Escuela Politécnica Superior de Linares

Master in Telecommunications Engineering

Universidad de Jaén

Escuela Politécnica Superior
de Linares

DESIGN AND IMPLEMENTATION OF A COMPANY'S COMMUNICATIONS INFRASTRUCTURE

Alumno: **Luisa María Parra Cabrera**

Tutor: Prof. D. José Ángel Fernández Prieto
Tutor: Prof. D. Joaquín Cañada Bago

Depto.: Ingeniería de Telecomunicación

March, 2021

INDEX

INDEX OF FIGURES

TABLE INDEX

1 ABSTRACT

In the final master's work to be developed, a network infrastructure design and implementation will be executed following the principles of the Cisco hierarchical network.

In the design and implementation of this hierarchical network, the quality of service parameters necessary for the applications of the company treated in this project will be taken into account.

Also, security will be applied to the network using security technologies, such as Vlan, port-based security, ARP security protocols, DHCP, etc., as well as a perimeter security system.

In the design and implementation part, Internet access and communication between various locations will also be taken into account, as well as remote access from outside these, through IPsec VPN.

2 INTRODUCTION

All the companies that exist today, need a communication with the outside both voice, to make calls and data, to make use of the large number of applications and services that are available.

To host all these communications that are needed within the company, it is necessary to use a network infrastructure that is scalable, flexible and secure, since more and more, companies keep sensitive data from it on their servers.

In order to achieve a network architecture with these principles, the basic principles of the Cisco hierarchical network will be used, as we will see in later sections.

In companies, just as the wired network is very important for all equipment to communicate with each other and with the outside world, the wireless network is becoming increasingly important as it allows its users to have mobility within the headquarters.

Speaking of mobility, and with the times, the use of teleworking is more and more common, so the remote and secure access of workers to the services and applications of the company must be taken into account, without them being physically at headquarters.

All these points to take into account will be developed in a more extensive way in the subsequent sections.

3 OBJECTIVES

The objectives of this end of master project are the following:

- Design the hierarchical local network.
- Study the quality of service (QoS) necessary for standard applications.
- Study security technologies in LAN networks, such as: VLAN, Radius, port-based security, security in protocols such as ARP, DHCP, etc.
- Design Internet access and access from other locations.
- Design DMZ zone, public and private servers zone.
- Design peripheral security system.
- Implement a part of the network, using the equipment available in the department.
- Verify access to the different areas of the network and that rejects unwanted access, both external and internal.
- Measure network performance.

4 ESTATE OF THE ART

Currently, communications in a company are increasingly important, due to the large number of applications and services that are used in daily work and internal company processes.

Due to this large amount of data transmission, it is necessary to have a scalable and flexible local area infrastructure (LAN), thus managing to separate the different services and meet their quality needs.

In addition to the usability of the network, another point to take into account is its security. Thecampus of a company, shows many services abroad that must be adequately protected.

In any company, another part of the internal network that is very necessary and that takes on a fundamental role, is the Wireless Fidelity (WiFi) network, which makes possible the mobility of workers within the building, defining collaborative spaces, meeting rooms, guests to the company ... Getting not only dependent on the workstations of fixed LAN sockets.

Regarding the subject of voice communications, at present TDM switchboards with primary accesses or through the Integrated Services Digital Network (ISDN) are no longer used, but the trend is to switch to IP switchboards, in which the logic of the calls are made through a software application that can be located virtually on the company's servers and the telephones are IP devices that connect to the building's LAN network, carrying out voice over IP communications.

Considering all the previous points, it can be concluded that every company needs a LAN network adequate to the current times, implementing the separation of services in a virtual local area network (VLAN) to provide the quality of service that need each of these services, in addition to providing security and communication with the outside of the company. Considering all this, the company's network architecture will be designed, following the principles of hierarchical networks established by Cisco.

4.1 Hierarchical Network Desing Principles

For the dimension of the network architecture, the object of this final master's work, the principles of design of hierarchical networks of Cisco will be taken into account. By following the guidelines set by cisco, the network will be able to meet the needs of the example company, for this network and be able to support emerging technologies as new technologies are adopted.

Applying the principles of hierarchical network will provide flexibility and growth to the network, in addition to having the following qualities:

- **Hierarchy:** A hierarchical network model is a useful high-level tool for designing a reliable network infrastructure. Divide the complex problem of network design into smaller, more manageable areas.
- **Modularity:** by separating the various functions that exist in a network into modules, it is easier to design. Cisco identified several modules, including the Enterprise Campus, Service Block, Data Center, and Edge Internet.
- **Resistance:** the network must be available so that it can be used both under normal conditions (maintenance periods) and abnormal conditions (hardware or software failures).

  Flexibility: the ability to modify parts of the network, add new services, or increase capacity without the need for major upgrades (that is to say replace major hardware devices).

Next, the network to be dimensioned must be categorized, taking into account the following sections:

- **Small network:** provides services for up to 200 devices.
- **Medium network:** provides services for 200 to 1000 devices.
- **Large network:** provides services for more than 1000 devices.

It will be taken into account that, to create a hierarchical network, the network must be divided into independent layers. Each layer in the hierarchy provides specific functions that define its function within the overall network. In this way, it will be possible to optimize the network and properly choose the hardware and software that perform the specific functions for that network layer.

The LAN network model to be dimensioned will include the following three layers:

- **Access layer:** provides access to the network for workgroups and users.
- **Distribution layer:** Provides policy-based connectivity and controls the boundary between the access and core layers.
- **Core layer:** Provides fast transport between distribution switches within the corporate campus.

With this layered distribution, you are dividing the network into smaller blocks, allowing it to be easier to manage and for local traffic to remain local, unless this traffic is destined for other networks, which in this case is moved to a top layer.

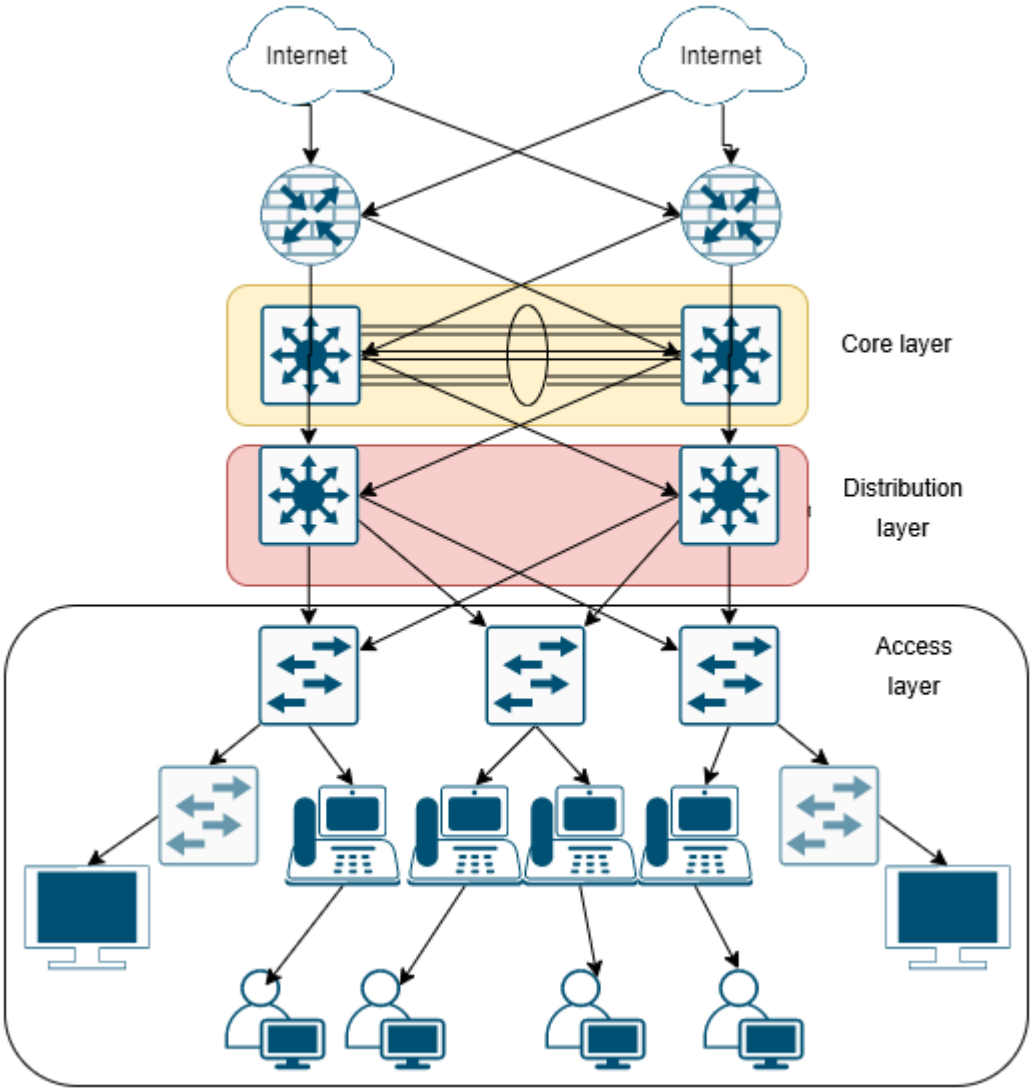


Figure 1. Network layers

4.1.1 Access layer

In the access layer, access to the network will be granted in the terminals for a LAN environment, while, if we are talking about a WAN environment, access to the network can be provided to the workers through remote access.

Layer 2 switches and access points are included in the access layer, which provide connectivity to the network equipment.

The functions of the access layer are as follows:

- Layer 2 switching
- High availability
- Port security
- Classification and marking of QoS, and confidence limits
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACL)

- Expansion tree
- Auxiliary Ethernet and VLAN power for VoIP

4.1.2 Distribution Layer

The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination.

For the distribution layer, a multilayer router or switch is used, which allows to segment work teams and isolate network problems.

The distribution layer can provide the following:

Agregación de enlaces LAN o WAN.

- LAN or WAN link aggregation.
- Policy-based security in the form of access control lists (ACLs) and filtering.
- Routing services between LAN and VLAN networks, and between routing domains (eg, EIGRP to OSPF).
- Redundancy and load balancing.
- A limit for aggregation and summarization of routes that is configured in the interfaces to the core layer.
- Broadcast domain control, since neither routers nor multilayer switches resend broadcasts. The device works as a demarcation point between broadcast domains.

4.1.3 Core layer

The network backbone or core layer, high-speed switches are used, designed to switch packets as fast as possible and interconnect the elements of the campus, such as service modules, distribution block, WAN perimeter ... For this function, They use switches like Cisco Catalyst 6500 or 6800.

For the core layer, the following characteristics must be taken into account:

- You must provide high speed switching (i.e. fast transport).
- It must provide reliability and fault tolerance.
- You must achieve scalability through faster teams, not more teams.
- You must avoid packet handling that implies a high demand for the CPU because of security, inspection, quality of service (QoS) classification or other processes.

4.1.4 Two-Level contracted core design

It should be borne in mind that when a company is small or medium, the economic expense of a hierarchical three-level network may be unfeasible, as well as, sometimes,

unnecessary. Therefore, in these cases, you can continue to follow the principles of the Cisco hierarchical network, but this time using the collapsed two-level core model.

In a collapsed core hierarchical network, the core and distribution layer are joined to form the collapsed core layer, thereby saving one layer of switches.

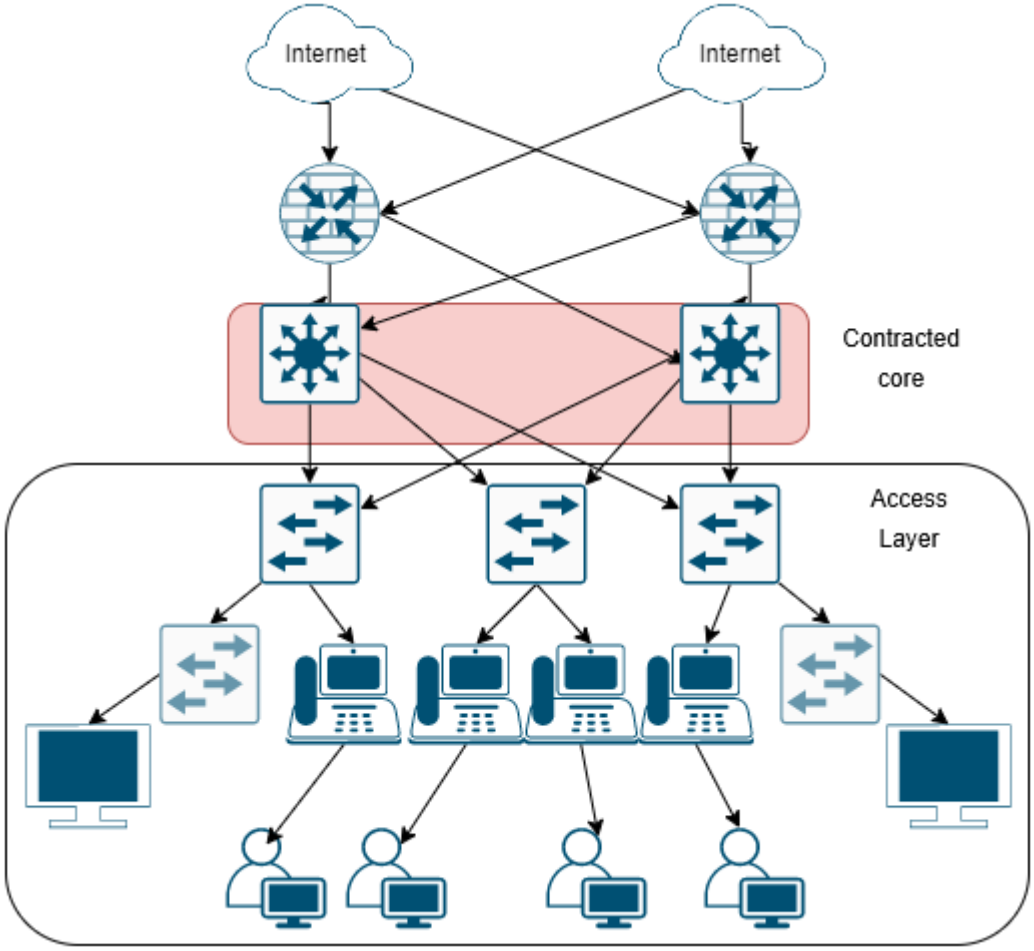


Figure 2. Two level contracted core desing

4.2 Quality of service (QoS)

In a corporate network in which countless services are used, an essential point is the management of the quality of service (QoS), thus offering a satisfactory experience to its users.

QoS is the set of mechanisms used to differentiate the different traffic flows that circulate through a network and guarantee that a connection can maintain the quality necessary for users to enjoy a satisfactory service.

In a Best Effort network, such as the Internet, all flows would try to use the bandwidth they need to transmit all their packets, but if the maximum bandwidth of the link is exceeded they will be forced to reduce their bandwidth so that everyone can keep sending packages, even if some are lost. Thanks to QoS management, it is possible to offer the necessary

resources for each traffic flow, managing the values that most affect the connections, since not all types of traffic have the same needs. For example, a video call can continue to work correctly if there is a not very high bandwidth, but if packets are lost the video call will begin to show failures. On the other hand, the transmission of a file can support losses through the forwarding of information, but if a very small bandwidth is available, the transmission can take too long and not be profitable.

The parameters that QoS manages are the following:

- **Delay:** It is a parameter that depends on the time it takes for a packet to be transmitted from one end of the network to the other.
- **Jitter:** It is a parameter that measures the difference between the arrival times between packets, whether they are consecutive or between all the packets of the same connection.
- **Bandwidth:** It is a parameter that indicates the maximum information capacity that a channel can carry.
- **Percentage of losses:** It is a parameter that indicates the percentage of packets that could not be delivered to the destination.

The QoS mechanisms that can be used can be differentiated into two categories:

- **Prioritized model of differentiated services:** Called Diffserv, it is about marking packets according to a desired type of service. Routers and switches in the network generally use traffic queuing strategies to prioritize traffic according to that mark in the packet.
- **Parameterized model of integrated services:** In this model, it is the applications that reserve a resource throughout the network using a resource reservation protocol. It is currently deprecated on large networks due to its scalability issues. Its main exponent was the RSVP protocol.

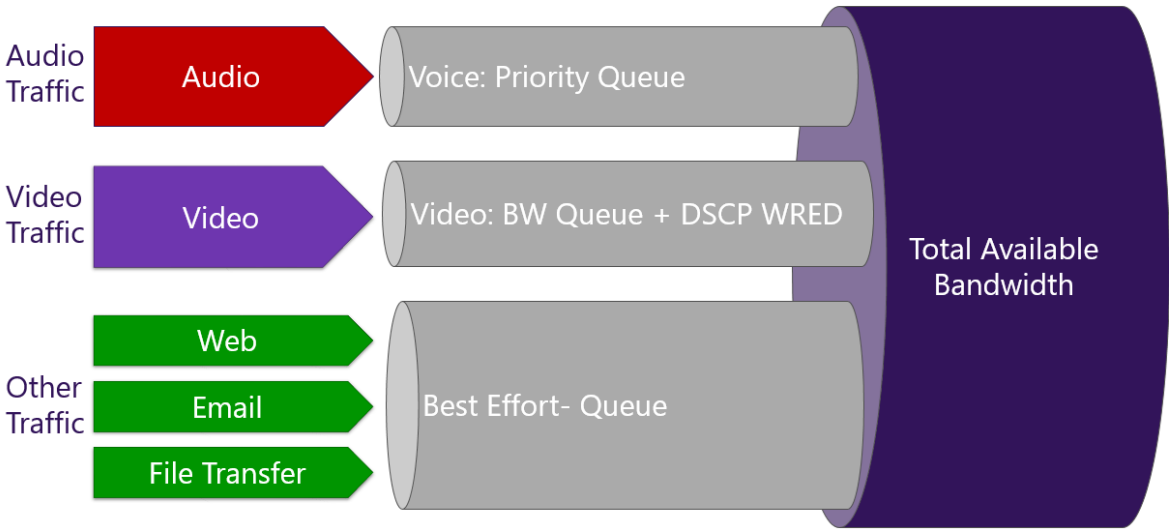


Figure 3. QoS

In the final master project, the object of this report, Diffserv will be used, so we will go a little deeper into this model.

The DiffServ architecture defines the DiffServ (DS) field, which replaces the IPv4 ToS field for making Per-Hop Behavioral (PHB) decisions about packet classification and traffic conditioning functions, such as measurement, marking, shape, and surveillance. .

The RFCs do not dictate how to implement PHB; this responsibility rests with the equipment manufacturer. Cisco implements queuing techniques that can base its PHB on IP precedence or the DSCP value of a packet's IP header. Based on DSCP or IP precedence, traffic can be classified into a certain class of service. Packages included in a class of service are treated in the same way.

The six most significant bits of the DiffServ field are called according to the DSCP. The last two CU bits (currently not used) of the DiffServ field were not defined within the architecture of the DiffServ field; they are now used as Explicit Congestion Notification (ECN) bits. Routers at the edge of the network classify packets and mark them with IP or DSCP precedence value on a diffserv network. Other core network devices that support the use of Diffserv use the DSCP value of the IP header to select a PHB behavior for the packet and provide the appropriate QoS treatment.

The DiffServ standard uses the same precedence bits (the most significant bits: DS5, DS4, and DS3) for the priority setting, but gives more information using the next three bits of the DSCP. DSCP values range from 0 to 63. One advantage of DSCP is that it has a wide range of values to associate with different traffic, which allows for a more specific assignment. The DSCP works in layer 3 of the OSI (Open Systems Interconnection) model. It follows the same classification as the CoS / 802.1p values.

DiffServ rearranges and renames the precedence levels in these categories:

LEVEL OF PRECEDENCE	DESCRIPTION
7	Stays the same (link layer and routing protocol remain active)
6	Stays the same (used for IP routing protocols)
5	Express Forwarding (EF)
4	Class 4
3	Class 5
2	Class 6
1	Best effort

Table 1. DSCP Categories

With this system, a device prioritizes traffic first by class. It then distinguishes and prioritizes traffic of the same class, taking into account the probability of dropping.

4.3 IP Telephony

The Voice Over Internet Protocol (VoIP) is a set of resources that make it possible for the voice signal to travel through the Internet using the IP protocol.

In IP telephony the following parts can be differentiated:

- **Customer:** The customer establishes voice calls, this information is received through the user's microphone (information input), it is encoded, packaged and, in the same way, this information is decoded and reproduced through the speakers or headphones (information output).
- **Server:** The servers are responsible for managing database operations, carried out in real time as in one outside of it. These operations include accounting, collection, routing, service administration and control, and user registration.

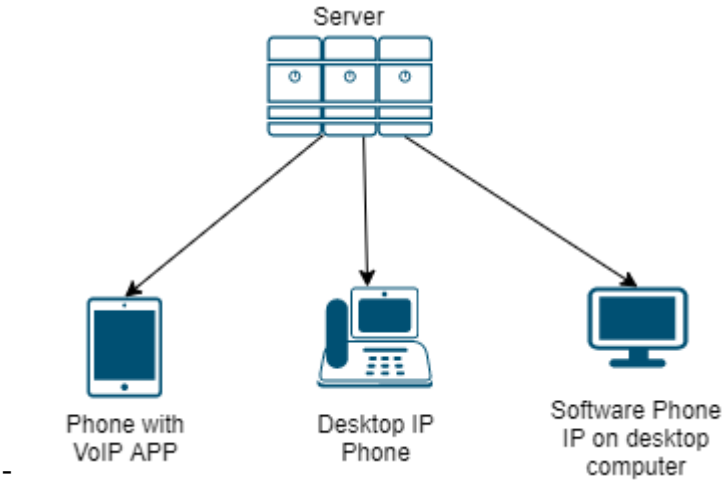


Figure 4. VoIP Arquitecture

4.4 WiFi Network

All network architecture of a company must have a WiFi network that provides freedom of movement for workers and guests in the building. Through the WiFi network, workers can access information from anywhere in the building, without having to be in a LAN workstation.

For the implementation of a WiFi system in the company, it will be necessary to install access points (AP) in the building. WiFi networks use the 2.4 GHz and 5 GHz bands, so APs that work on both frequencies can be used or only one of them can be selected.

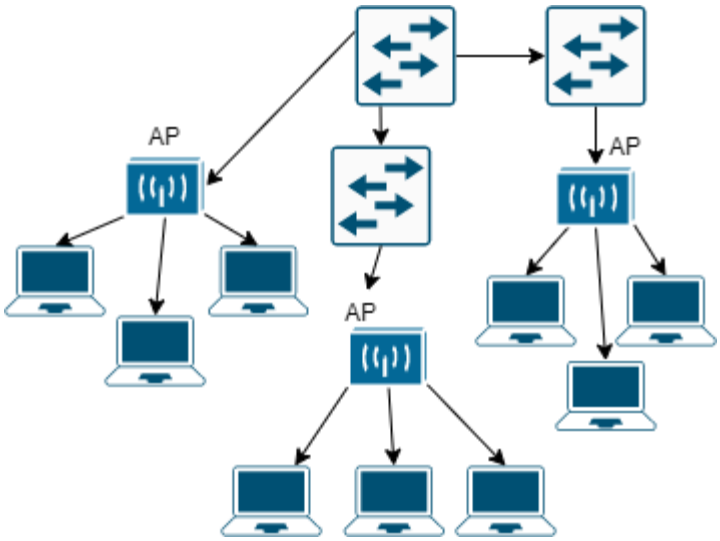


Figure 5. WIFI Arquitecture

4.5 Layer 2 security features

The very definition of a LAN network makes this type of network vulnerable, since it connects computers and devices in a specific area to share data and information between them. These networks incorporate methods of direct connection to the internet, to facilitate work performance, but in the same way, the doors of the company are opened if security measures are not in place.

In any LAN network, the hardware must be kept up to date, including servers and switches, as well as security patches. It is also necessary to have a security layer of data and information. The human factor plays an important role, since the creation of secure passwords and security education to prevent possible cases of identity theft or fraud is essential.

A very important part of LAN security, and one that does not depend on the human factor, is the control of access to the LAN. Thanks to this security technique, you can know who is using the network and allow or deny the entry of that device and restrict the resources that that particular user can use on the network.

For the control of access to the LAN network, the security mechanisms detailed in the following points can be used.

Layer 2 security functions include port security, DHCP Snooping, Address Resolution Protocol (ARP), VLAN network segmentation ...

4.5.1 Port Security

The port security function limits and identifies the MAC addresses of the different computers that are allowed to access the port.

When different secure MAC addresses are assigned to a port, this port does not send packets to MAC addresses that are not included in the secure group. In this way, when a computer with a MAC address not included in the table of secure MAC addresses, an intruder will be detected and will not be allowed access to the network.

This management of the secure MAC tables can be done on the switch itself or make use of a RADIUS server that stores the secure addresses.

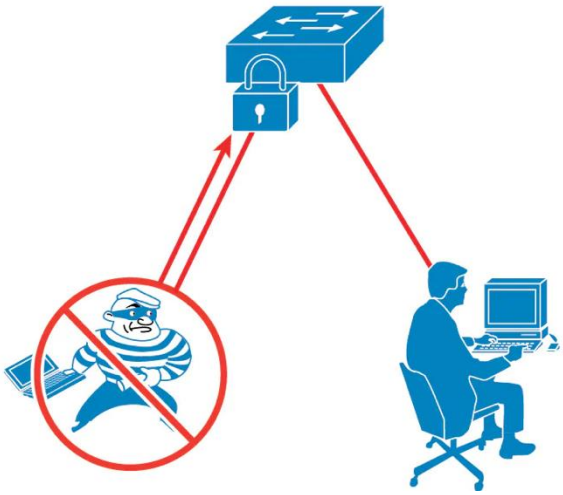


Figure 6. Security port

4.5.2 Servidor Radius

Remote Access Dial In User Service (RADIUS) is a protocol that offers a network security mechanism, as well as flexibility, expandability, and simplified management of access credentials to a network resource.

