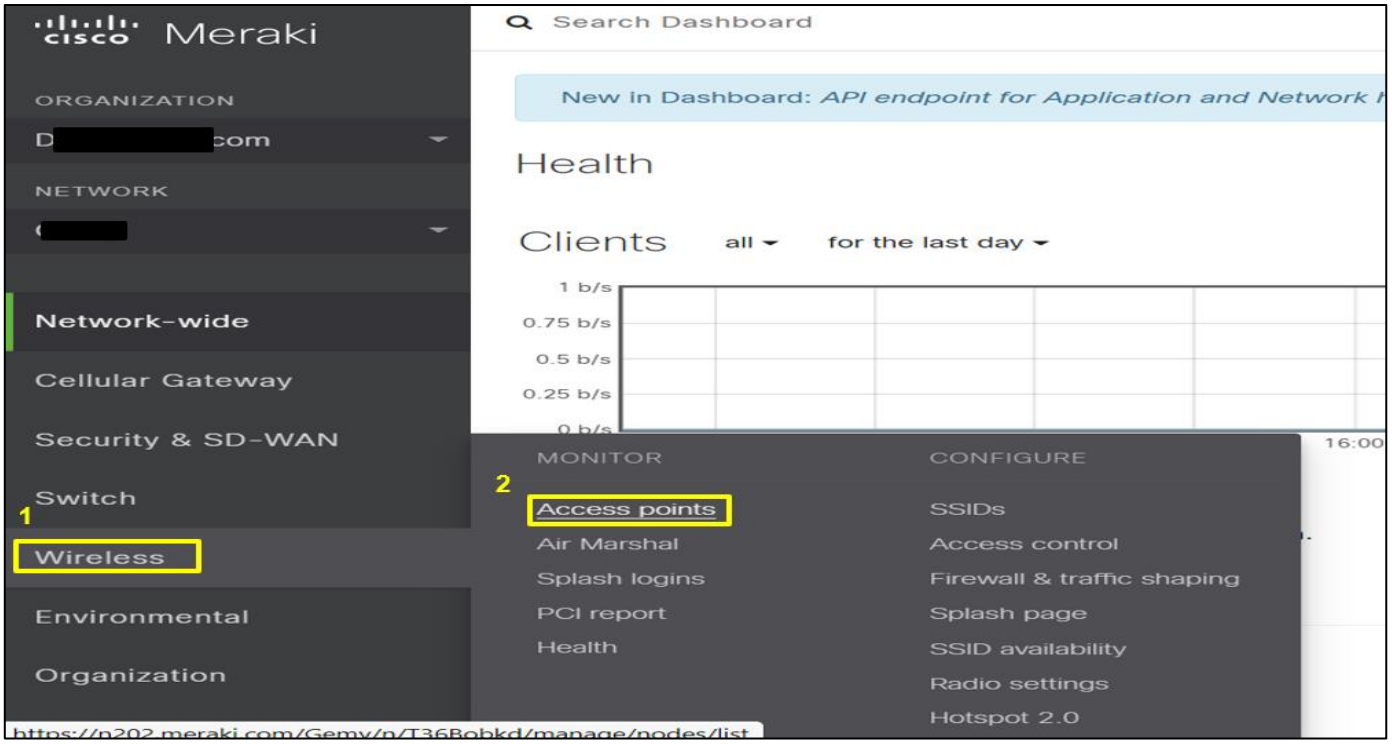

Fig 28 Selecting the Wireless Access Point

To add an Access point on the Dashboard using its serial number already saved in the part mentioned at the top:

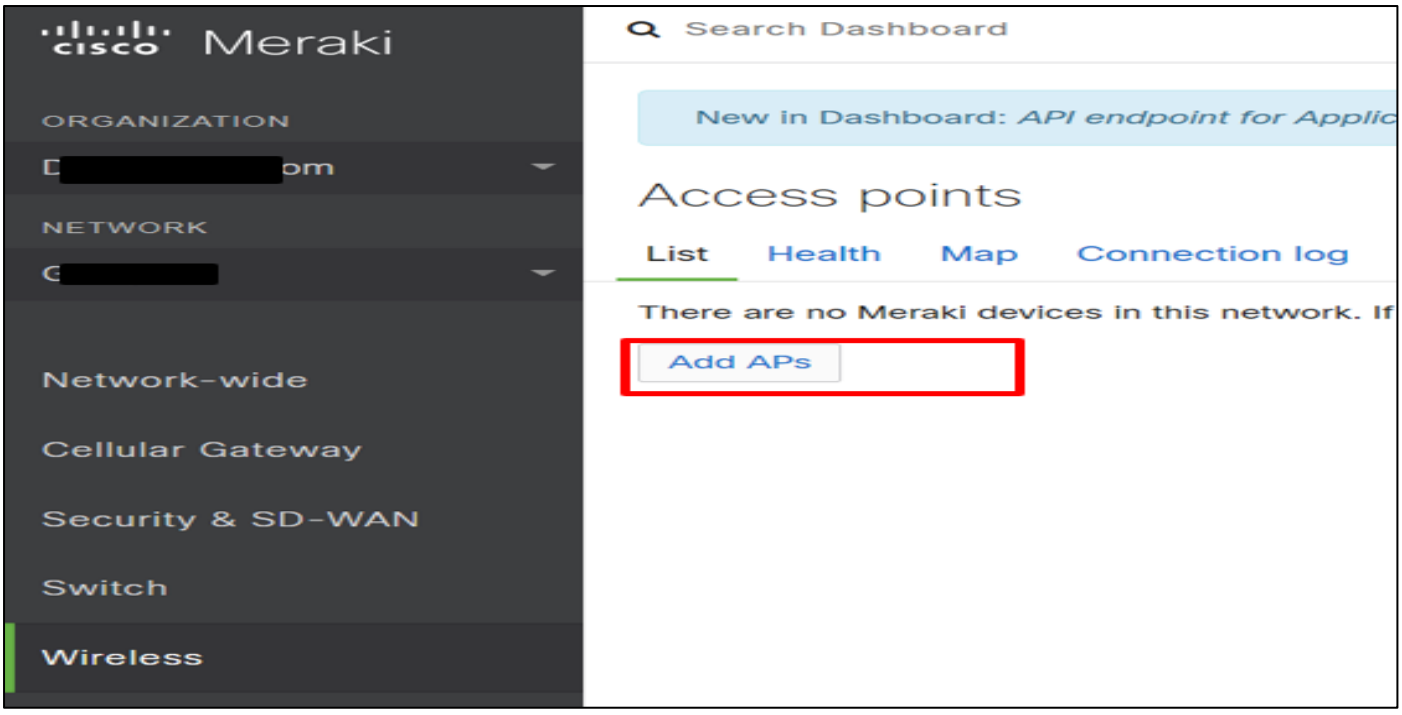

Fig 29 Adding the Wireless Access Point

Below is the screenshot showing the creation of the SSIDs.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