This protocol is used with the client-server scheme, that is, the user who connects with some credentials to access a resource asks a server to verify their credentials and allow or not the user access to the resource.

Thanks to the radius server, security policies such as port-based security can be applied, since RADIUS can store the information necessary to allow or not the access of a certain device to the LAN through physical access.

In addition to providing security to the wired LAN, RADIUS can be used for the management of users of the WiFI network, allowing access to stored users, either by MAC or IP or by using a captive portal where the user will enter the credentials provided to you.

This second option is widely used in guest WiFi networks, controlling at all times the start and end of the user's browsing period.

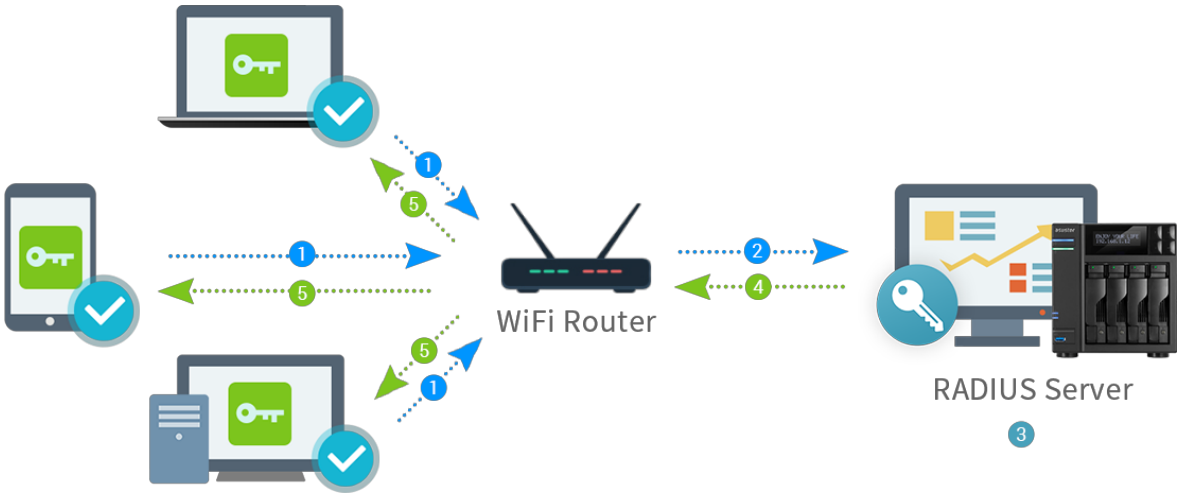


Figure 7. Radius Server

4.5.3 DHCP Snooping

The DHCP Snooping security feature acts as a firewall between untrusted hosts and DHCP servers. Using this function, you can distinguish between untrusted devices connected to the end user and trusted devices connected to the DHCP server or other switch.

When a switch receives a packet from an untrusted interface and the interface belongs to a VLAN that has DHCP Snooping enabled, the switch compares the source MAC address and that of the DHCP client. If the MAC address of the source and client match, the switch will transmit the packet. If, on the other hand, it is not registered, the switch drops the packet.

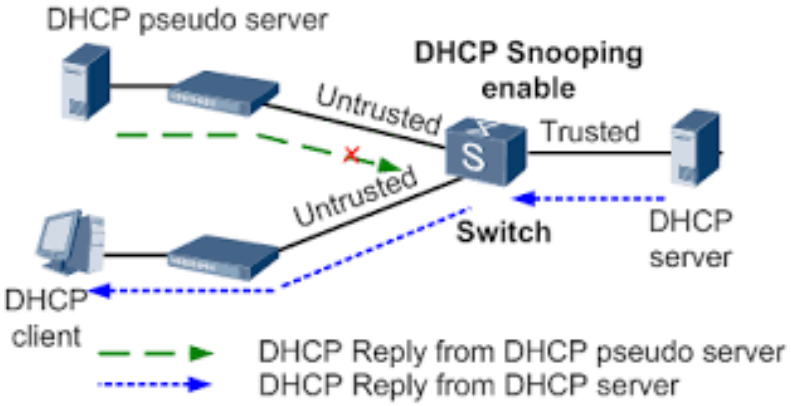


Figure 8. DHCP Snooping

4.5.4 Dynamic ARP Inspection

Dynamic ARP Inspection is a security feature that validates ARP packets on a network. Ensures that only requested ARPs and valid responses are relayed across the network.

Dynamic ARP Inspection determines the validity of an ARP packet based on valid MAC and IP address binding, stored in the DHCP Snooping tag database. This database is built by DHCP Snooping, if DHCP Snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any control. However, on untrusted interfaces, the switch only forwards the packet if it is valid.

4.5.5 IP Source Guard

IP Source Guard is a security feature that uses the DHCP Snooping database and manually added IPs to restrict IP traffic on non-routed Layer 2 interfaces.

It can be used to prevent traffic attacks originated when a host tries to use the IP address of its neighbor.

4.6 Perimeter security features

A perimeter security system is a set of equipment that is dedicated to the protection of the entire computer system of a company.

One of the essential elements in this type of system is the firewall.

A firewall is a critical security device for protecting the perimeter. It can act in several layers of the OSI model (mainly network and transport, although they can also be applied). It can be an application, a device, or a combination of both. Its main function is to isolate internal networks and block external networks according to the policies of each organization.

There are network firewalls, which control the traffic in transit on the network.

There are computer firewalls that control a computer's connection to a network. For example, on personal computers, personal firewalls determine which packets can enter and which packets can exit.

Firewalls analyze IP packets, and taking into account source address, destination address, protocol and destination port, decide to allow or block their passage.

4.6.1 Virtual Private Network (VPN)

This technology allows the secure extension of the LAN, over a public or uncontrolled network such as the Internet. This functionality is accomplished by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of both methods.

A VPN network consists of the WAN connection of several sites, being a private connection in the eyes of the user.

To establish a VPN connection, the user must be identified and the data to be transmitted must be correctly encrypted. In addition, users must have updated keys.

4.6.1.1 VPN Gateway to Gateway

The VPN Gateway to Gateway allows the connection between two routers in a secure way and that a client at one end appears to be from the same remote network at the other end. This functionality allows data and resources to be easily and securely shared over the Internet.

When it comes to bringing this functionality to the company that is the object of this TFM, it allows the economic saving of resources, by not having to have all the services and servers replicated in all the company'scampus.

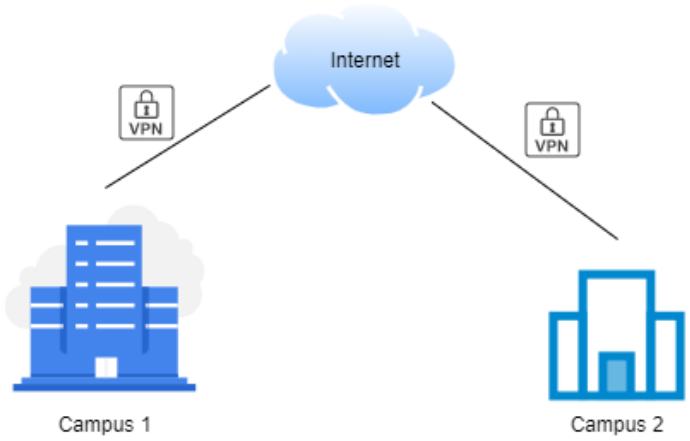


Figure 9. VPN Gateway to Gateway

4.6.1.2 VPN Client to Gateway

The VPN client to gateway is a connection between a remote user and the network. The VPN client is configured on the user's computer, so that the user can access the network remotely.

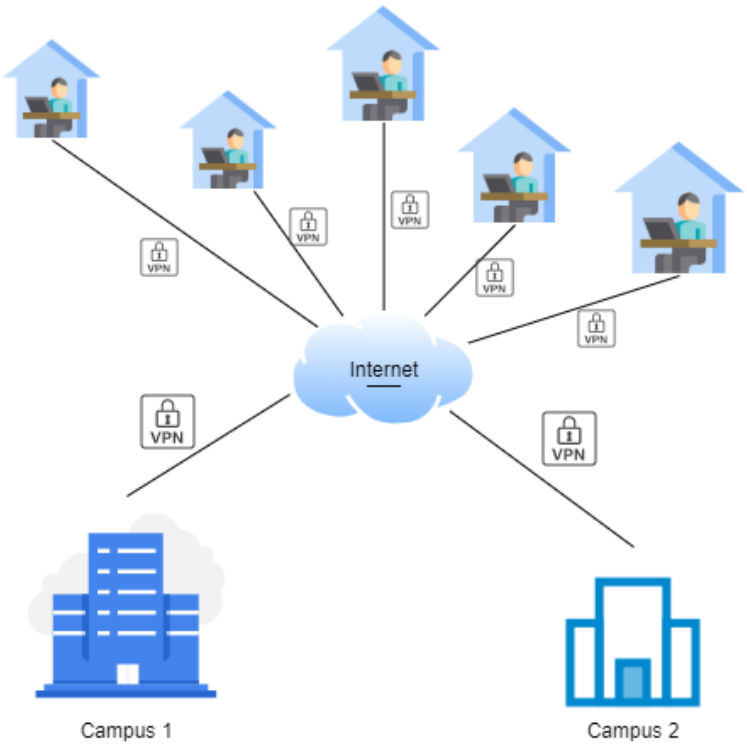


Figure 10. VPN Client to Gateway

4.6.2 DMZ

A demilitarized zone (DMZ) or perimeter network is a local network that sits between an organization's internal network and an external network, usually on the Internet. The goal of a DMZ is that connections from the internal and external network to the DMZ are allowed, while in general connections from the DMZ are only allowed to the external network (DMZ computers should not connect directly to the internal network). This allows computers in the DMZ to serve the external network, while protecting the internal network in the event that intruders compromise the security of computers located in the DMZ.

The DMZ is commonly used to locate servers that need to be accessed from the outside, such as email, web, and DNS servers. And it is precisely these services hosted on these servers that can establish data traffic between the DMZ and the internal network,

such as a data connection between a web server and a protected database located on the internal network.

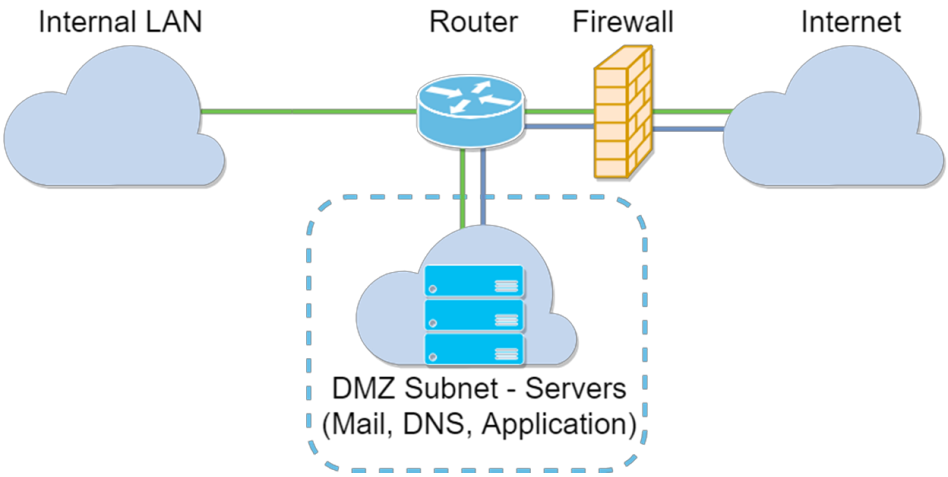


Figure 11. DMZ Zone

5 DESING OF THE NETWORK ARCHITECTURE

For the design of the network architecture, of this final master's work, it will be taken into account that the company, which will use the infrastructure, has the following disposition:

- It has 400 employees
- It has 2 geographically separated locations
- The maincampus, has 300 employees
- The principal campus of the company, has 100 employees
- In both locations, a WiFi network is required, both for employees and guests
- The company has two different departments
- The company has employees with the telework modality, so it needs them to be able to connect to the resources of the campus.

The network is going to be dimensioned so that it is scalable, secure and robust, has optimal performance and is easily administrable for subsequent maintenance.

Therefore, for the campus, a structure that follows the principles of the Cisco hierarchical network has been chosen, with the following layers:

- Core layer
- Distribution layer
- Access layer

With these layers, an infrastructure with high availability will be achieved through a hierarchical network design. In addition, it integrates IP communications, mobility and security.

While in campus 2 a contracted core structure has been chosen, which will allow to follow the principles of the hierarchical cisco network, obtaining the benefits of this structure, but saving equipment costs by using a single layer of L3 switches.

Greater security and flexibility will be provided by managing access, VLANs, and VPNs with IPsec.

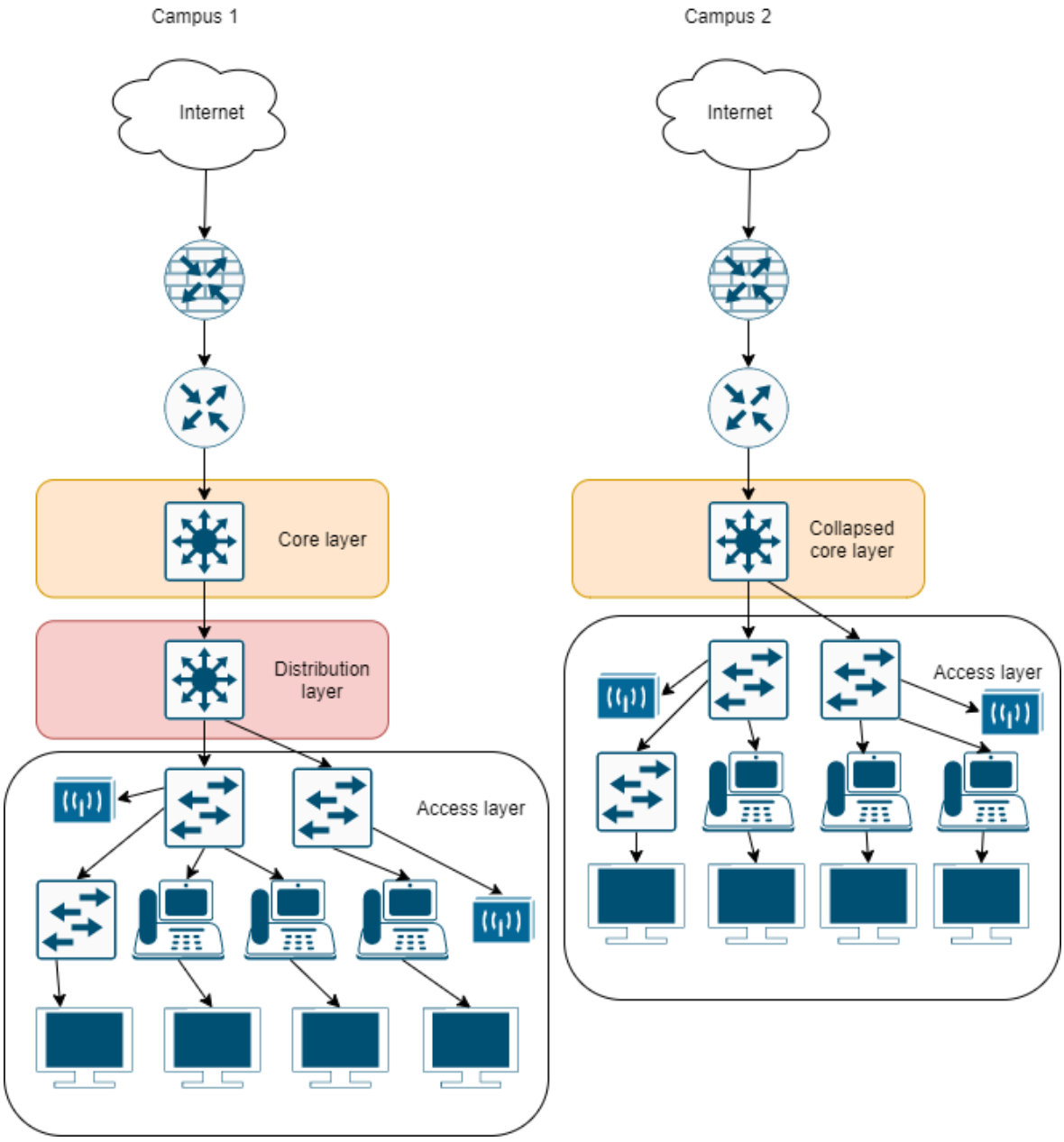


Figure 12. Network desing

For the campus 1, the following network elements will be available:

- **1 FirePower 2110**: Firewall for perimeter security
- **1 Cisco RV320 Gigabit Dual WAN VPN**: Router for internet access, LAN security and VPN creation
- **2 Cisco Catalyst 3750**: Layer 3 switch for fast communication at the core layer, hosting the MAC address table and the IP routing table. It will also control intra-VLAN communication and packet routing between different VLANs.
- **12 Cisco SG300-52 Gigabit Managed Switch**: Layer 2 switch for Layer 2 communication, and access to workstations and VoIP.

For campus 2, the following network elements will be available:

- **1 FirePower 2110**
- **1 Cisco RV320 Gigabit Dual WAN VPN**
- **1 Cisco Catalyst 3750**
- **4 Cisco SG300-52 Gigabit Managed Switch**

5.1 Interconnection of sites and remote Access

As indicated in the characteristics of the company, it is necessary that both campus are interconnected, so that resources can be shared. For this interconnection, a VPN (virtual private network) with IPsec (Internet Protocol security) will be carried out between both sites, allowing workers from site 2 to connect to the resources of campus 1.

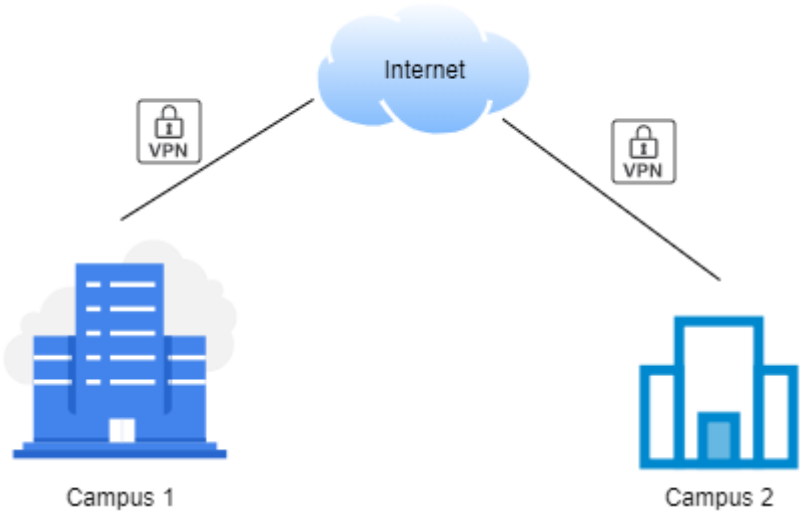


Figure 13. Interconnection of two Campus

Teleworking is also necessary, so workers will be given access to the company network through a VPN client to Gateway. For this, workers will have a VPN client installed

on their computer that will allow remote access to the company network. In this case, the chosen VPN client is Shrew Soft Client.

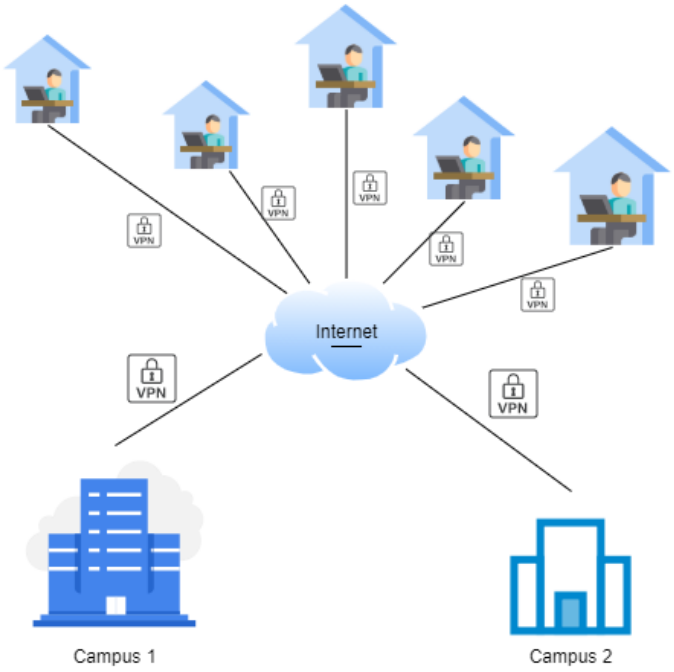


Figure 14. Remote Access via VPN client to gateway

The configuration of the VPN Gateway to Gateway and the VPN Client to Gateway will be carried out using the Cisco RV320 Gigabit Dual WAN VPN router. In addition, this device will provide the internet network interconnecting the WAN perimeter with the access layer.

5.2 Network security

For the perimeter security of both sites, a Cisco Firepower 2110 Firewall will be used, which has the functions of a conventional firewall, in addition to the Cisco analysis software, which host the next generation Firewalls. These characteristics will provide our network with extra security against external threats, ensuring:

- Block threats automatically using Cisco Advanced Malware Protection (AMP).
- Gain deeper visibility through the Firepower Next Generation Intrusion Prevention System (NGIPS).
- Detect, analyze and protect with Cisco Talos Threat Intelligence

For internal security, the network will be divided into 4 VLANs, and the accesses to them and the inter-VLAN permissions will be managed through the L3 switches. In the same way, the allowed MAC tables will be managed, through the security configuration in the port

through MAC, making the switch filter the devices that try to connect to the LAN and allow only the connections of the devices, of which its MAC is stored. The MAC store in this case will be stored in the same switch.

Another security mechanism that is going to be implemented is DHCP snooping to provide the network with a security mechanism to avoid receiving false DHCP response packets and registering wrong addresses. To do this, the device ports will be classified as trusted or untrusted.

Using the Cisco RV320 Gigabit Dual WAN VPN Router, a DHCP server will be included in each VLAN.

The IPs assigned to each VLAN will be the following:

	Network Campus 1				Network Campus 2			
	VLAN 1	VLAN 2	VLAN 3	VLAN 4	VLAN 1	VLAN 2	VLAN 3	VLAN 4
NETWORK	10.10.0.0/25	10.20.0.0/25	10.30.0.0/25	10.40.0.0/25	10.10.0.128/25	10.20.0.128/25	10.30.0.128/25	10.40.0.128/25
Broadcast	10.10.0.127	10.20.0.127	10.30.0.127	10.40.0.127	10.10.0.255	10.20.0.255	10.30.0.255	10.40.0.255
HOST MIN	10.10.0.1	10.20.0.1	10.30.0.1	10.40.0.1	10.10.0.129	10.20.0.129	10.30.0.129	10.40.0.129
HOST MAX	10.10.0.126	10.20.0.126	10.30.0.126	10.40.0.126	10.10.0.254	10.20.0.254	10.30.0.254	10.40.0.254
HOST	126	126	126	126	126	126	126	126
IP ROUTER	10.10.0.1	10.20.0.1	10.30.0.1	10.40.0.1	10.10.0.129	10.20.0.129	10.30.0.129	10.40.0.129
DHCP MIN	10.10.0.50	10.20.0.50	10.30.0.50	10.40.0.50	10.10.0.178	10.20.0.178	10.30.0.178	10.40.0.178
DHCP MAX	10.10.0.100	10.20.0.100	10.30.0.100	10.40.0.100	10.10.0.228	10.20.0.228	10.30.0.228	10.40.0.228
PPTP MIN	10.10.0.101	10.20.0.101	10.30.0.101	10.40.0.101	10.10.0.229	10.20.0.229	10.30.0.229	10.40.0.229
PPTP MAX	10.10.0.110	10.20.0.110	10.30.0.110	10.40.0.110	10.10.0.238	10.20.0.238	10.30.0.238	10.40.0.238
SSL MIN	10.10.0.111	10.20.0.111	10.30.0.111	10.40.0.111	10.10.0.239	10.20.0.239	10.30.0.239	10.40.0.239
SSL MAX	10.10.0.120	10.20.0.120	10.30.0.120	10.40.0.120	10.10.0.248	10.20.0.248	10.30.0.248	10.40.0.248

Table 2. Network Distribution

VLAN 1 will be used for common equipment in the company, such as servers, routers, switches, printers, etc. On the other hand, VLAN 2 and VLAN 3 will be used to differentiate company departments and VLAN 4 for VoIP.

In the following figures, you can see the interconnection of the equipment of the different layers in the two sites, without the firewall.

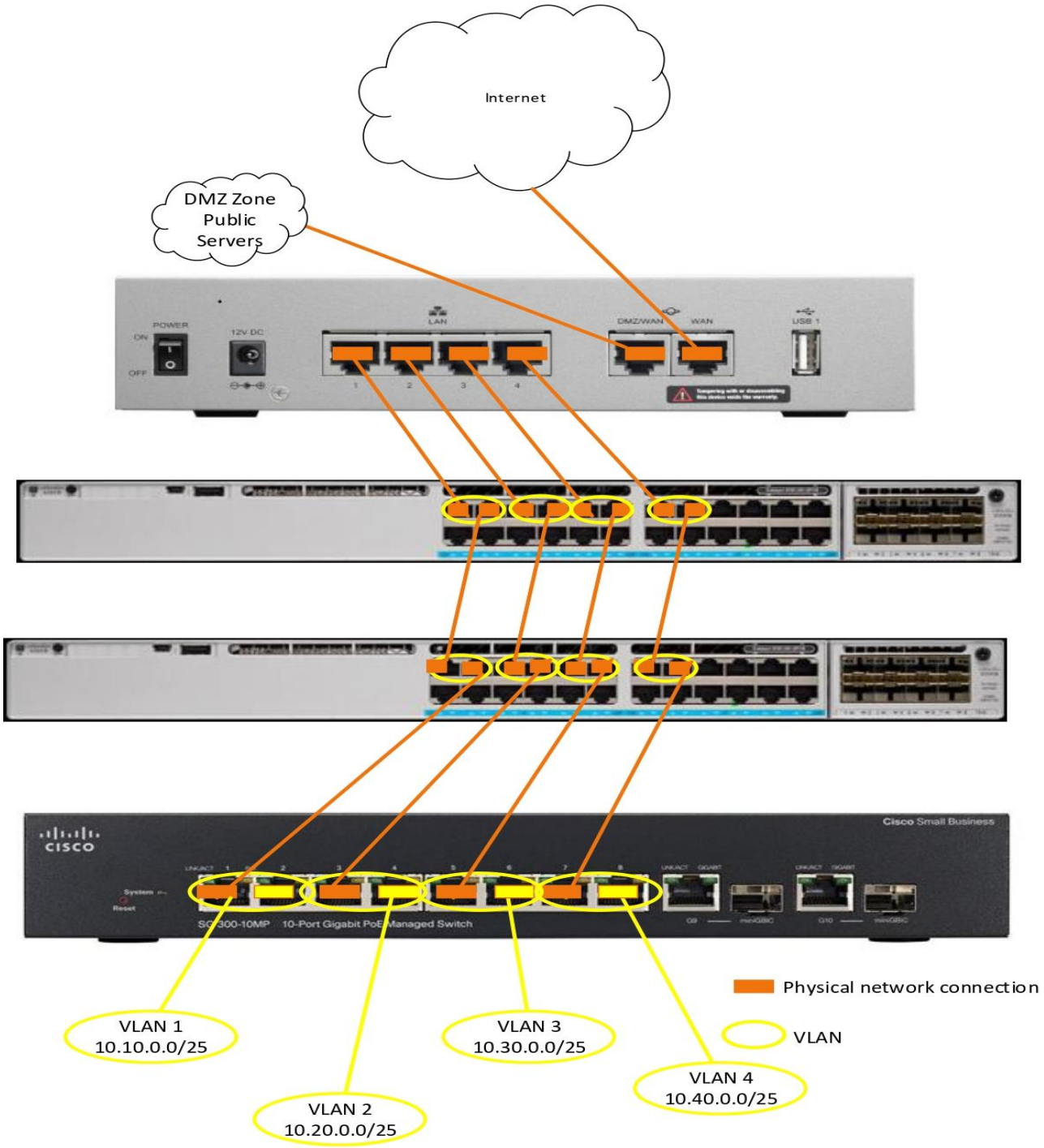


Figure 15. Network connection Campus 1

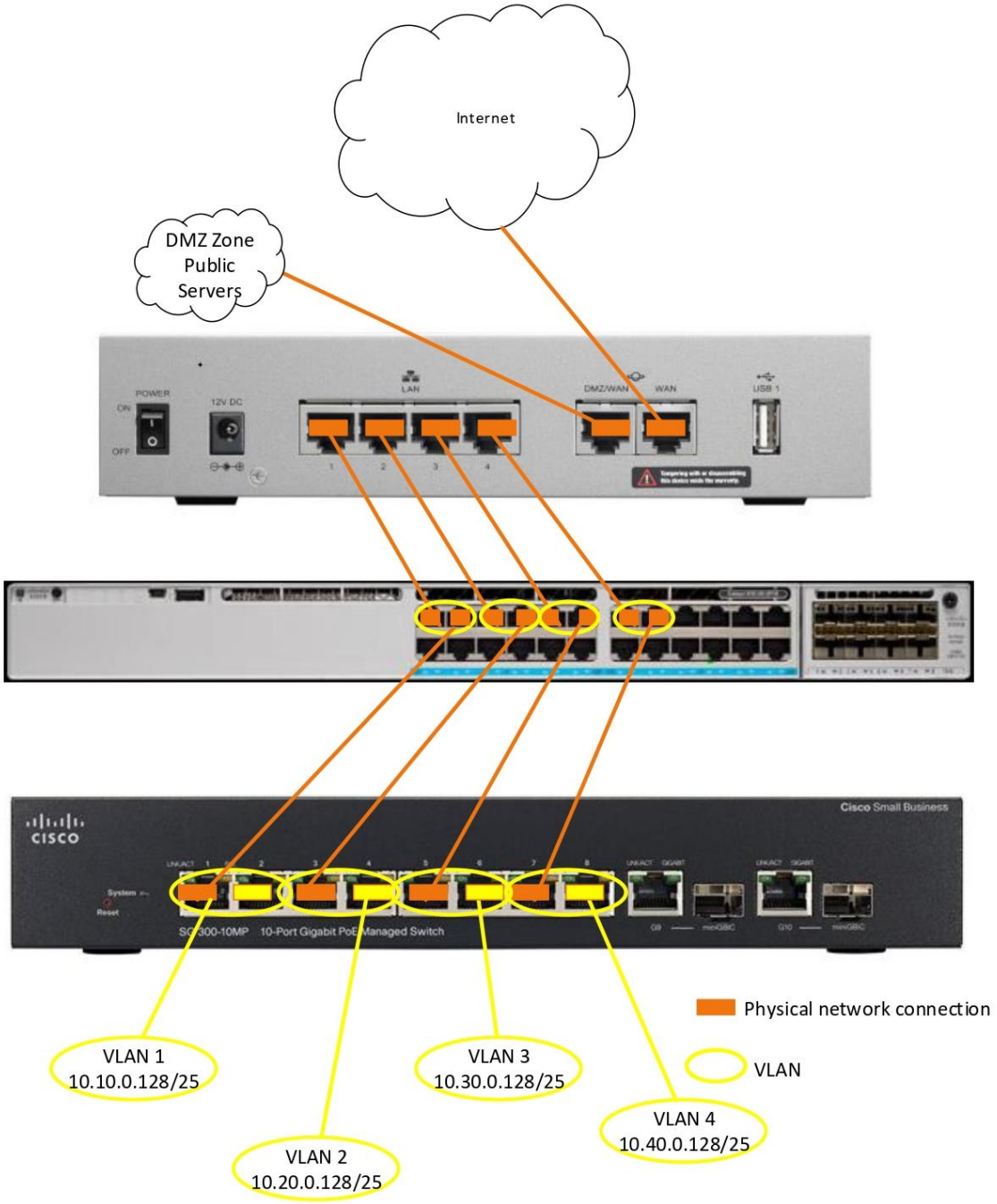


Figure 16. Network connection Campus 2

Regarding public servers, email and DNS will be hosted in the DMZ, configured using the Cisco RV320 Gigabit Dual WAN VPN router, ensure that internal users have secure connectivity to Internet services.

Finally, we are going to add the IP Source Guard network security mechanism is that it restricts IP traffic on Layer 2 ports that are not trusted by filtering traffic based on the manually configured IP or DHCP snooping binding database. This feature helps prevent IP spoofing attacks when one host tries to spoof and use the IP address of another host. Any

IP traffic entering the interface with a source IP address other than the one assigned (via DHCP or static configuration) will be rejected.

5.3 QoS

The QoS function will be used to manage network traffic, prioritizing specific services, while still offering the best performance to lower priority services.

In the network to be configured, real-time and VOIP traffic will be prioritized, so that videoconferences can be made without problems and phone calls work correctly. Two services in which, if packets are lost, communication is severely impaired.

For the rest of the traffic, the Best effort system will be used, which does not guarantee the delivery of the packet, but does ensure that it will try to get the packet with ordinary priority on the LAN.

5.4 VoIP telephony

Asterik, free software, distributed under the GNU license, will be used for the VoIP-based PBX telephone exchange.

With this switchboard you will be able, in addition to call management, definition of NVR, call queues, answering machine ...

For the client, VoIP terminals will be used that will be distributed in the different work stations.

For users with remote work, a softphone will be used through the Jitsi software that will be installed and configured on the worker's computer, thus being able to make calls from their VoIP user with their computer.

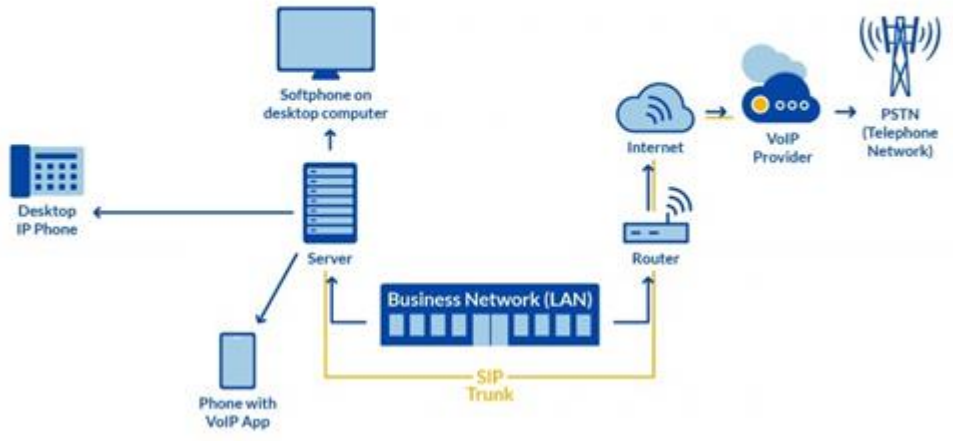


Figure 17. VoIP Diagram

5.5 WiFi Network

For the WiFi network, Ruckus ZoneFlex R500 Dual-Band 802.11ac 2X2: 2 Access Points will be used with a controller installed on the company's private servers, for the management of all the company's access points.

The chosen controller is the Virtual SmartZone Essentials (Vsz-E). Through the controller, you can configure all the APs in the company, as well as keep them updated with the latest firmware.

The APs located in campus 2 will connect with the controller through the IPsec VPN tunnel, ensuring secure communication.

In addition, the APs will be included in two zones, to differentiate the APs from the two locations and to be able to have them located in the event of a breakdown.

All APs will be configured to broadcast two SSIDs, one for workers and one for guests.

The controller will connect with a Radius server to manage connected devices and control connection permissions, and a hotspot will also be added so that guest users can register and make use of the wireless connection.

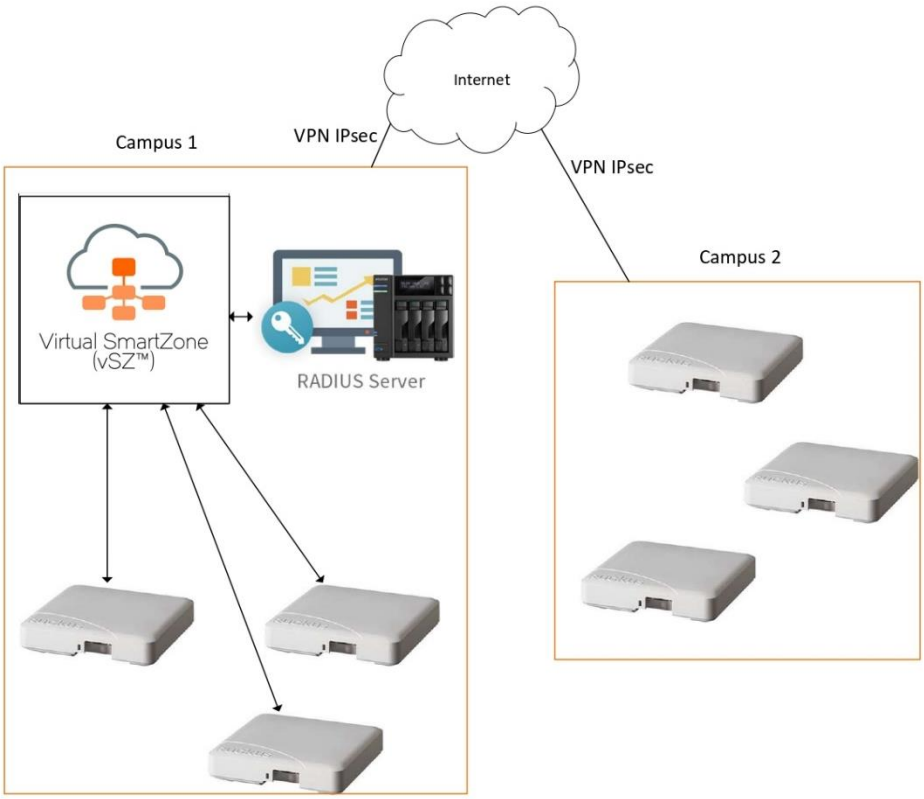


Figure 18. WiFi Diagram

6 IMPLEMENTATION

For the implementation of this final degree project, a variation of the previously described design will be implemented, to be able to make the architecture with the elements found in the laboratory.

For both sites, a Cisco RV320 Gigabit Dual WAN VPN router and a Cisco Small Business SG300-10 switch will be used.

Through the RV320 router, layer 3 functions will be performed, such as inter-VLAN configuration, also LAN security functions and the connection with the outside and communication between both sites through IPsec VPN, as well as the communication of remote workers with the office using a VPN client to gateway. Another functionality that will be configured in this device is QoS.

With the SG300-10 switch, connectivity will be provided to the workstations at both locations. And security functionalities will be implemented such as port security through MAC, DHCP Snooping, IP source guard, ARP Inspection ...

In the following figures, you can see the implemented scheme:

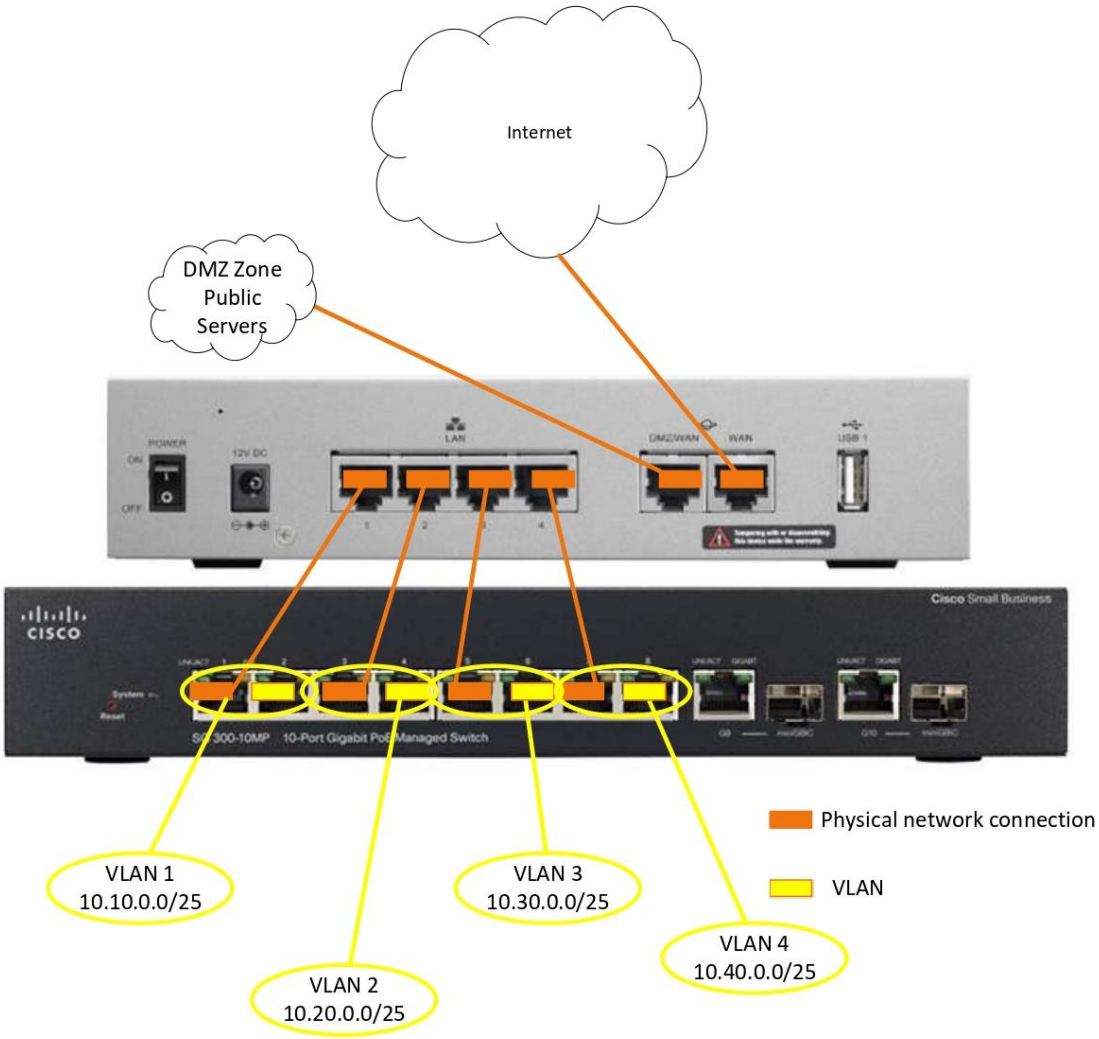


Figure 19. Implementation campus 1

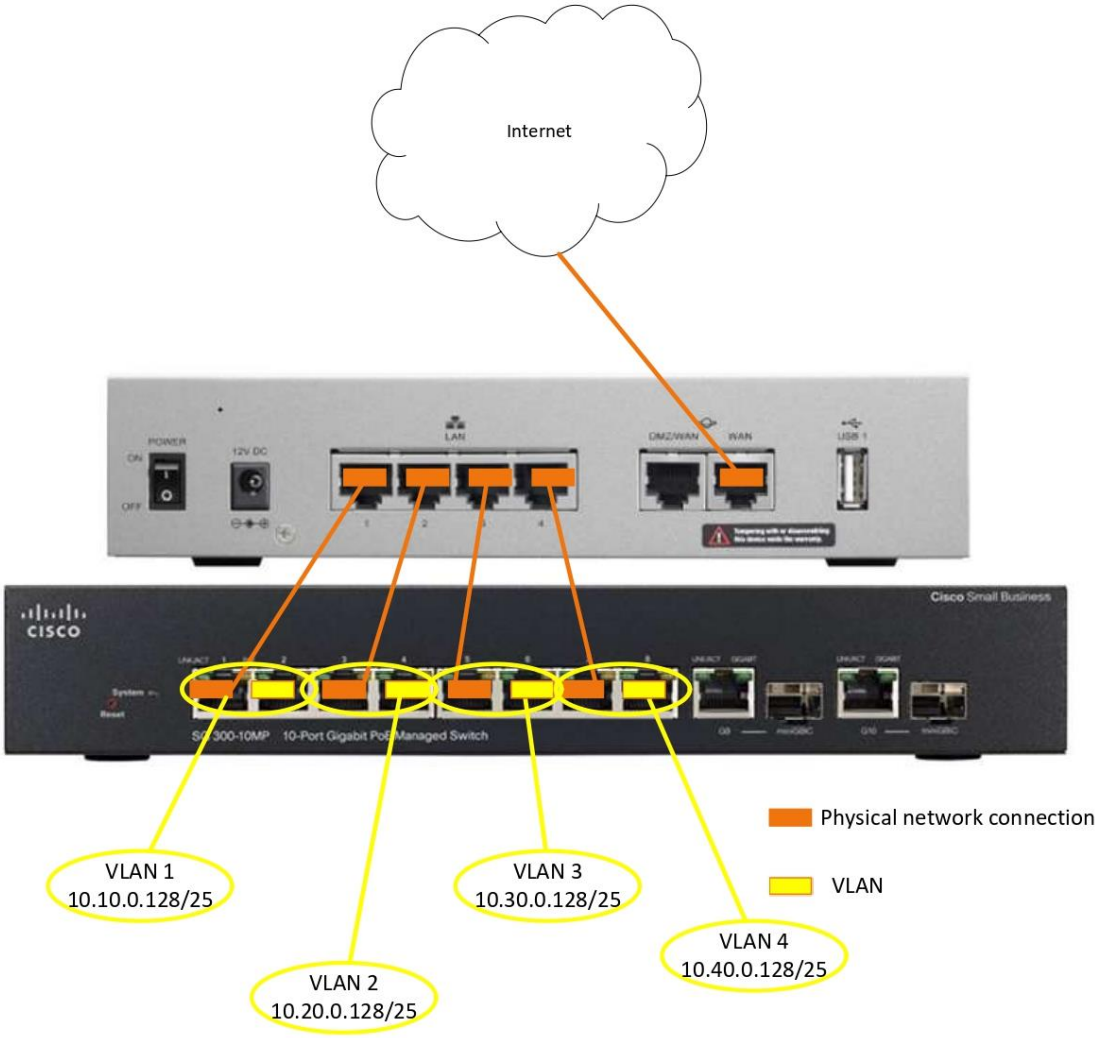


Figure 20. Implementation campus 2

Regarding the IPs used, the same ones that have been indicated in the design will be used.

6.1 Configuration Cisco Small Business SG300-10

First, the Cisco Small Business SG300-10 switch has been reset to the factory state. To do this, the Reset button has been held down for a few seconds, causing it to be reset and thus all the device's LEDs turn on for a few seconds.

When the device is in its initial state, it is assigned the IP 192.168.1.254, and the power LED indicator flashes continuously. Once the definitive IP is assigned, this led will remain on steady.

The web administrator of the device will be used to configure it, for this reason we will access the device through a web browser, entering the IP 192.168.1.254 in the address bar.

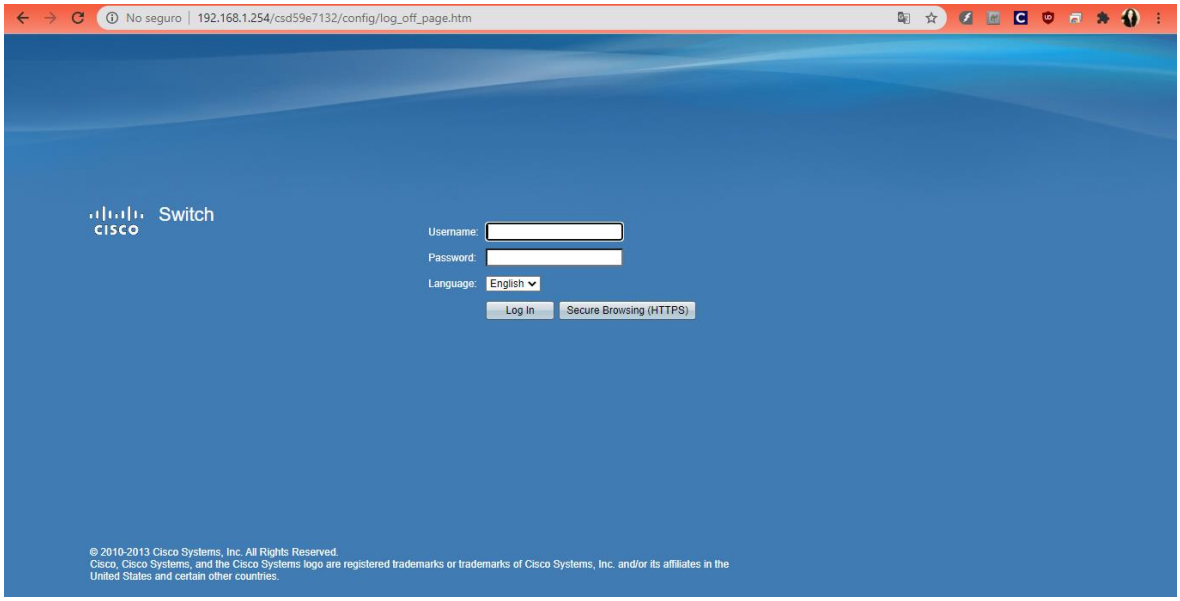


Figure 21. Access to the web browser

At this point, we will enter the default username and password, which is cisco in both cases.

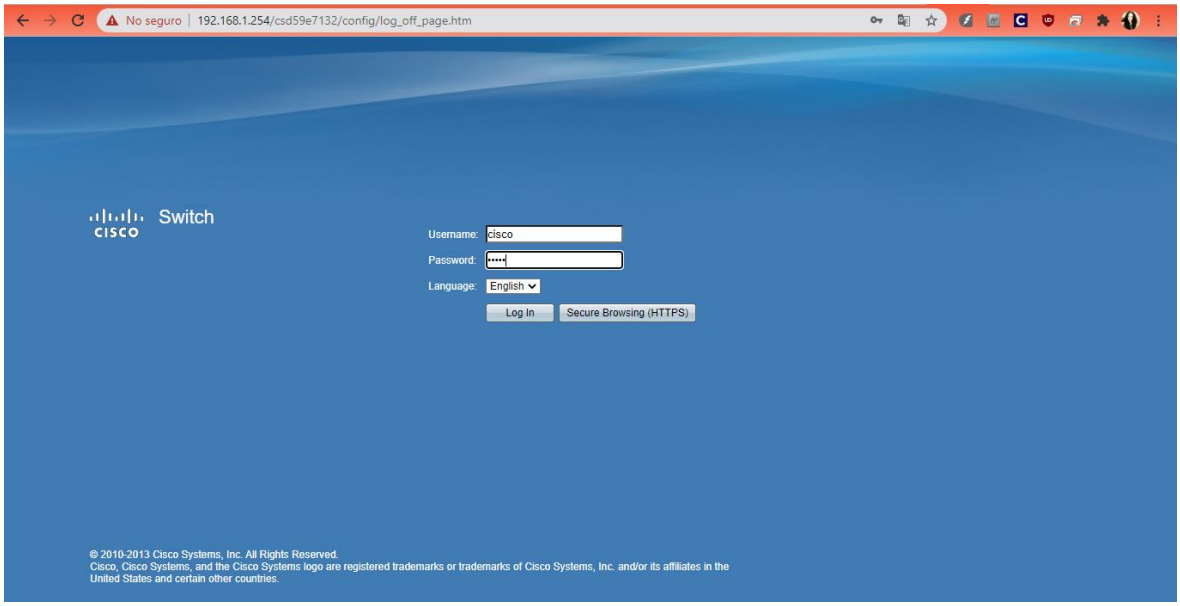


Figure 22. User and password are entered

Next, you are asked to change the device password, so TFM-Luisa has been chosen as the password.