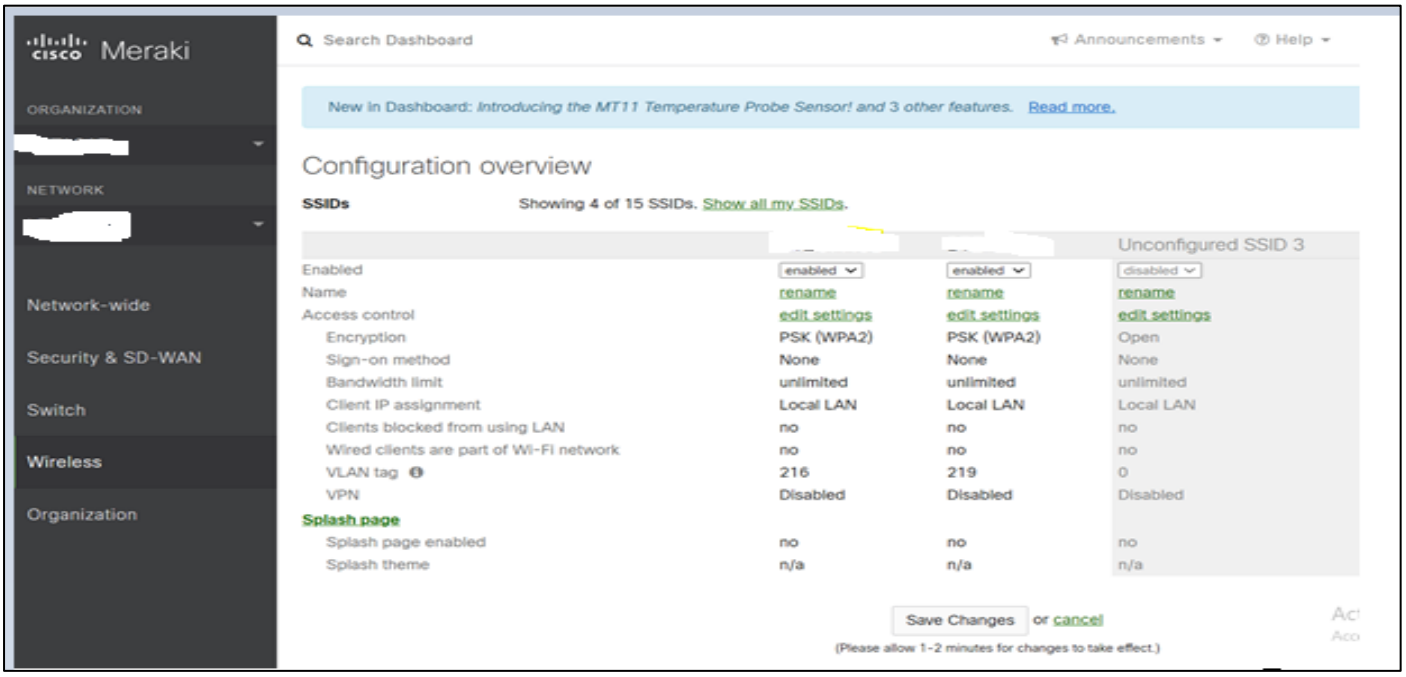

Fig 30 Configuration du SSID

Below is an overview of how an access point works.