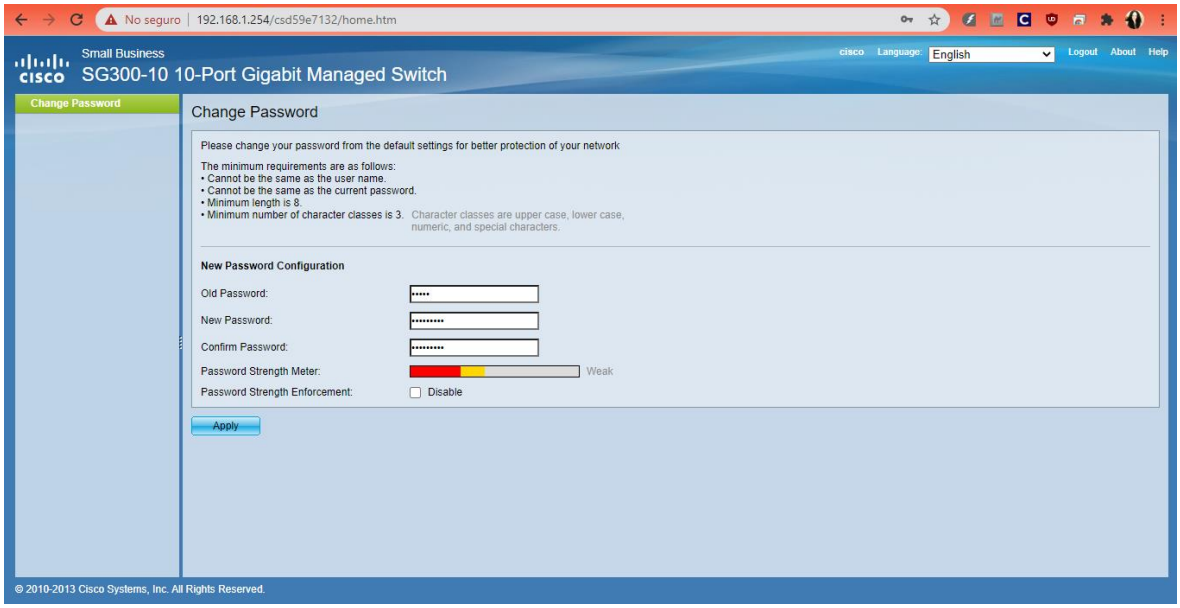


Figure 23. Change of password

The configuration of the equipment will begin by changing the IP address to one of the range to be used. For VLAN 1, the address range 10.10.0.0/25 will be used, and for this specific device the IP 10.10.0.2/25.

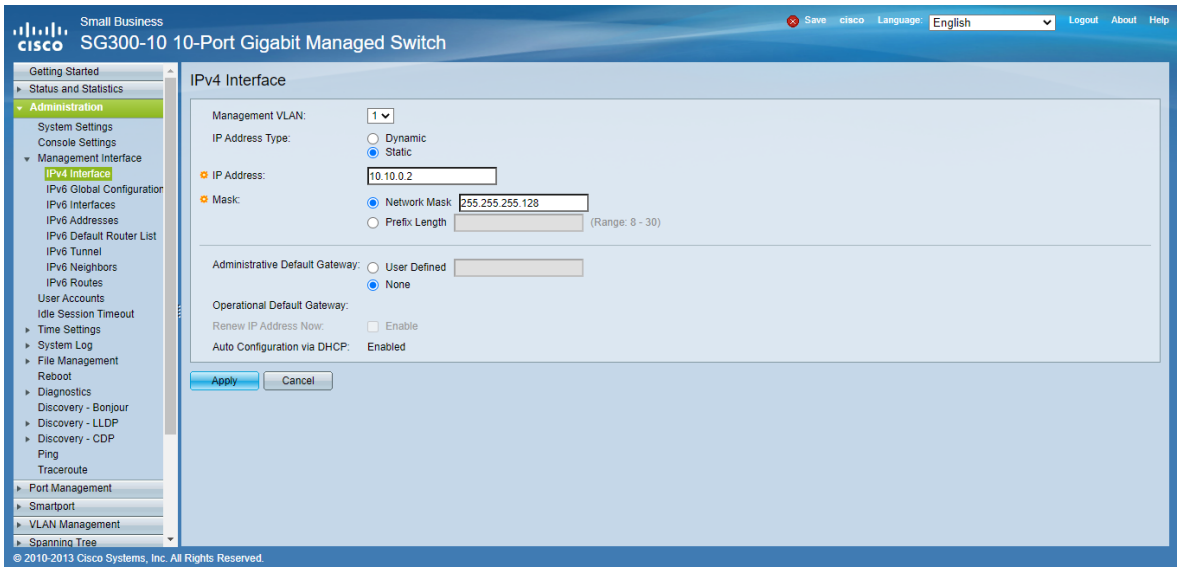


Figure 24. IP change

The device warns that the connection with the equipment will be lost, a warning that will be accepted and it will reconnect with the equipment on the new IP.

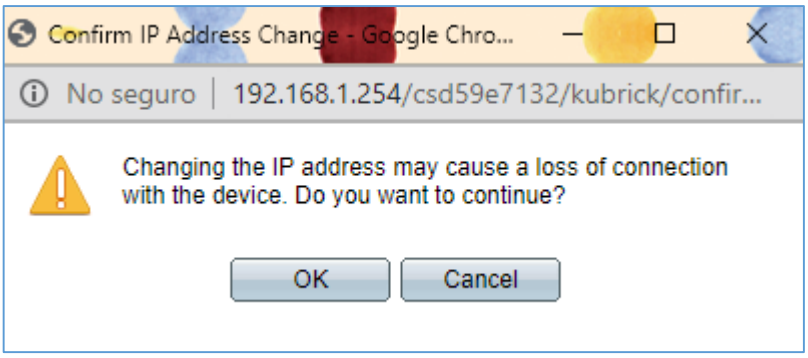


Figure 25. Accept reconnection

6.1.1 Network Division Using Vlan

Next, two PCs will be connected to the switch, PC1 on port 1 and PC2 on port 4, both ports are within VLAN1, therefore, both PCs should communicate.

As can be seen in the figure below, the communication between PC1 (10.10.0.100) and PC2 (10.10.0.200) is carried out without problems.

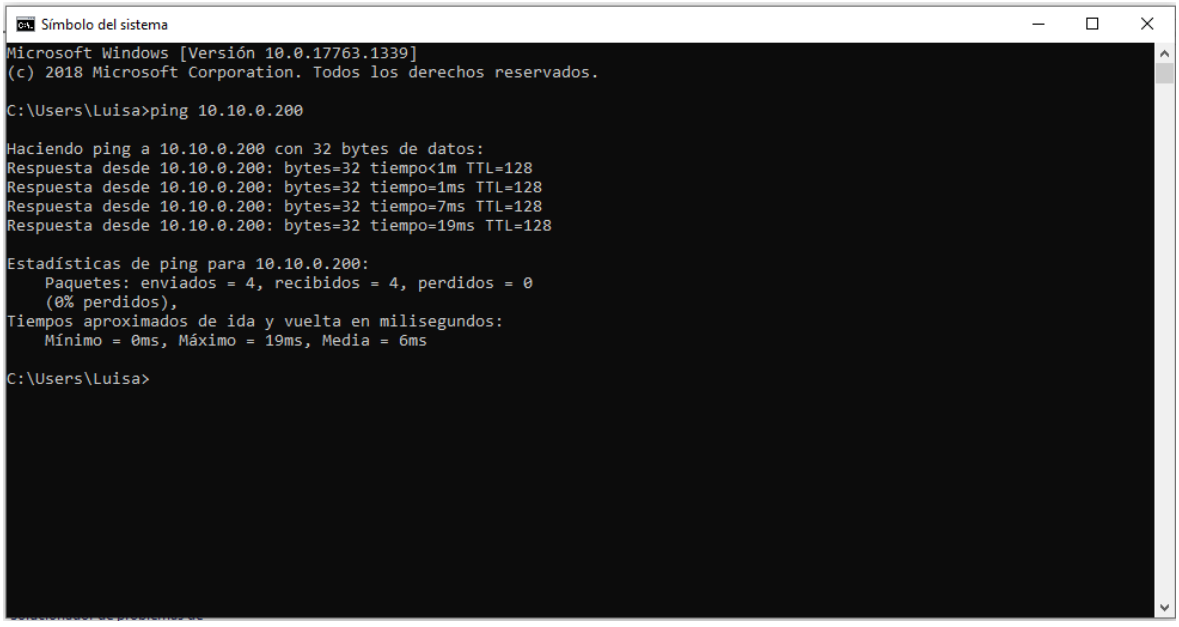


Figure 26. Comunication PC1-> PC2

As in the figure below, you can see the communication between PC2 (10.10.0.200) and PC1 (10.10.0.100).

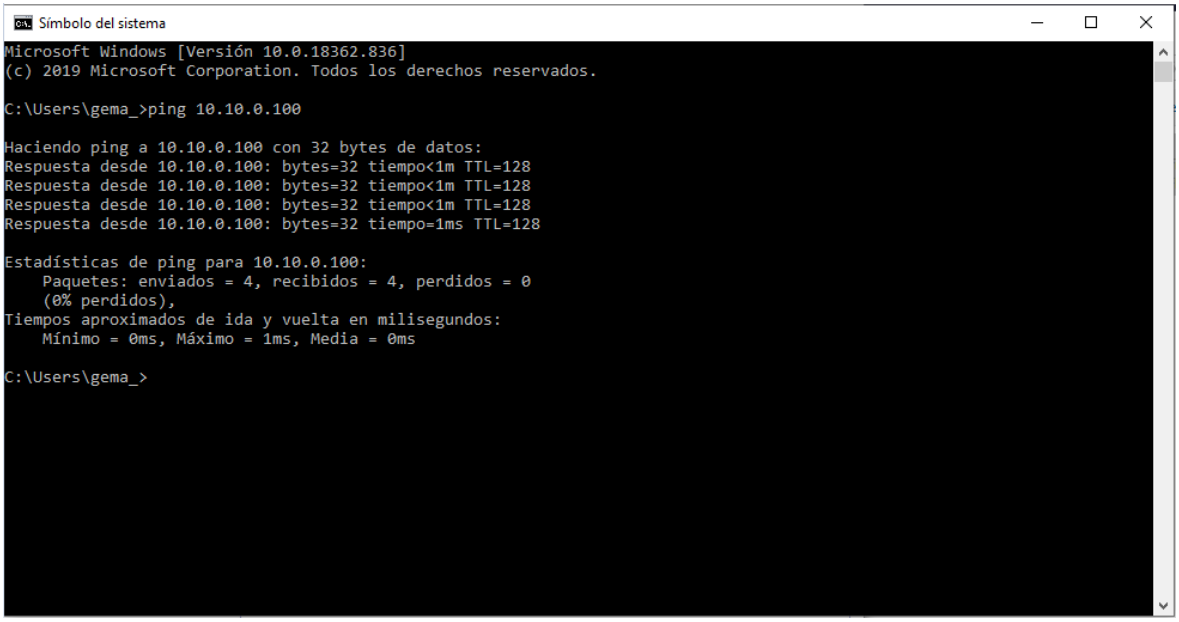


Figure 27. Comunication PC2-> PC1

Once you have the new IP address in VLAN 1 and verified that we have connectivity between the switch ports being in the same VLAN, three more VLANs will be created. VLAN 2 will have the address range 10.20.0.0/25, VLAN 3 will host the address range 10.30.0.0/25, and lastly, VLAN 4 will contain addresses in the range 10.40.0.0/25.

To create the new VLANs, go to the VLAN MANAGEMENT -> CREATE VLAN section and click on ADD VLAN.

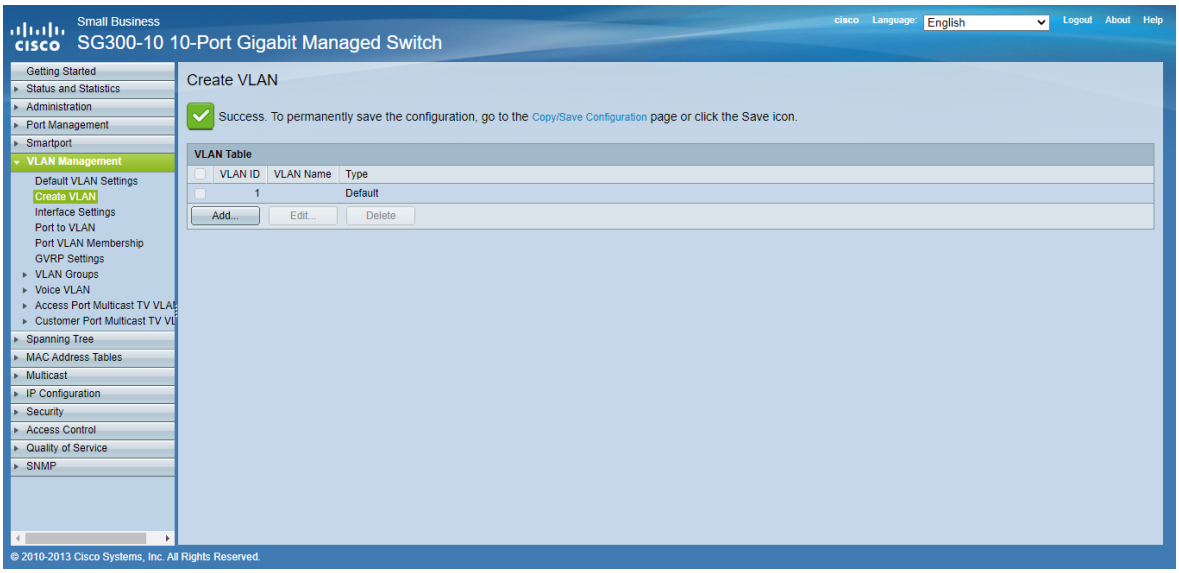


Figure 28. Add VLAN

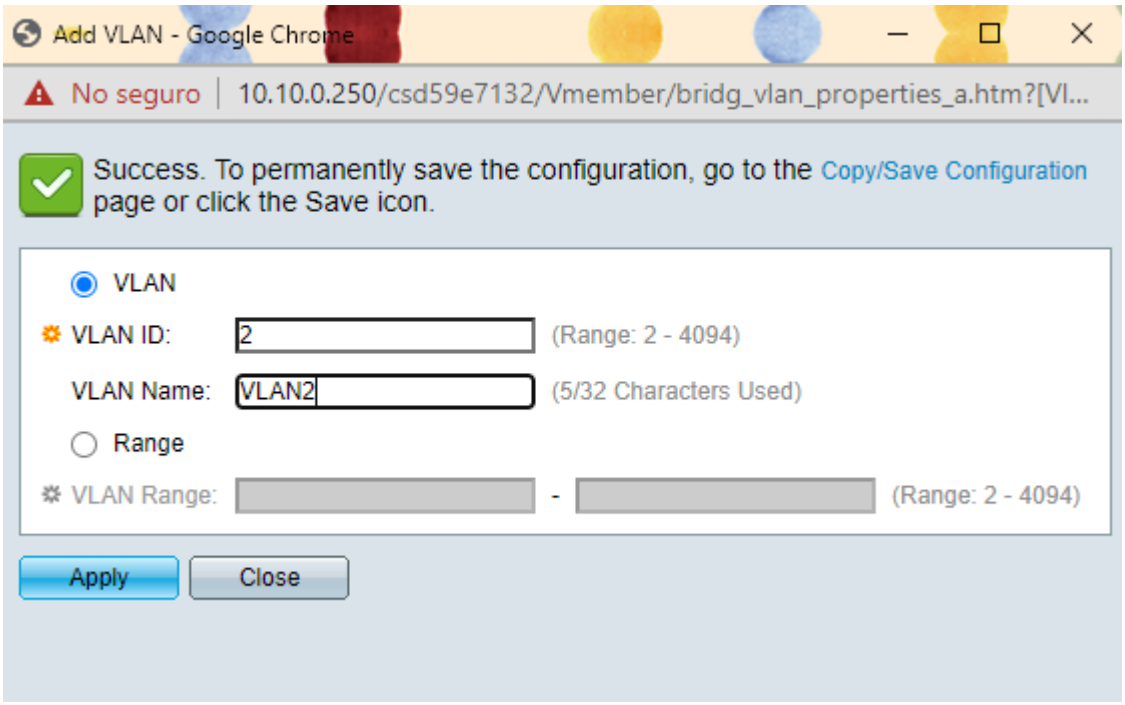


Figure 29. Add VLAN2

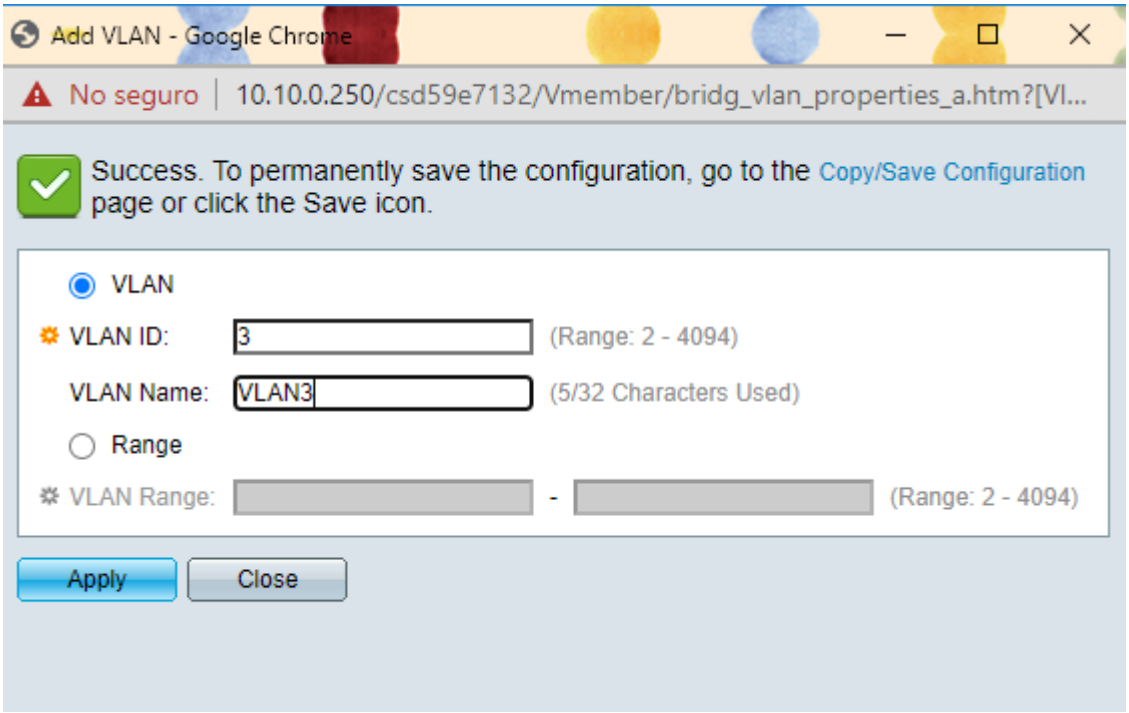


Figure 30. Add VLAN3

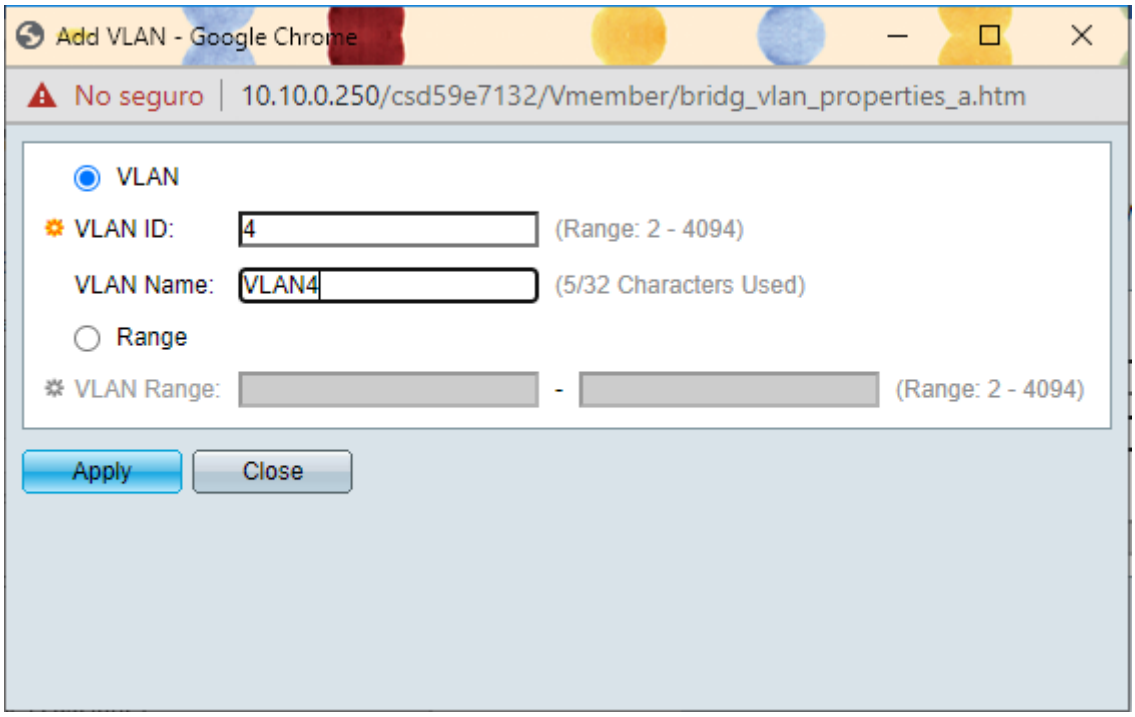


Figure 31. Add VLAN4

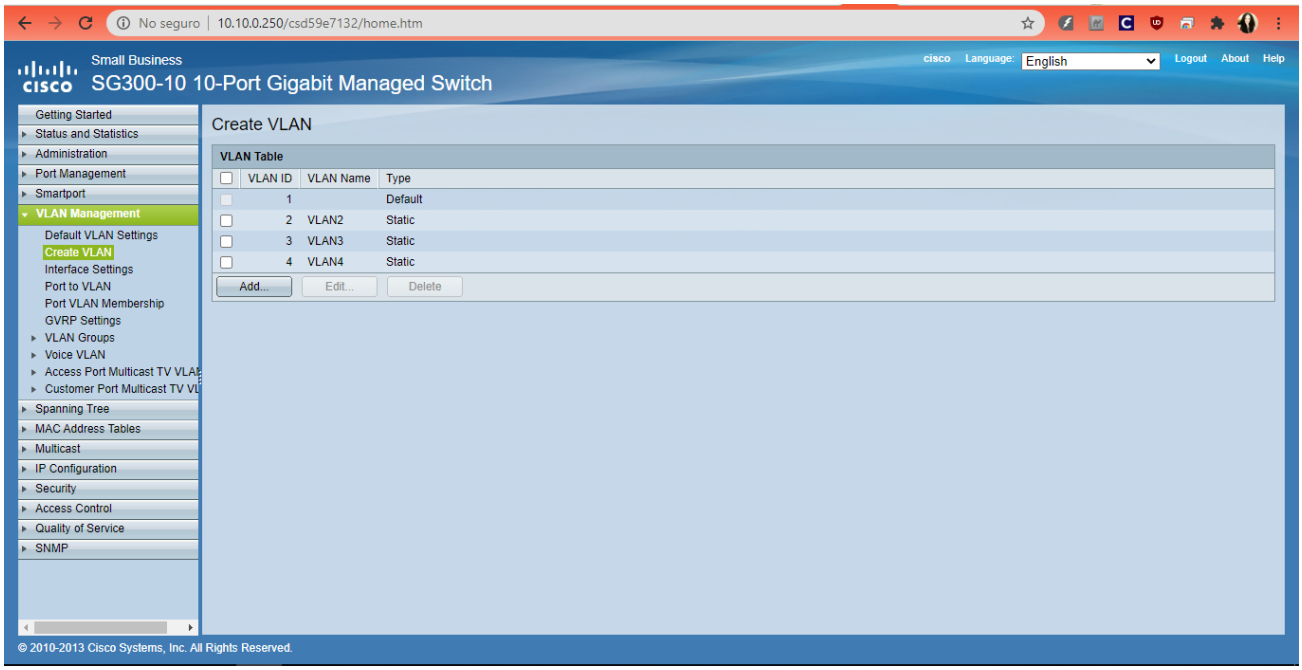


Figure 32. Add de 4 VLAN

Next, the switch ports will be assigned to the different VLANs. For this, the following provision will be followed:

- Port 1 -> Vlan1 in TRUNK mode
- Port 2 -> Vlan1 in TRUNK mode
- Port 3 -> Vlan2 in ACCESS mode
- Port 4 -> Vlan2 in ACCESS mode

- Port 5 -> Vlan3 in ACCESS mode
- Port 6 -> Vlan3 in ACCESS mode
- Port 7 -> Vlan4 in ACCESS mode
- Port 8 -> Vlan4 in ACCESS mode
- Port 9 -> Vlan1 in TRUNK mode
- Port 10 -> Vlan1 in TRUNK mode

From now on, VLAN 1 will be used for common equipment in the company, such as servers, routers, switches, printers, etc. However, the other VLANs will each correspond to teams from a different department.

To configure the ports that belong to each VLAN, click on Vlan Management -> Port to Vlan and the ports that belong to the selected Vlan are marked as untagged.

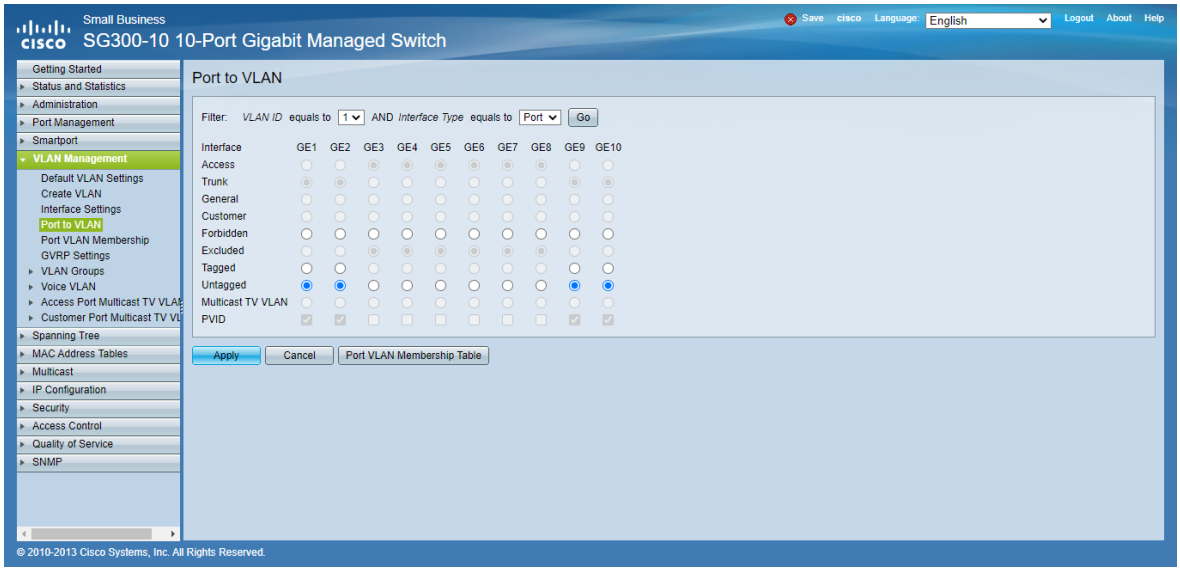


Figure 33. Port selection for VLAN1

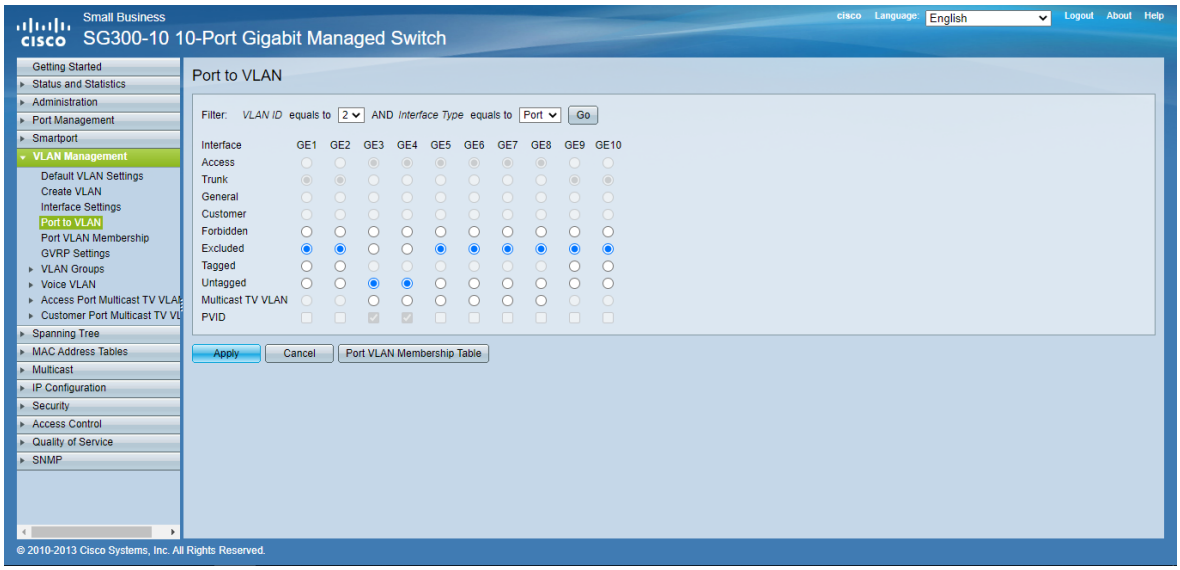


Figure 34. Port selection for VLAN2

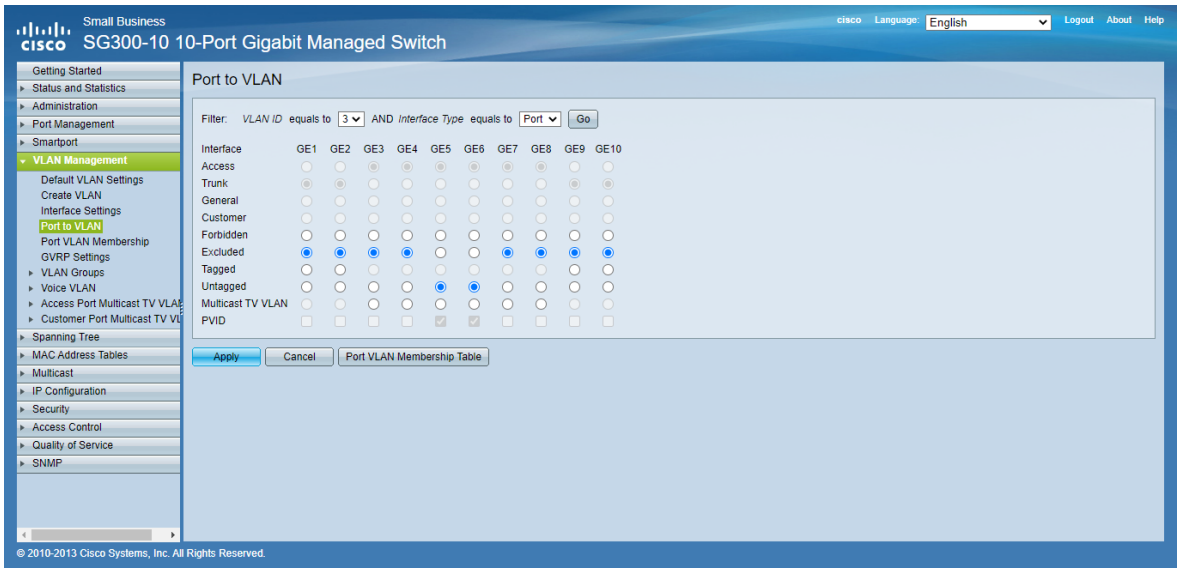


Figure 35. Port selection for VLAN3

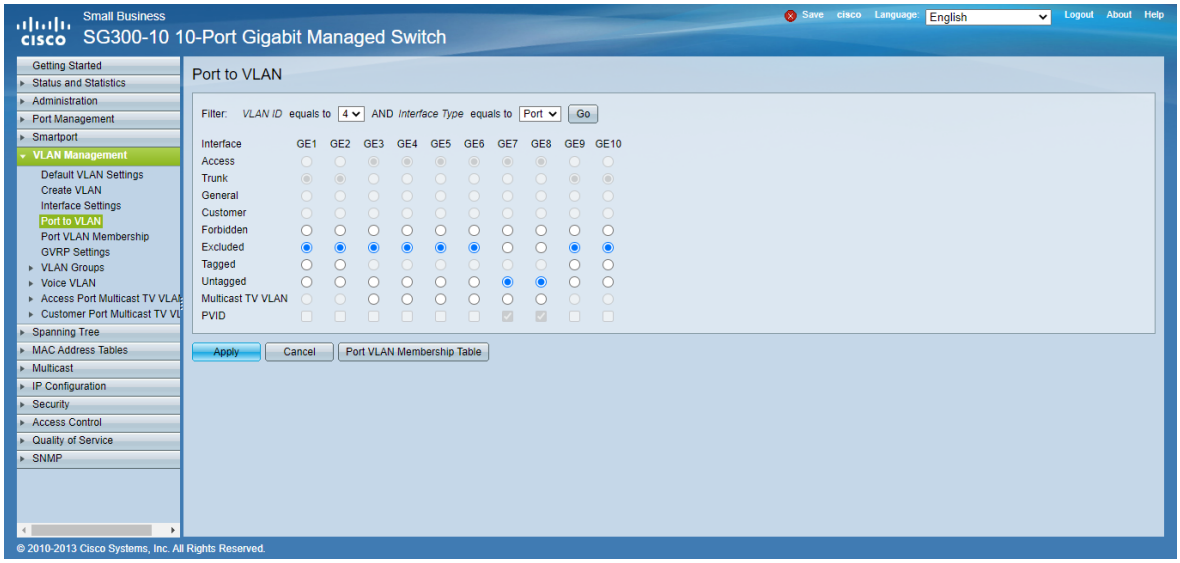


Figure 36. Port selection for VLAN4

To configure the ports in Access mode, you must access VLAN Management -> Interface Settings and select the port to edit. Next, press EDIT and select ACCESS mode.

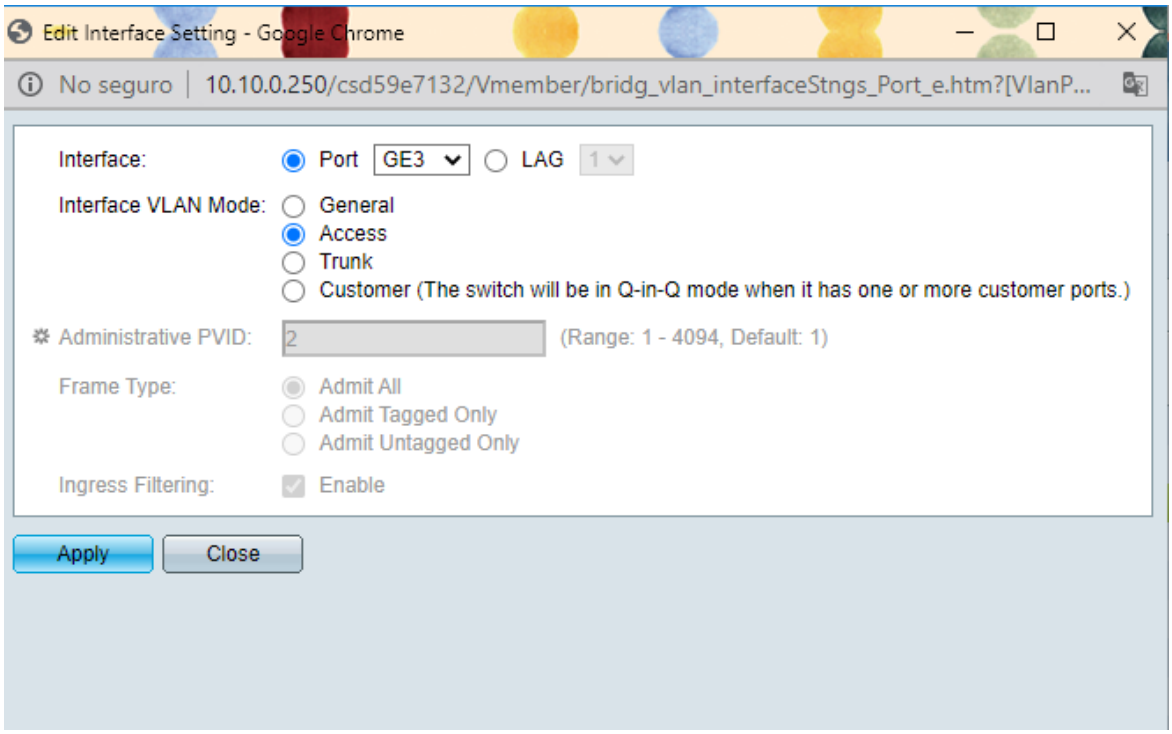


Figure 37. Access mode selection

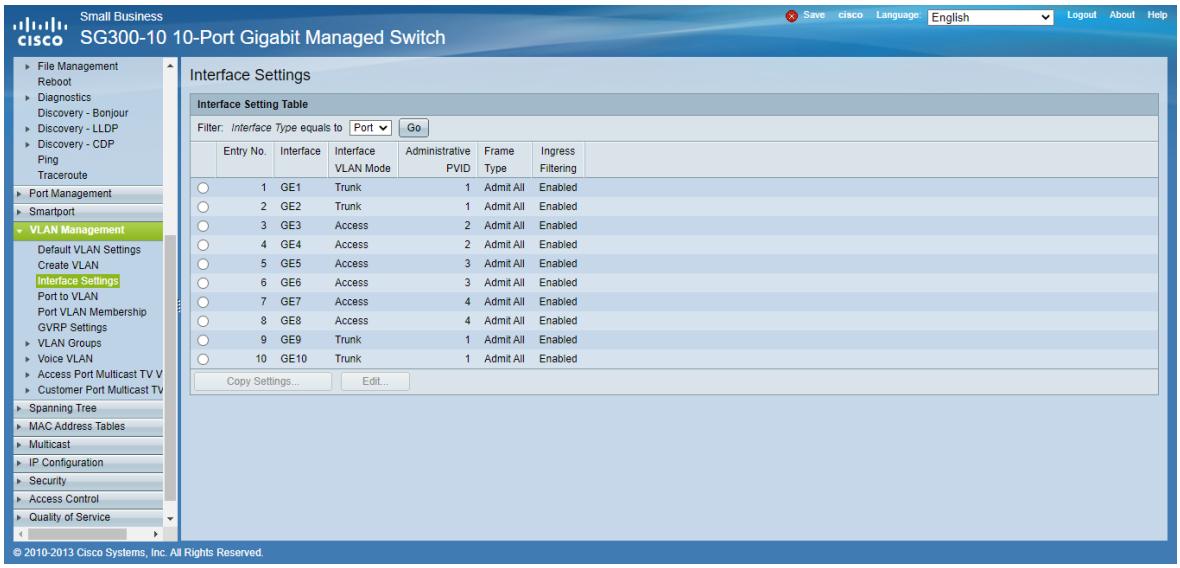


Figure 38. Port configuration

In the following figures, it can be seen that there is no communication between the PC1 equipment hosted in VLAN2 and the PC2 equipment hosted in VLAN3.

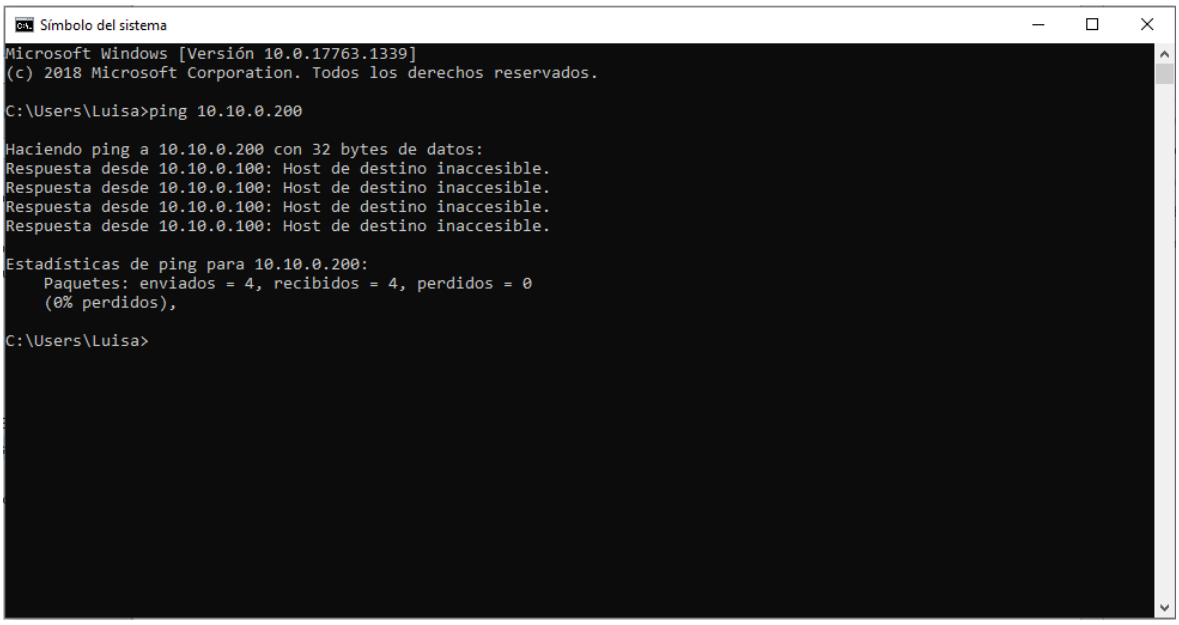


Figure 39. Host unreachable on different Vlan

6.1.2 Port security

Next, security will be configured on the port using MAC, making the switch filter the devices that try to connect and allow only connections from devices that have their MAC stored.

It will be shown as the device with MAC 84: 7b: eb: 1e: 25: a0 is allowed to connect to the GE2 port, while if we connect another PC to that port, the connection is not allowed.

To make the configuration, it is going to indicate that the GE2 port is a secure port, for this, click on Port Management -> Port Settings and indicate that the port is secure.

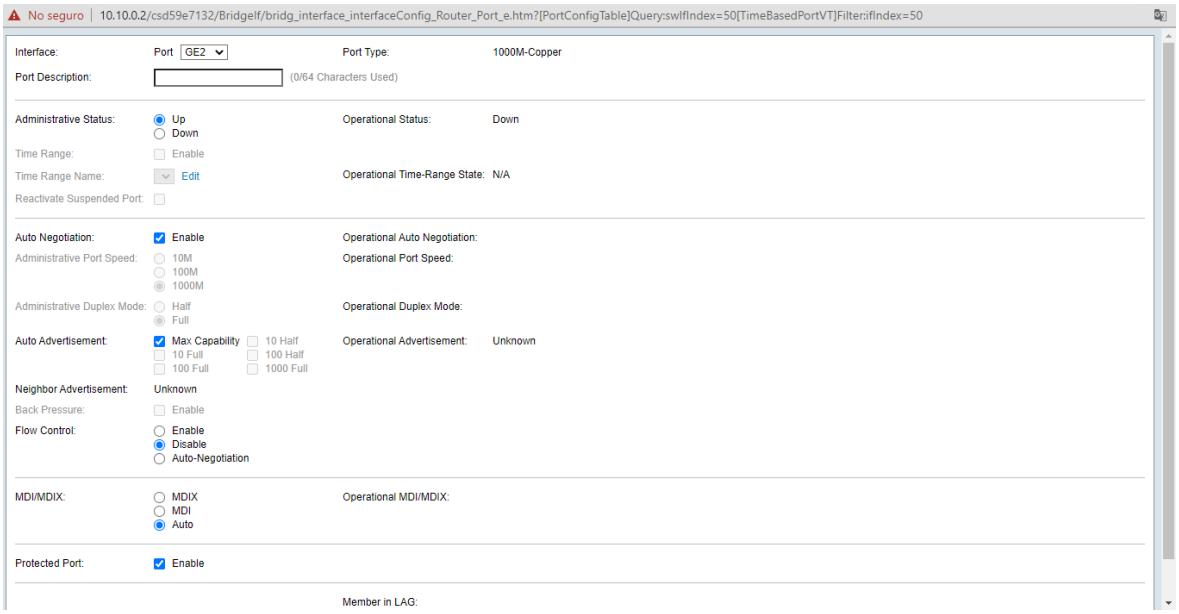


Figura 40. Port secure

This will make the GE2 port appear safe.

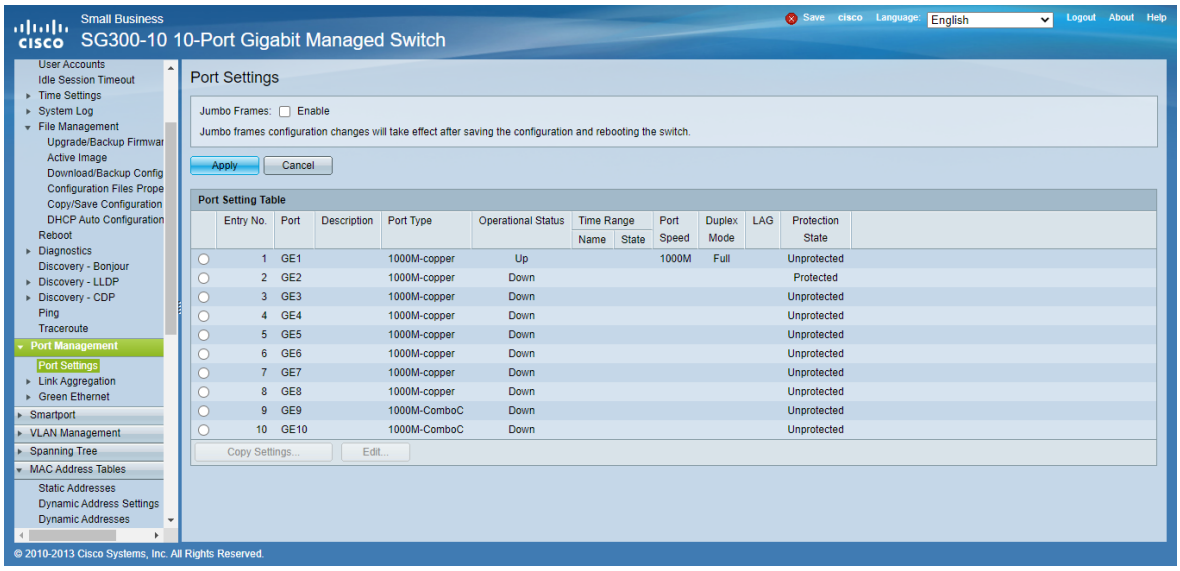


Figure 41. Port secure

The affected ports are then configured in Security> Port Security.

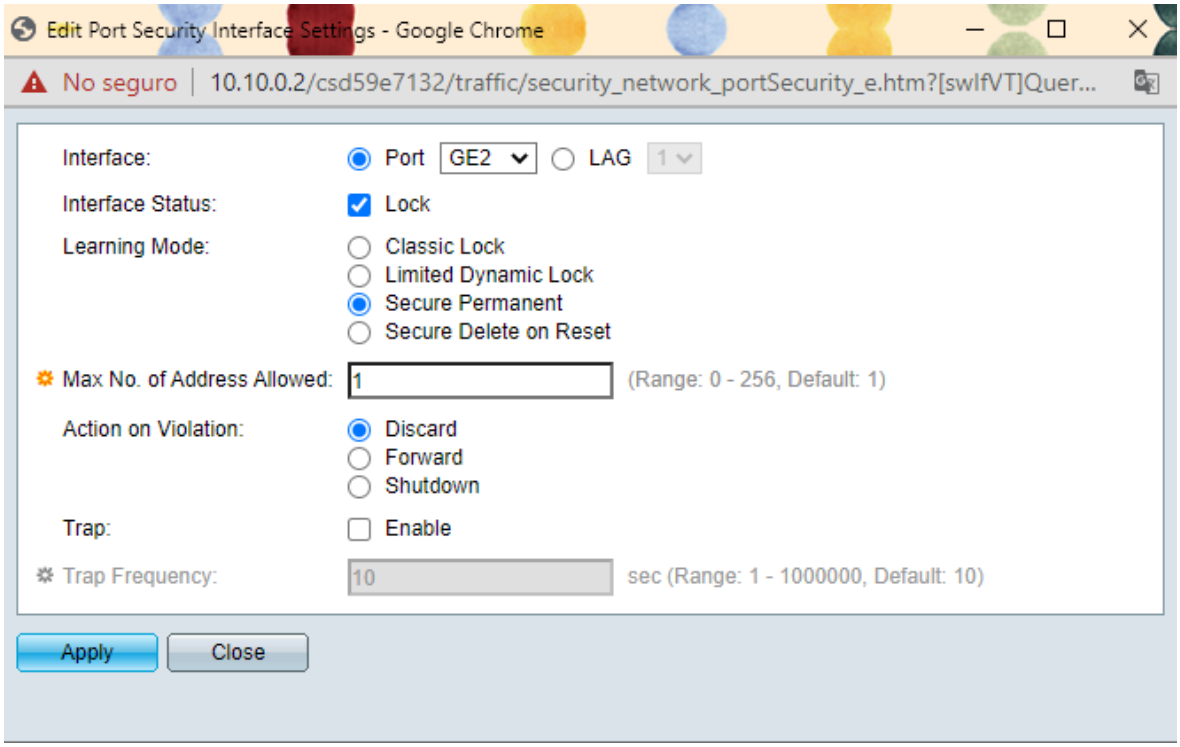


Figure 42. Port security

Obtaining the following configuration:

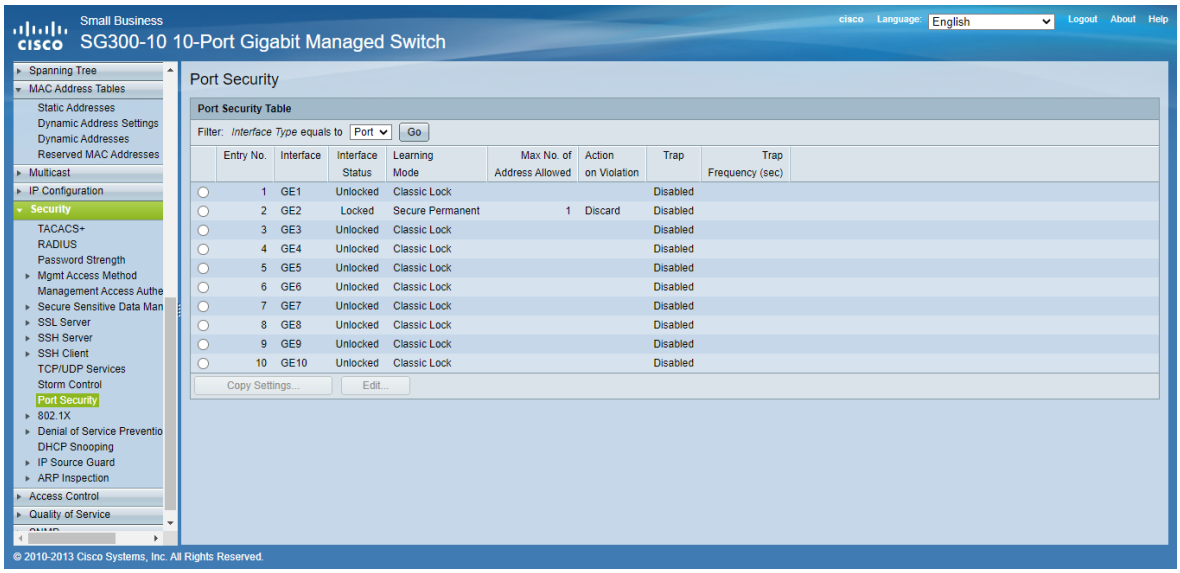


Figure 43. Port security

Finally, the MAC of the allowed equipment is included. This configuration is carried out in the MAC Address Tables -> Static Addresses -> ADD section.