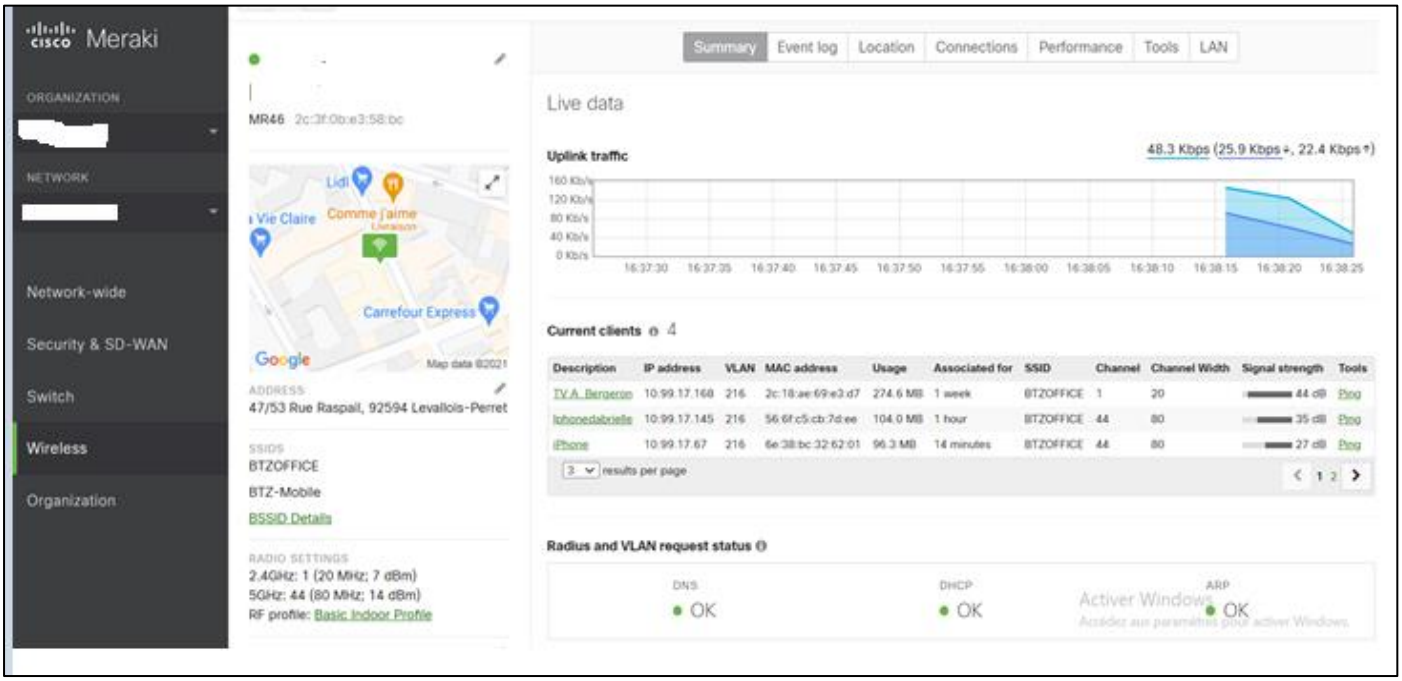

Fig 31 Access point operation

V. CONCLUSION

We have just presented a cloud-based LAN network optimization solution, showing the different advantages it offers in terms of infrastructure availability, flexibility and security.

We were interested in the manufacturer CISCO Meraki which offers equipment designed to operate on the cloud and has data centers located around the world, which allows local data confidentiality with high availability for sovereignty in sensitive countries and regions. and high-speed connections to facilitate reliable cloud management communication.

These data centers hold certifications such as ISO27001. Additionally, all data centers undergo daily penetration testing by an independent third party. Other key data center features include:

- Service level of 99.99% uptime;
- 24/7 automatic fault detection;
- Real-time replication of data between Datacenters;

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14792223

- Possibility of Management and configuration regardless of where the administrator is located;

➢ « *Zero Touch deployement* »:

All configurations are done upstream on the centralized cloud platform using the serial number of the equipment. The equipment recovers its configuration once installed on site.

Faced with the increase in user traffic and the need for quality of service, this solution is best suited for current companies that wish to maintain infrastructures in operational condition.

REFERENCES

➢ *Works*

[1]. Equinix. (n.d.). *Network optimization thanks to the network performance hub*.

[2]. Safieddine, I. (2018, January). *Optimization of cloud computing infrastructures in green data centers*. MATTER.

➢ *Course Notes*

[3]. Baudron, J. (2021, May). *High-speed infrastructure, network sizing* (MS.RS). Télécom SudParis.

[4]. Maudoux, J. F. (2020–2021). *Evolution of the supervision of Mobile and convergent networks* (Specialized Master). Télécom SudParis.

[5]. Moungla, H. (2020, October). *RLE Algorithms and protocols* (MS.RS). Télécom SudParis.

[6]. Swiniarski, G. (2020–2021). *Project management course: Lot 1 Cloud Computing* (Télécom SudParis, MS RS).

➢ *Webography*

[7]. https://dwn.vn/datacenter-architecture-en accessed on December 15, 2024

[8]. https://medium.com/@dixitra20/cisco-meraki-interview-questions-and-answers-ce1edbeb687c accessed on December 15, 2024

[9]. https://bouchecousue.com/blog/management-out-of-band/ accessed on November 22, 2024

[10]. https://www.linkedin.com/posts/santanu-de-5b3567283_what-is-cisco-meraki-cisco-meraki-meraki-activity-7108473487945535488-r6YY accessed November 8, 2024

[11]. http://soup01.com/en/2022/06/08/meraki001_basic-setup-2/ accessed December 2, 2024