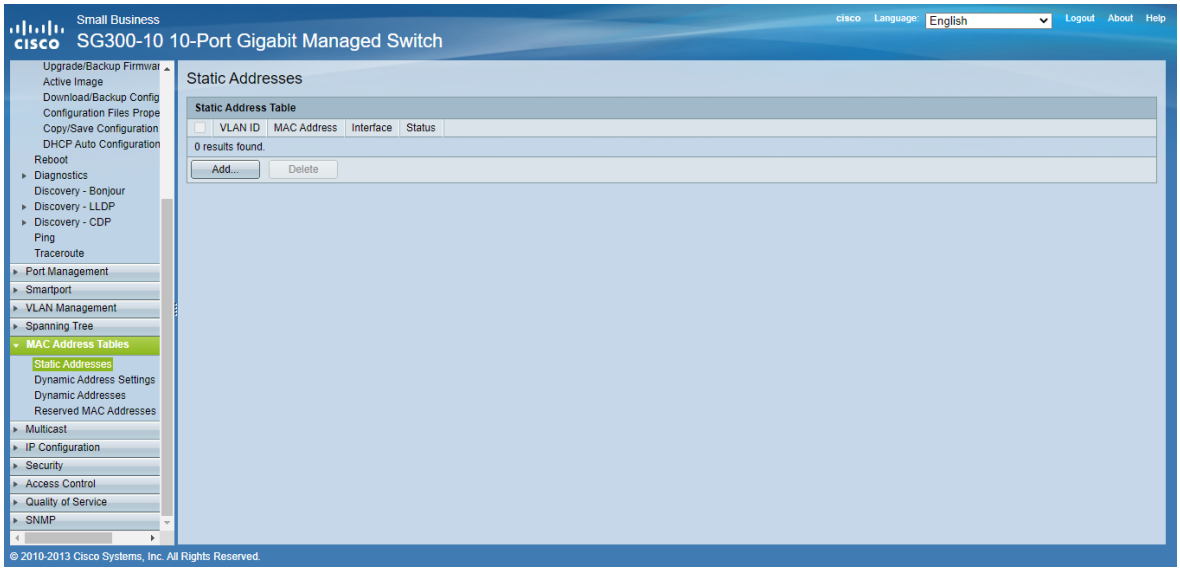


Figure 44. Configure Static Addresses

The MAC of the allowed device is added and the port for which it is the permission is indicated. Finally, the SECURE option is chosen.

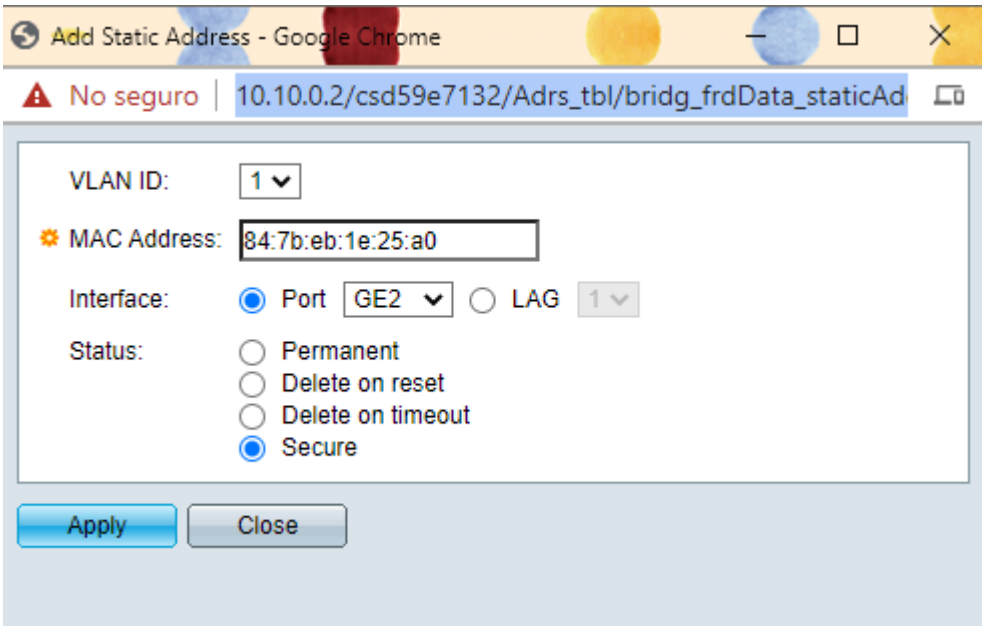


Figure 45. MAC allowed

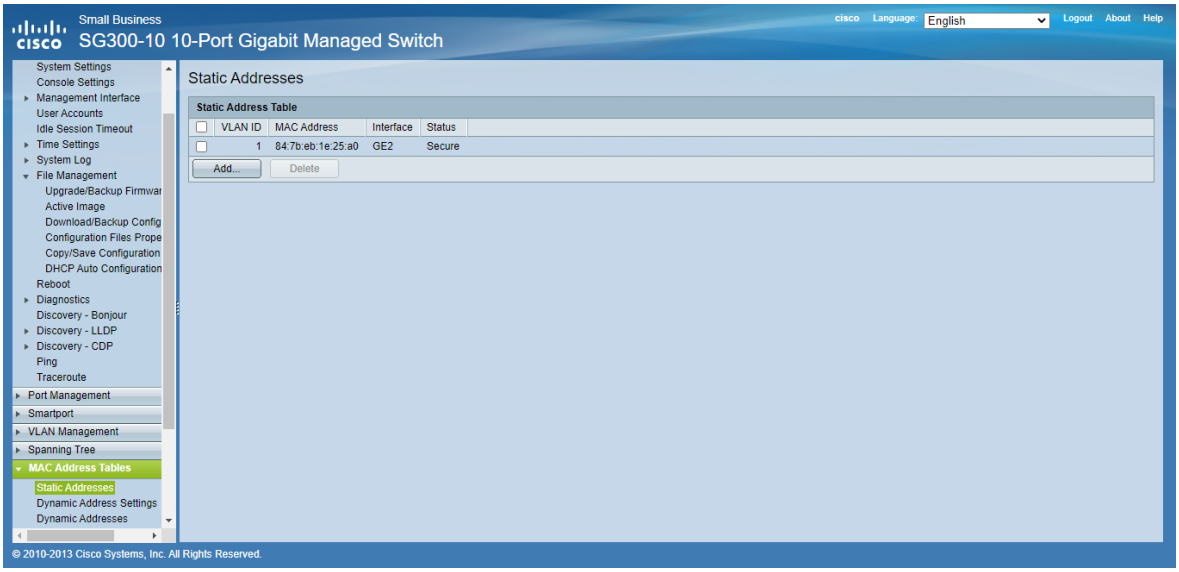


Figure 46. MAC allowed

Thus, MAC 84: 7b: eb: 1e: 25: a0 is allowed for interface GE2.

The test has been done connecting another device to the GE2, and it does not have access to the DHCP of the network and with a fixed IP it cannot access the network either. So the setup works.

6.1.3 DHCP Snooping

DHCP snooping provides a network security mechanism to avoid receiving false DHCP response packets and registering false addresses. To do this, the device ports will be classified as trusted or untrusted.

First, the interfaces are going to be marked as trusted. To do this, click on IP configuration -> DHCP Snooping / Relay -> DHCP Snooping Trusted Interfaces.

Interface GE1 is chosen as Trusted Interface.

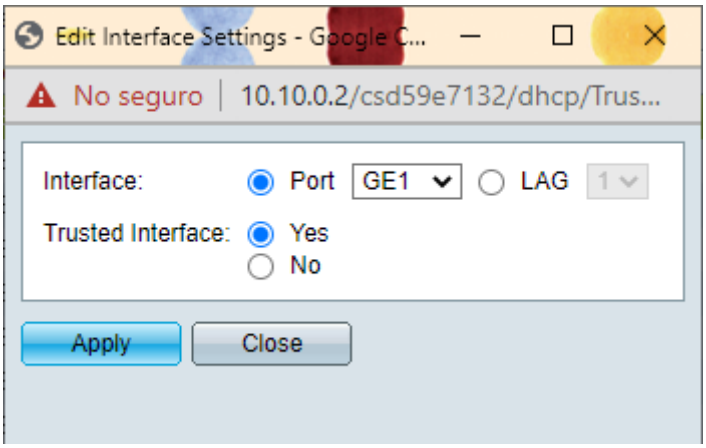


Figure 47. Trusted Interface

Obtaining the following result:

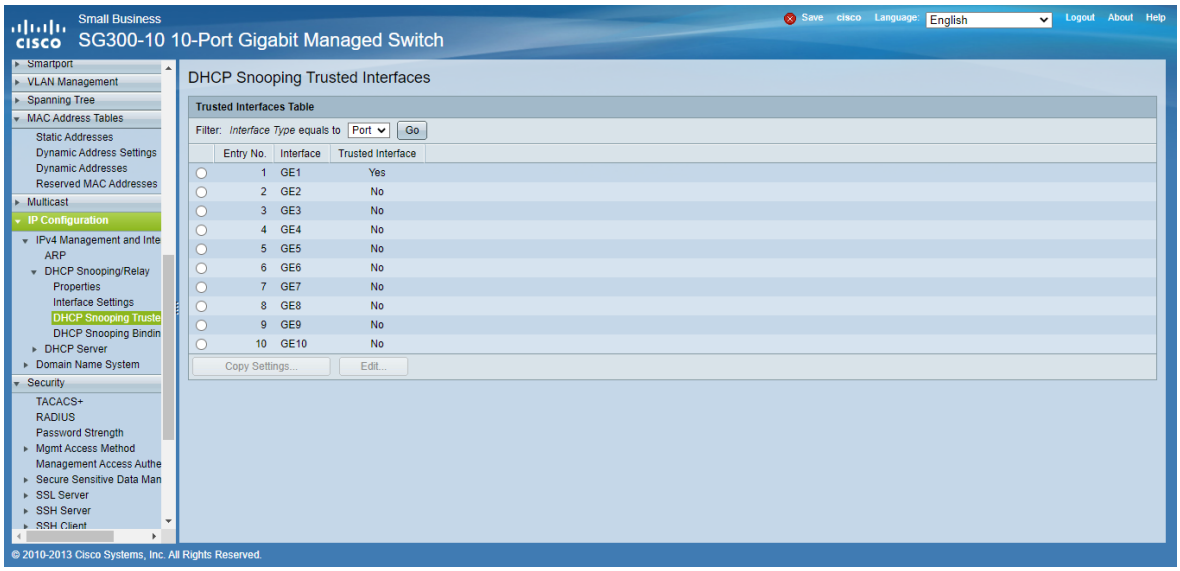


Figure 48. Trusted Interface

Next, we activate DHCP Snooping. For this configuration, click on IP configuration -> DHCP Snooping / Relay -> Propierties.

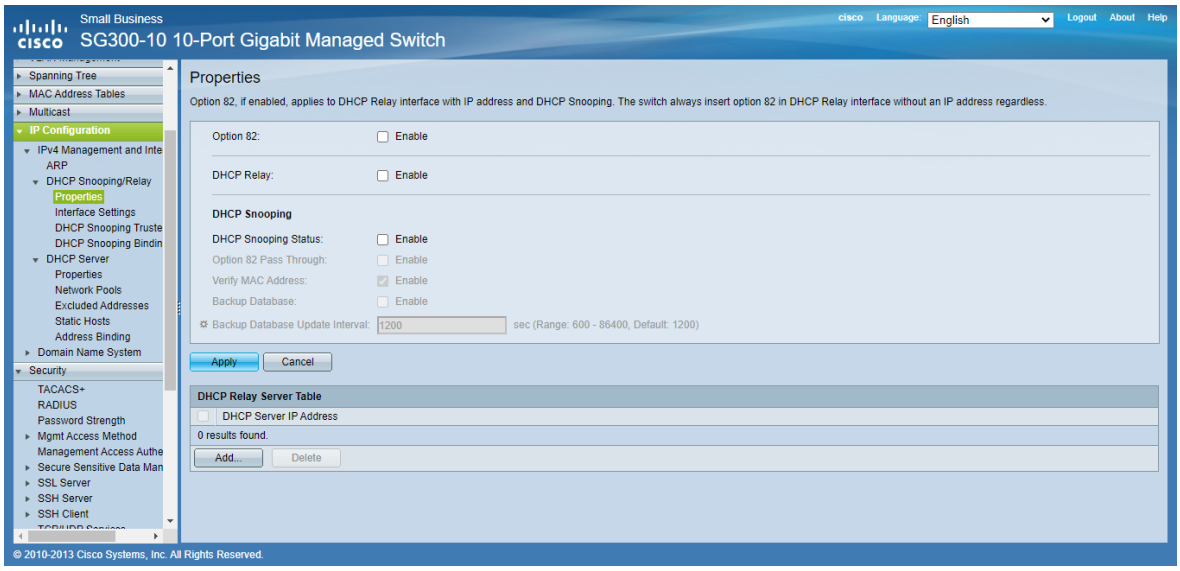


Figure 49. DHCP Snooping

First, Option 82 will be marked as enable. This option will protect the switch from attacks such as IP or MAC address spoofing. This provides information about the actual location of the DHCP server, the name of the Vlan where it is located and the remote ID or MAC address of the DHCP packet header.

Also, the DHCP relay field will be checked so that DHCP relay is enabled throughout the switch.

Finally, the DHCP Snooping field will be enabled.

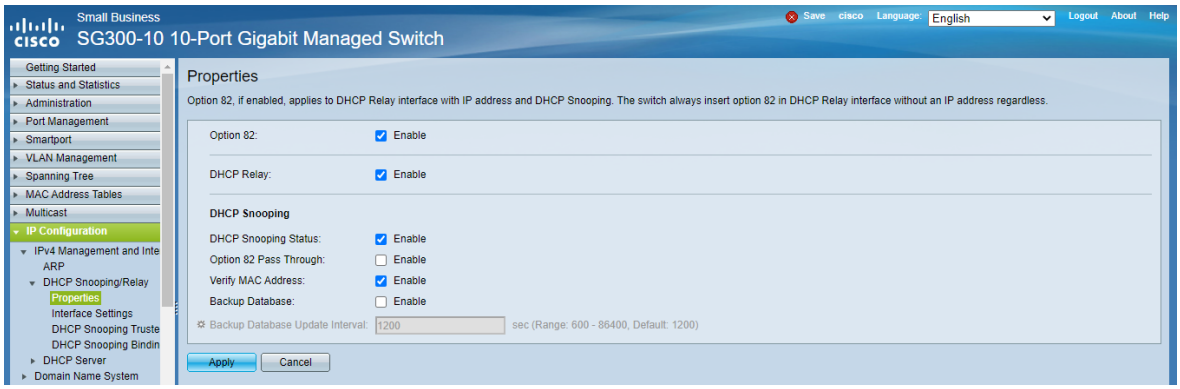


Figure 50. DHCP Snooping

The following is the existing DHCP server on the network. In this case, the server is included in the RV320 router on the network.

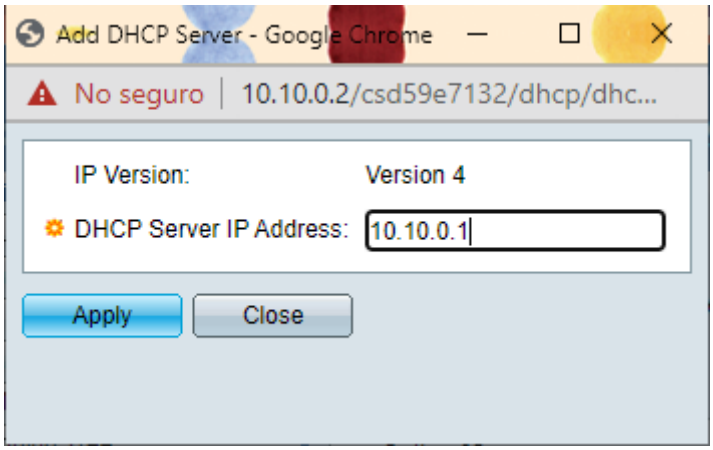


Figure 51. DHCP Server IP Address

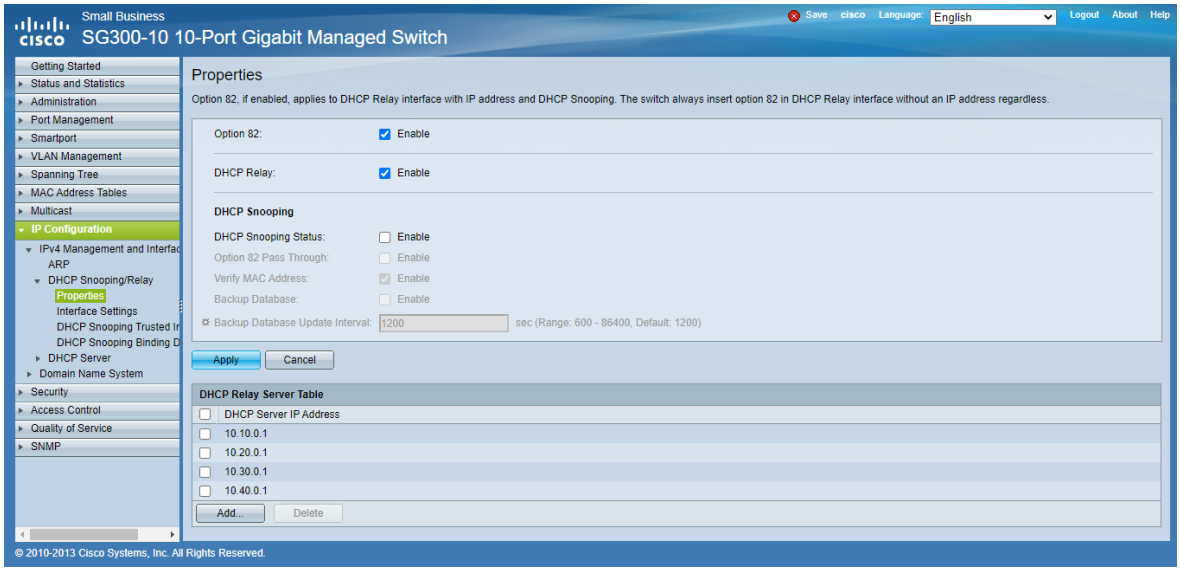


Figure 52. DHCP Server

Click on IP Configuration -> DHCP Snooping / Relay -> Interface settings. At this point, the interfaces on which the DHCP server can act will be enabled.

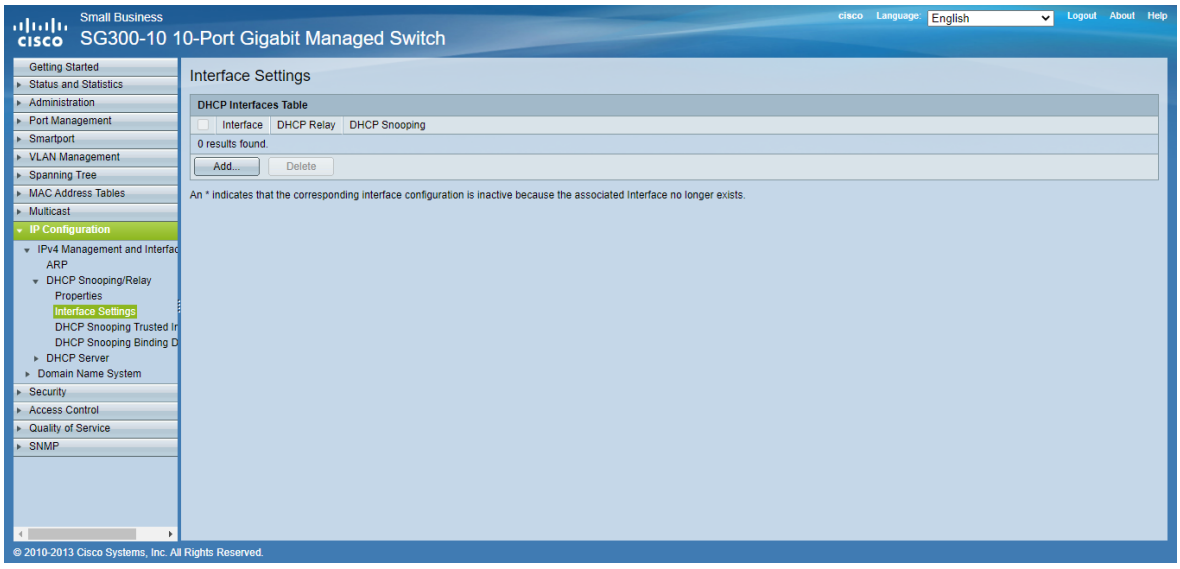


Figure 53. Interface settings

The allowed Vlans are chosen for each DCHP Server.

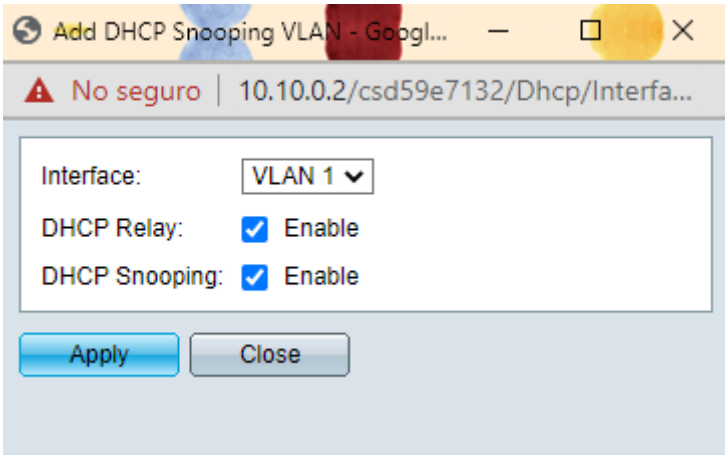


Figure 54. DHCP Relay and Snooping

Below are the Vlans, in which DHCP relay and DHCP Snooping have been activated.

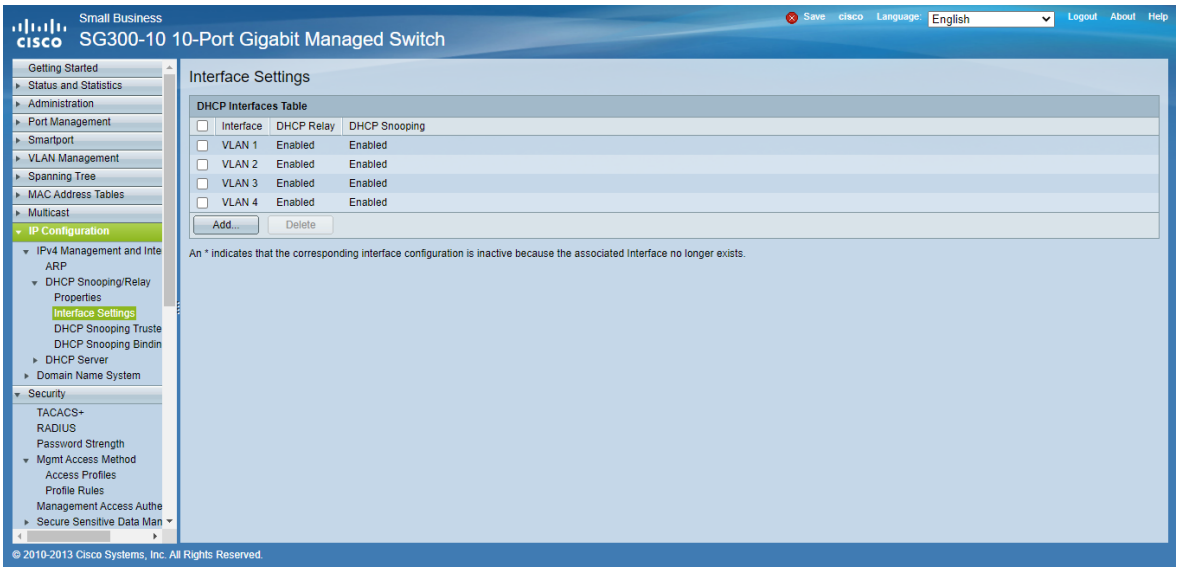


Figure 55. Vlan DHCP Relay and Snooping

In the following figure, we can verify that the DHCP server is giving IP to the computer connected to the switch.

Figure 56. DHCP IP

6.1.4 IP source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on manually configured IP or DHCP snooping binding database. This feature helps prevent IP spoofing attacks when one host tries to spoof and use the IP address of another host. Any IP traffic entering the interface with a source IP address other than the one assigned (via DHCP or static configuration) will be rejected.

The IP Source Guard feature is used in conjunction with the DHCP Snooping feature on Layer 2 interfaces that are not trusted. Creates and maintains a source IP table that it learns using DHCP Snooping or by configuring it manually (static source IPs). The IP Source Binding table stores the IP address and associated MAC and VLAN. IP Source Guard is only supported on Layer 2 ports, including trunk and access ports.

For this configuration, click on Security> IP Source Guard> Binding Database.

First, the retry frequency will be set to 60 sec, therefore, the Ternary Content Addressable Memory (TCAM) will be checked every 60 sec.

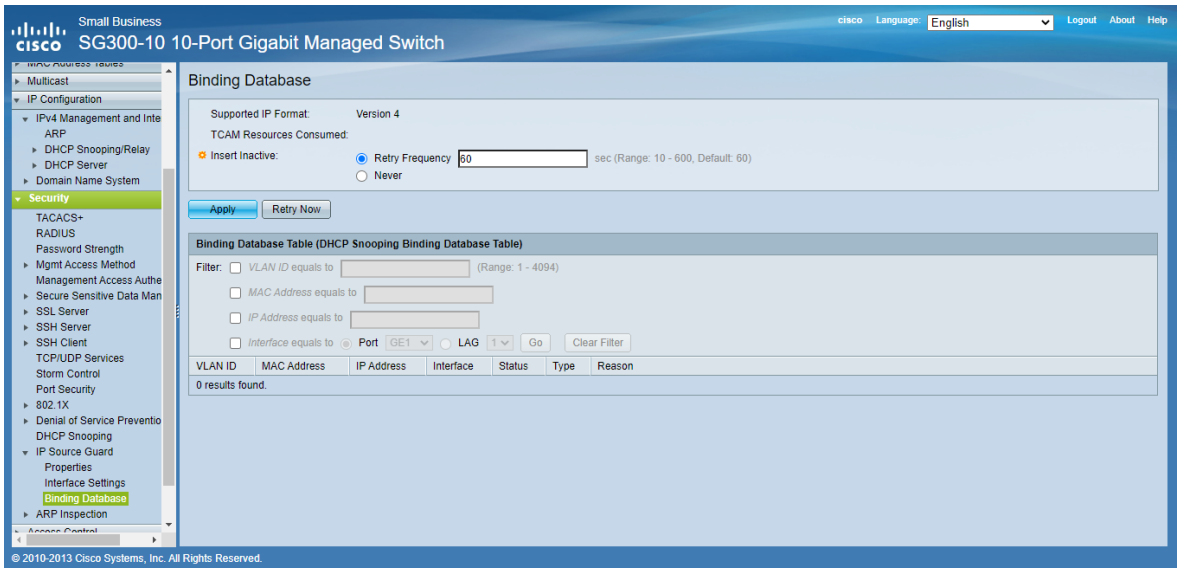


Figure 57. Binding Database

Next, a team will be added to the table. To do this, click on IP Configuration -> DHCP Snooping / relay -> DHCP Snooping Binding and add the equipment.

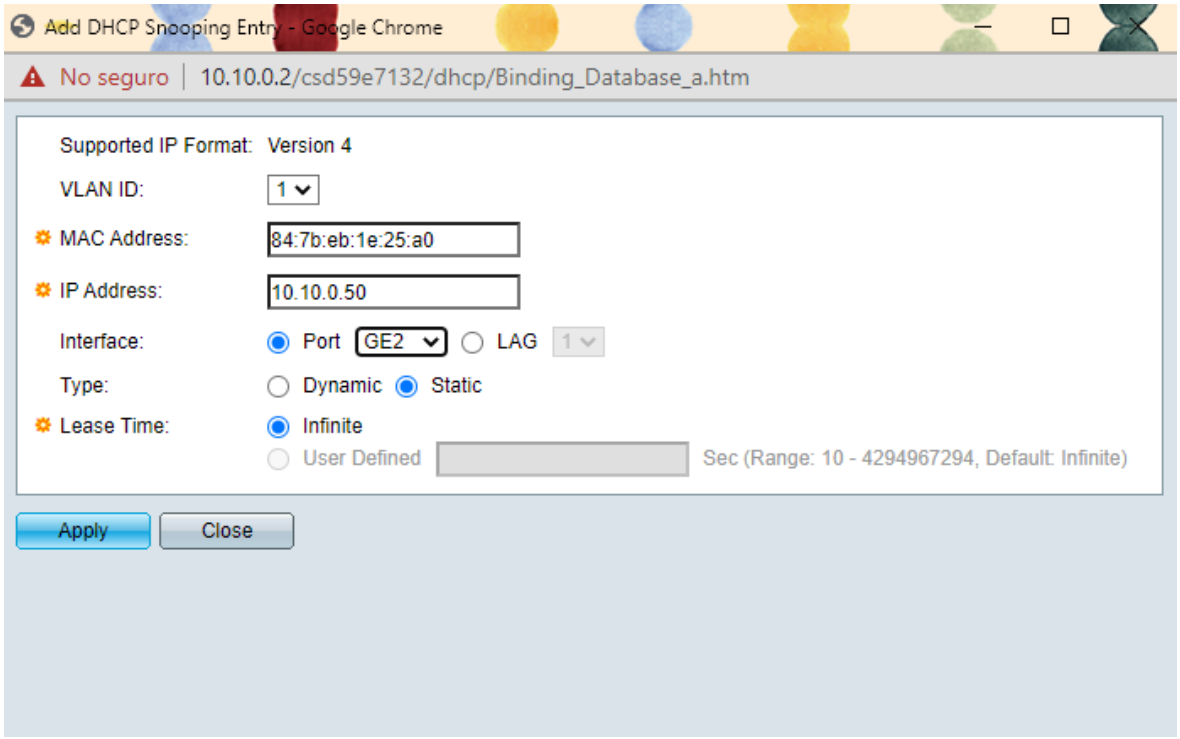


Figure 58. Add trusted PC

The following configuration remains:

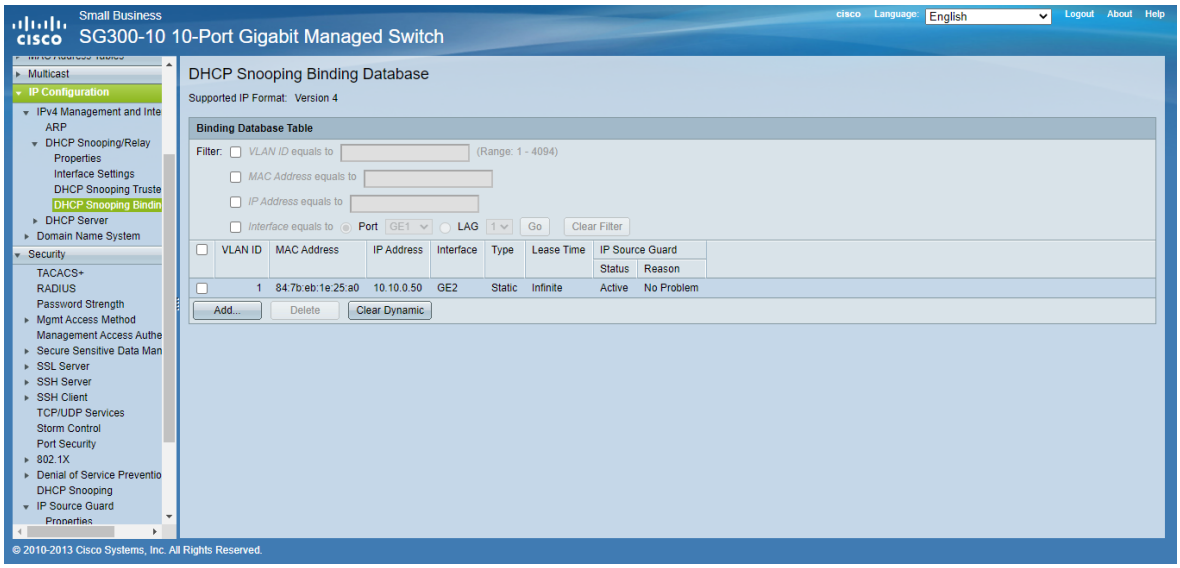


Figure 59. DHCP Snooping Binding Database

In the Reason column it may appear:

- No problem: The interface is active.
- No Snoop VLAN: DHCP Snooping is not enabled on the VLAN.
- Trusted Port: The Port is reliable
- Resource Problem: TCAM check time timed out.

In this case, the equipment is connected without any problem.

It has been verified that by putting a fixed IP 10.10.0.5 on the equipment, different from the one saved, the equipment does not have access to the network.

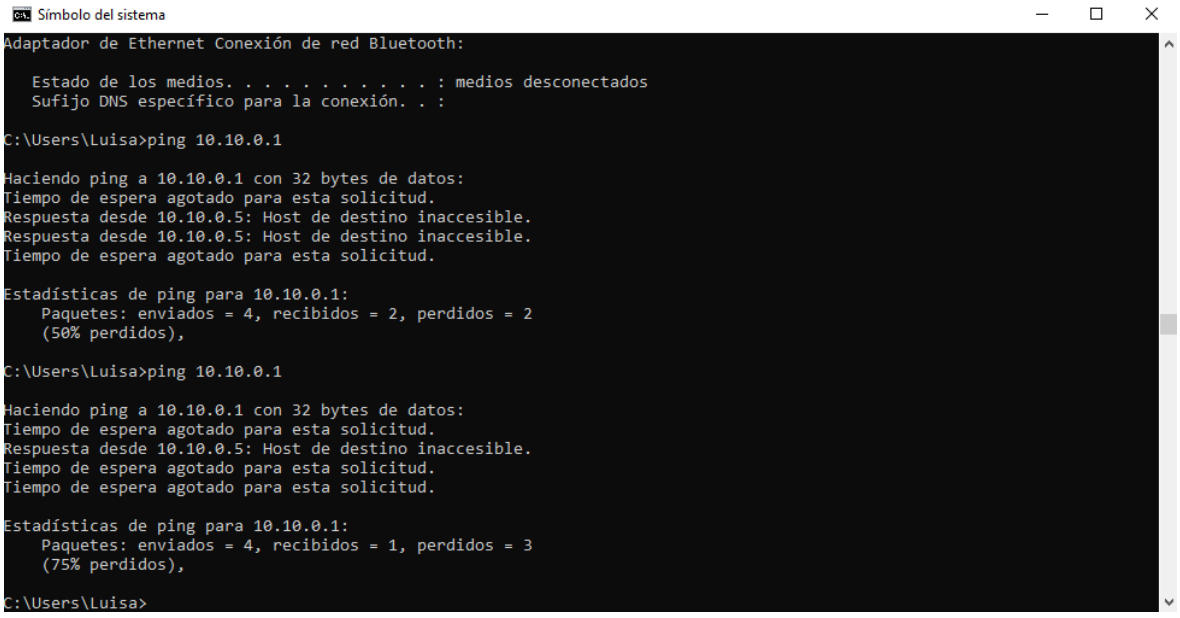


Figure 60.IP untrusted

6.1.5 ARP Inspecction

The Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses. ARP inspection is used to protect a network from ARP attacks. ARP inspection increases traffic security by inspecting packets that are on interfaces defined as untrusted. When a packet reaches an untrusted interface, ARP inspection looks at the source IP address and MAC address of the packet. If they match the IP address and MAC address found in the ARP access control rules, then the packet is forwarded; otherwise, the packet is discarded.

For this configuration, click on Security -> ARP Inspection -> Properties and mark as active.

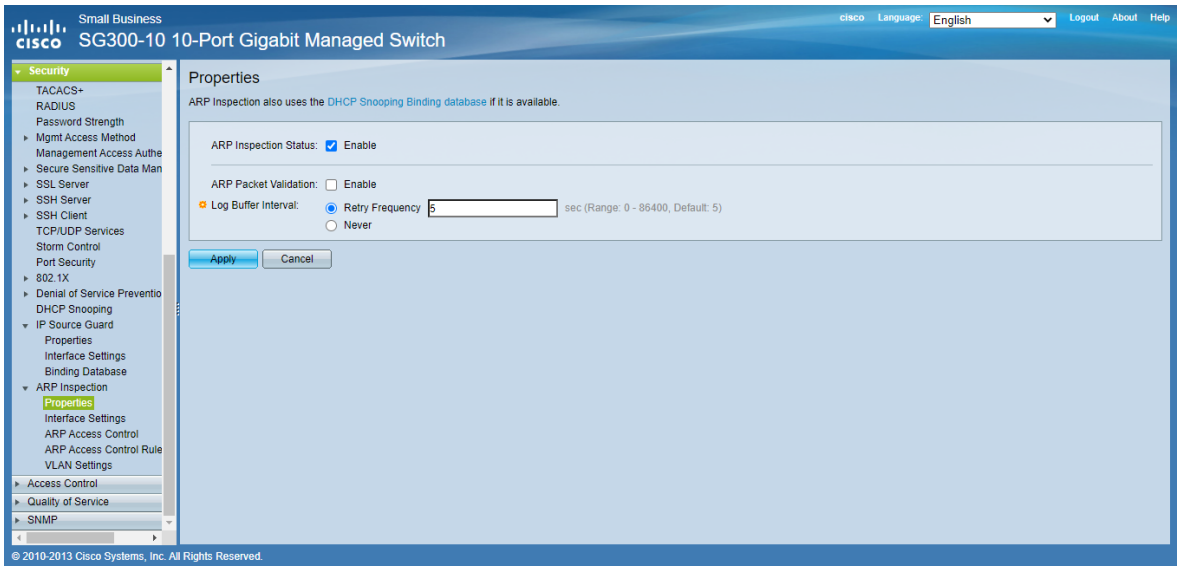


Figure 61. ARP Inspection

Next, click on Security -> ARP Inspection -> ARP Access Control and enter the MAC and IP of the device.

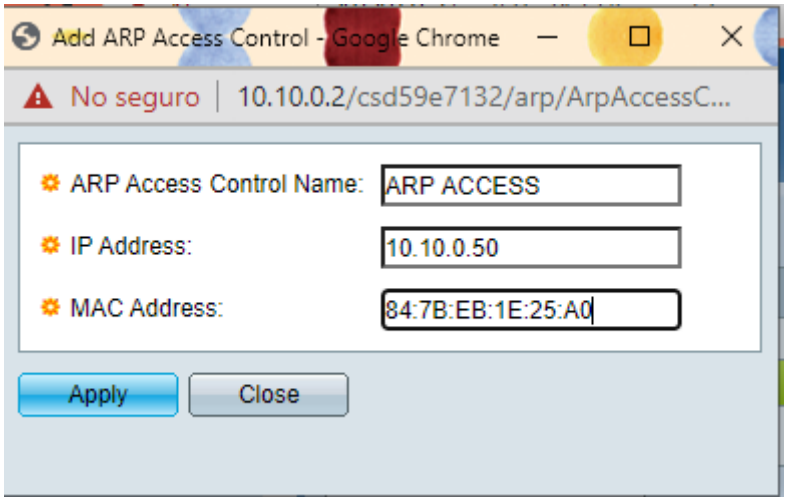


Figure 62. ARP Inspection

Obtaining the following result:

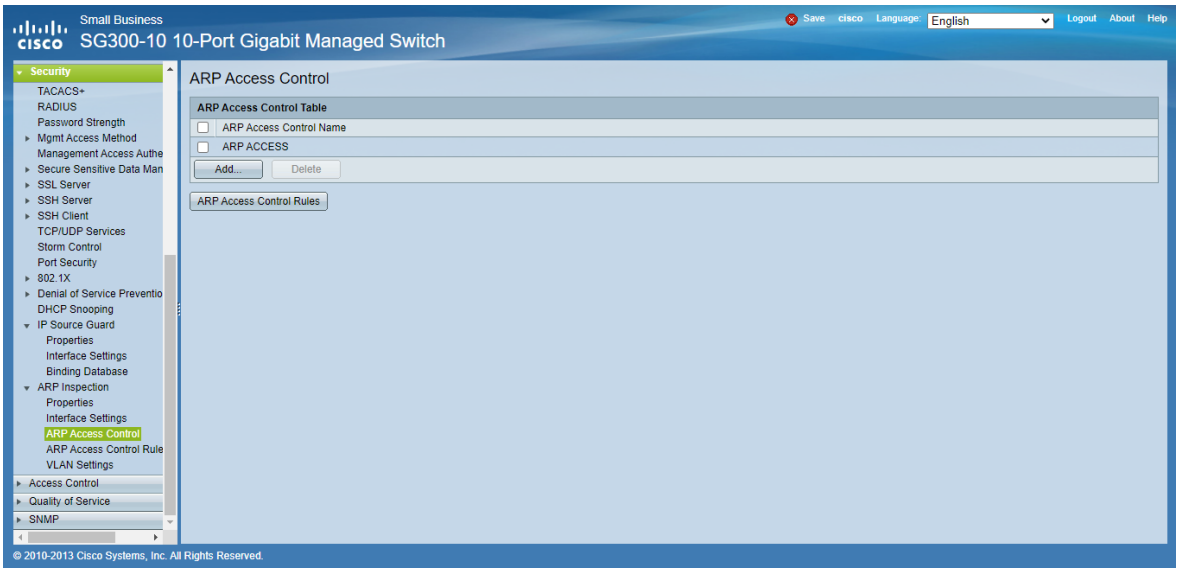


Figure 63. ARP Access Control

Then the rules are added in Security -> ARP Inspection -> ARP Access Control Rules. In our case, it is not necessary, since it was created by default in the previous step, but if we wanted to add more devices in this “ARP ACCESS” rule, it would be done in this step.

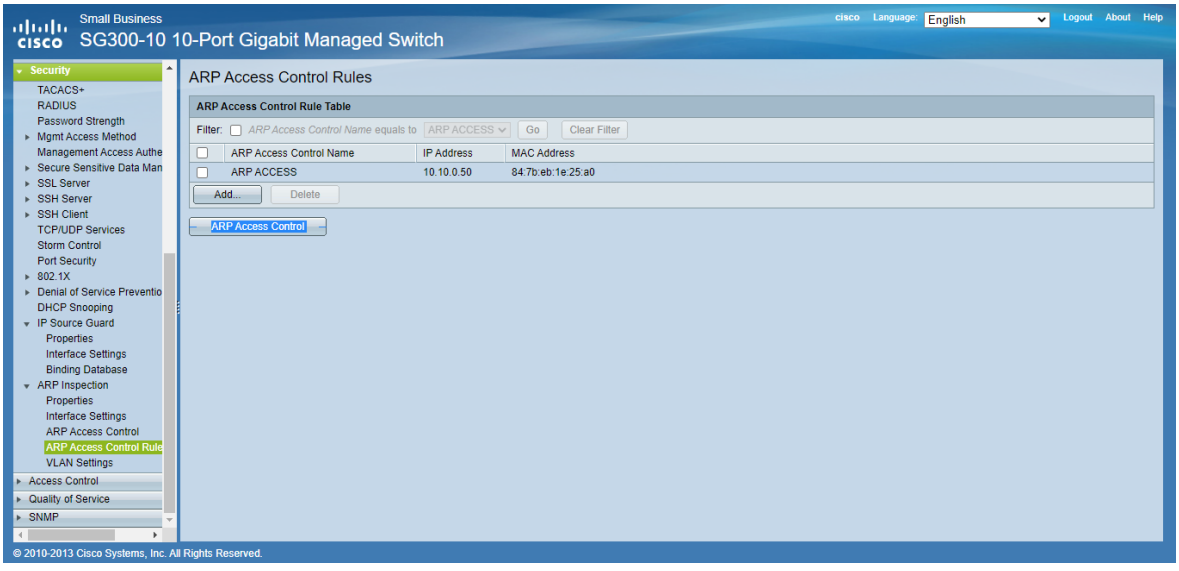


Figure 64. ARP Access Control Rules

Finally, the rule is configured in the VLAN, it can only be assigned one ARP Access Control group per VLAN. Click on Security -> ARP Inspection -> VLAN Settings

VLAN1 is added to the right column and the changes are applied.

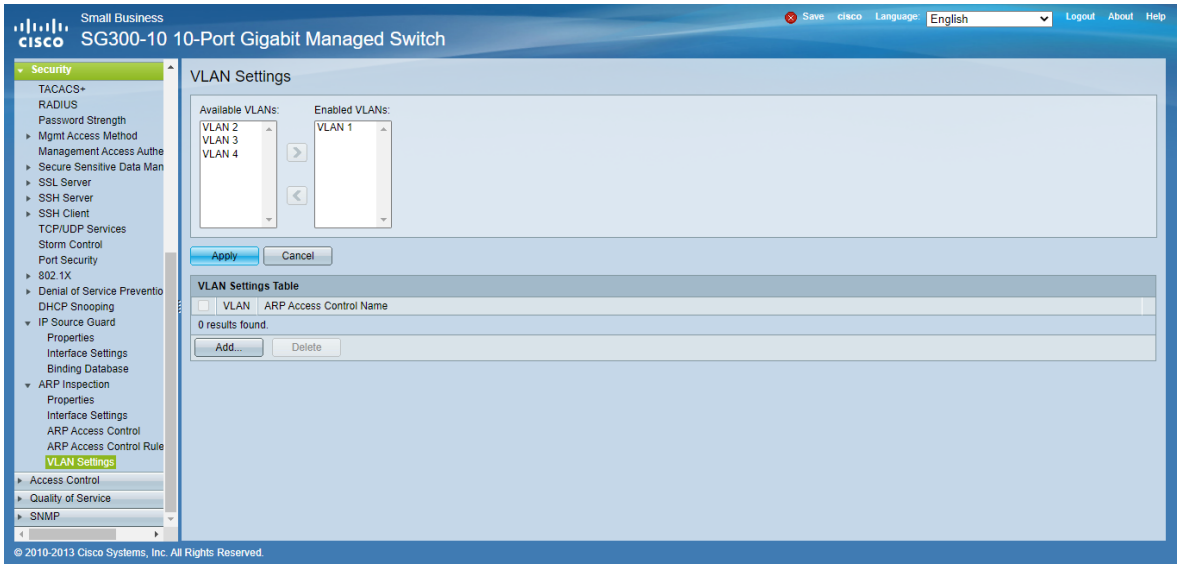


Figure 65. Enabled VLAN

Next, in the VLAN Settings Table, click on ADD and add the Vlan and the rule that was created before.

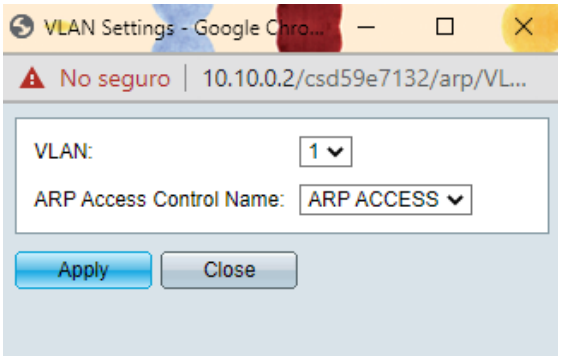


Figure 66. Settings Table

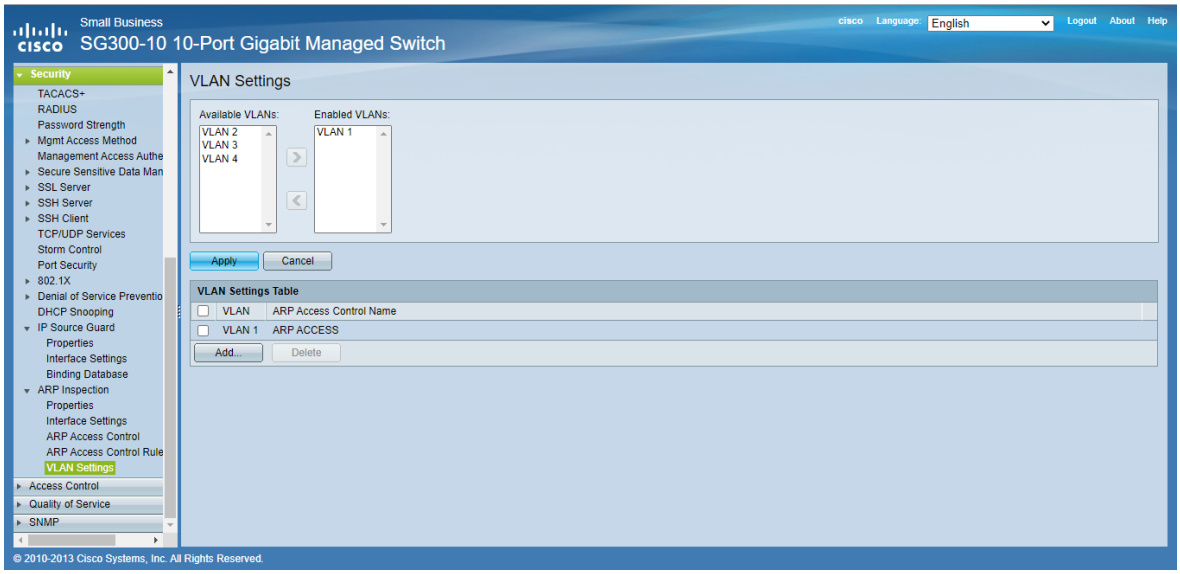


Figure 67. Vlan Settings

Finally, the configuration has been verified and by changing the IP to the equipment, it loses all connectivity with the network.

6.2 Cisco RV320 Gigabit Dual WAN VPN Router Configuration

6.2.1 Configuration Router A

First, the Cisco RV320 Gigabit Dual WAN VPN router has been reset to the factory state. To do this, the Reset button has been held down for a few seconds, causing it to be reset and thus all the device's LEDs turn on for a few seconds.

When the device is in its initial state, it is assigned the IP 192.168.1.1. The IP address of the PC that is going to be used will be configured, for the access and subsequent configuration of the router, so that it takes an IP by DHCP, in this way the router will assign the equipment an IP within the range 192.168.1.x.

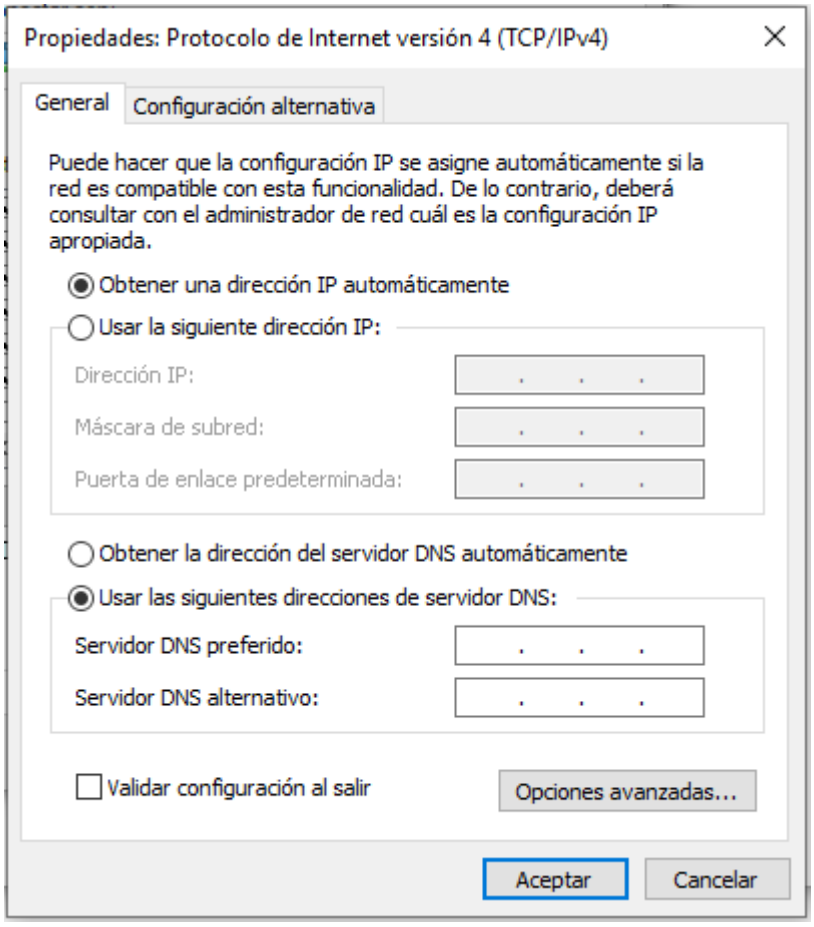


Figure 68. Dynamic IP configuration on the PC

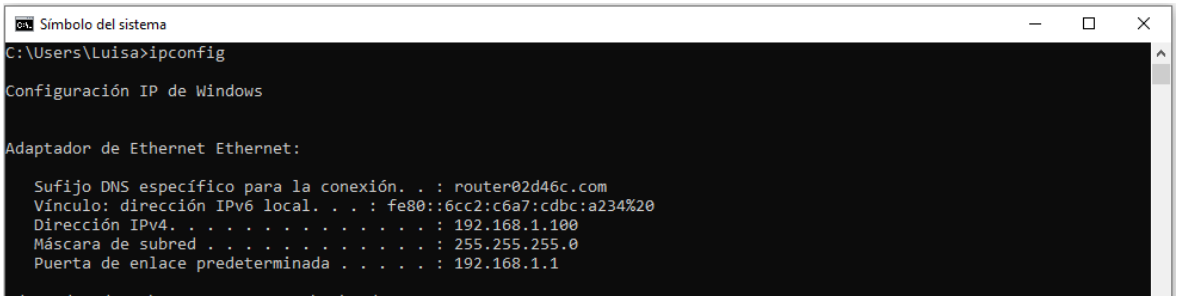


Figure 69. Dynamic IP assignment to PC

The web administrator of the device will be used to configure it, for this reason we will access the equipment through a web browser, entering the IP 192.168.1.1 in the address bar.

Next, we will introduce the default username and password, which is cisco in both cases.

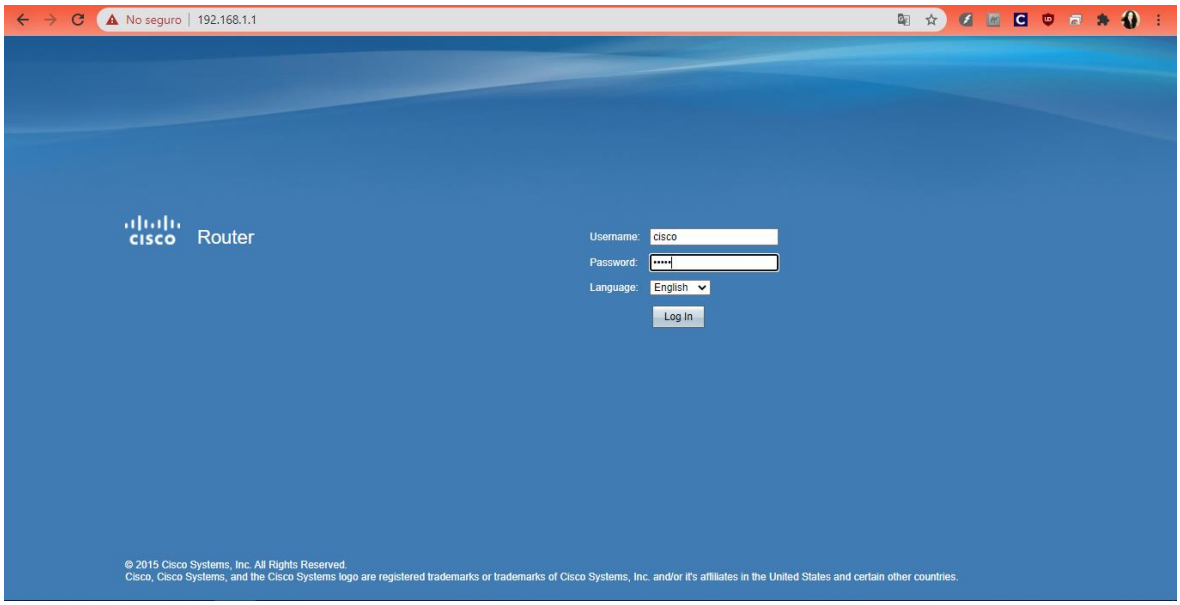


Figure 70. User and password input

First, the password to access the router will be changed to TFM-Luisa.

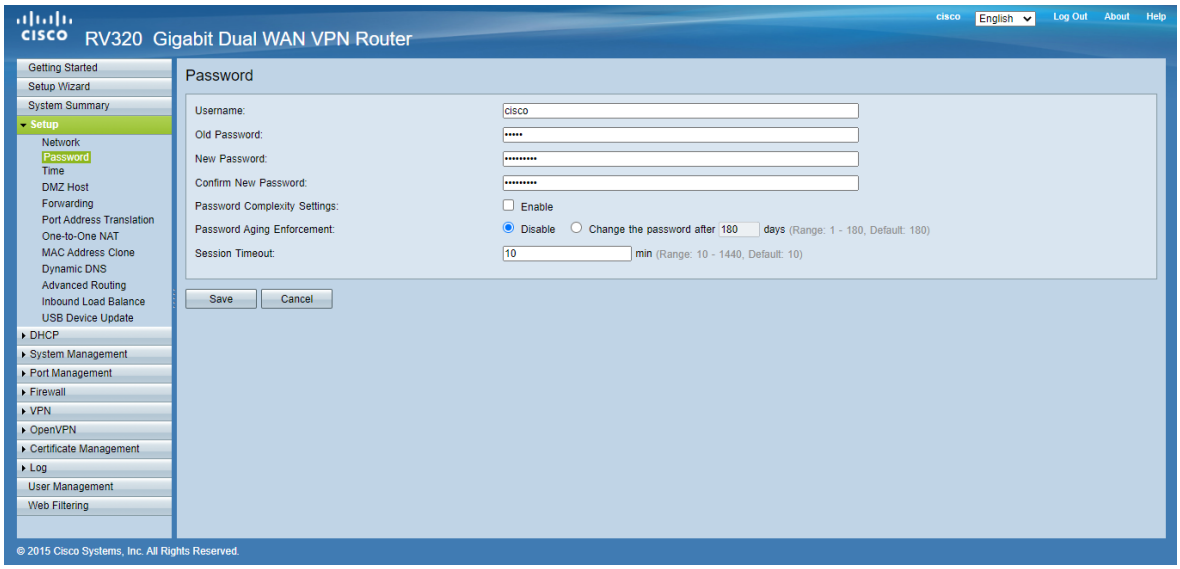


Figure 71. Change of password

Now, the architecture connected to the router will be equipped with the internet. To do this, a network cable will be connected from the router of the Internet access company to the WAN 1 of the device.

In this case, the WAN will be assigned an IP from the IP address range of the telephone operator's router, 192.168.0.200. Ideally, it would be to configure the telephone operator's router in bridge mode and configure the WAN using the operator's pppoe username and password. However, Vodafone does not allow it, so the operator's router had to be configured as DMZ and redirected all the ports to the IP 192.168.0.200.

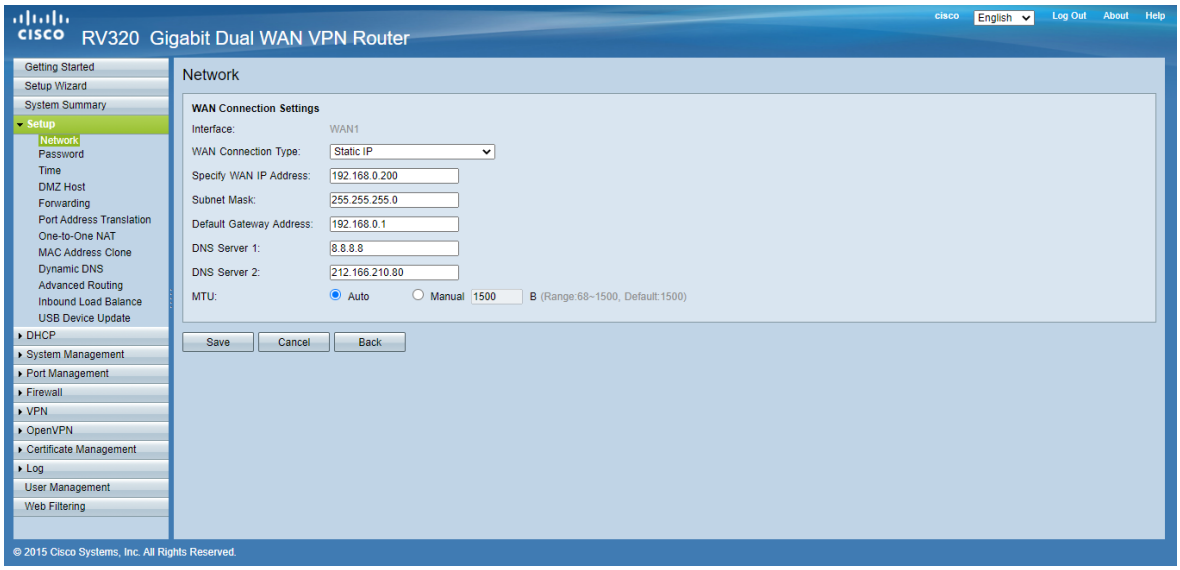


Figure 72. Wan with static IP address

Next, the router will be configured as a Gateway, to provide internet to all the computers that hang from it.

To do this, use the side menu and follow the following directory Setup -> Advanced Routing and configure it as Gateway.

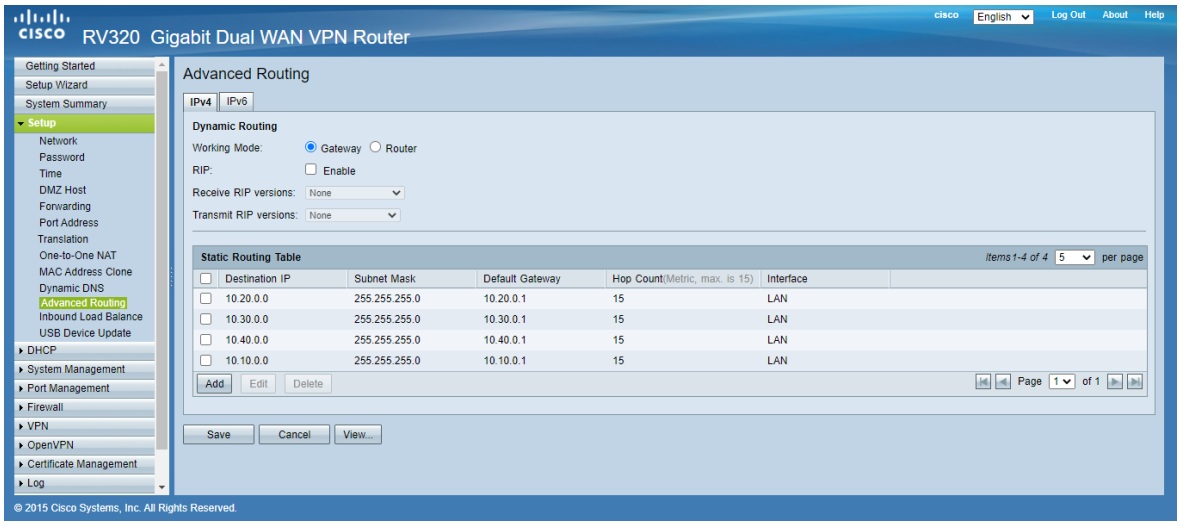


Figure 73. It is configured as Gateway

On the other hand, VLAN 4 will be created, accessing PORT MANAGEMENT -> VLAN MEMBERSHIP through the side menu. Subsequently, click on ADD and create Vlan 4.

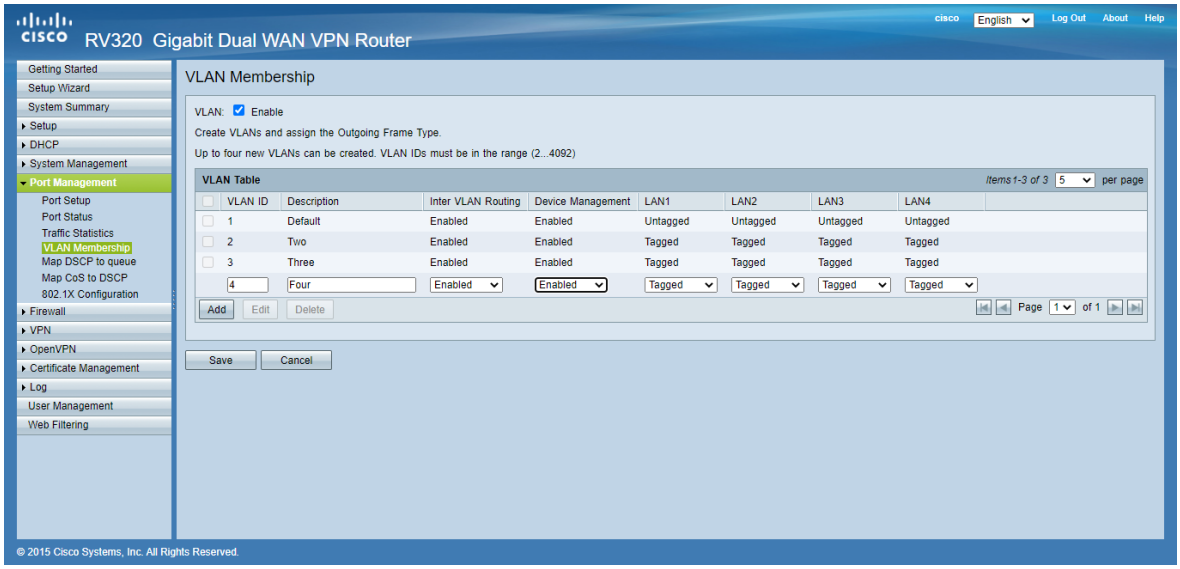


Figure 74. Add VLAN4

Next, the IP address ranges will be assigned to the different VLANs, accessing through the side menu DHCP -> DHCP settings.

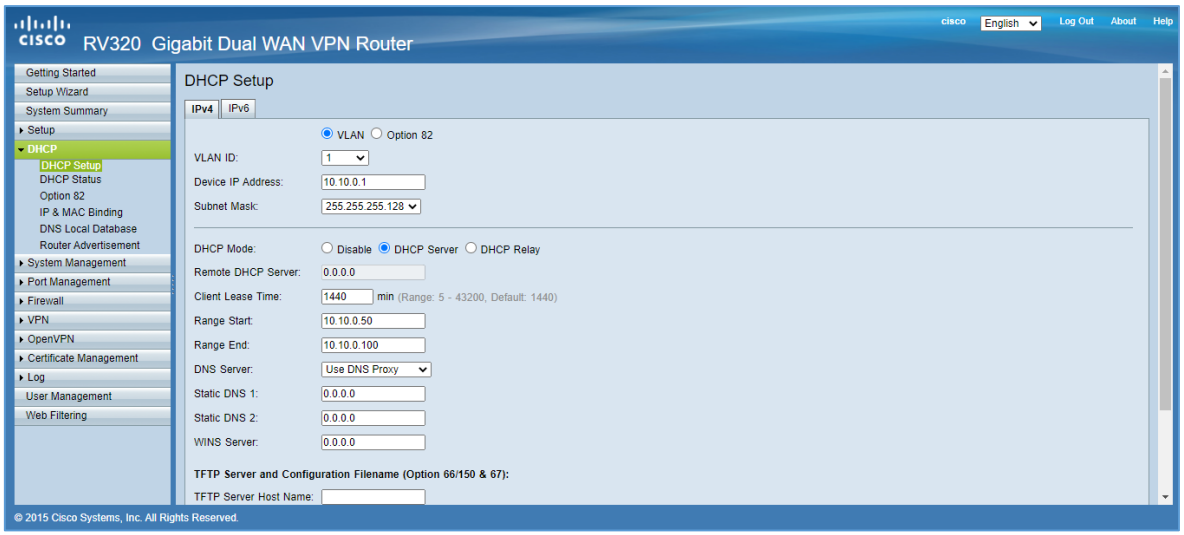


Figure 75. Vlan 1 IP address ranges assignment

The device notifies of the network change and redirection.

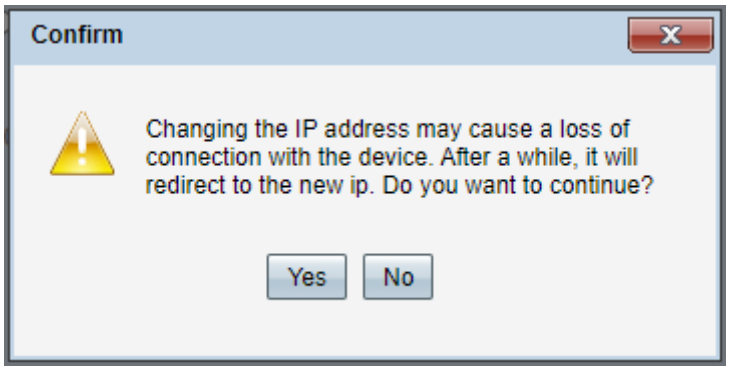


Figure 76. New IP redirect notice

Once the new address is accessed, the rest of the Vlan are configured to have the desired IP address range and the DHCP server correctly provides the IPs to the computers.

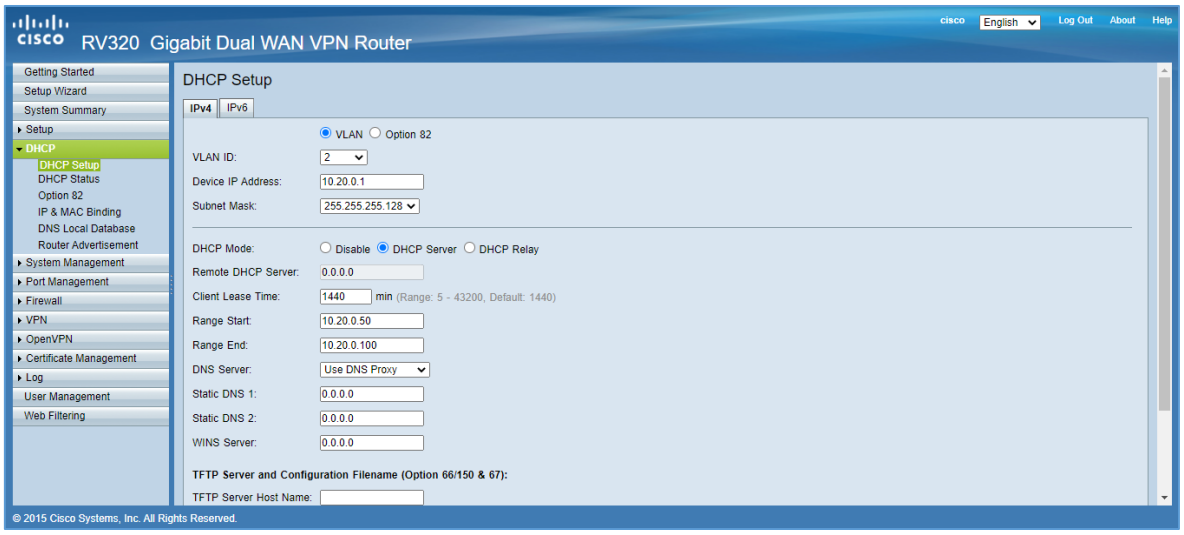


Figure 77. VLAN2 IP address configuration

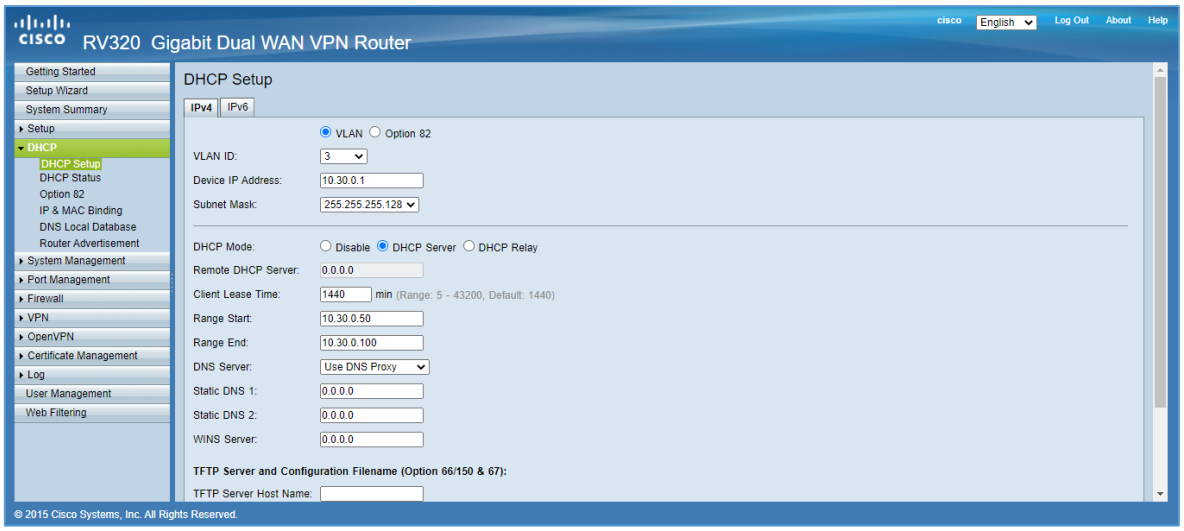


Figure 78. VLAN3 IP address configuration

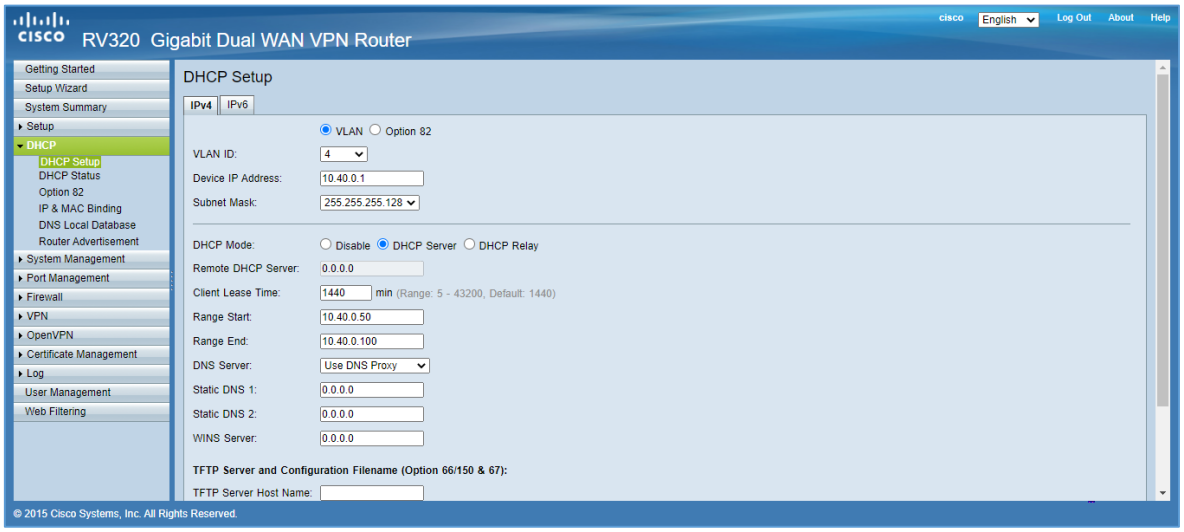


Figure 79. VLAN4 IP address configuration

Next, the Vlans will be added to the different interfaces, in this case, one Vlan per port will be used:

- Vlan 1 -> port 1
- Vlan 2 -> port 2
- Vlan 3 -> port 3
- Vlan 4 -> port 4

In this case, all Vlan will be tagged to Vlan1, while Vlan 1 will not be able to access any.

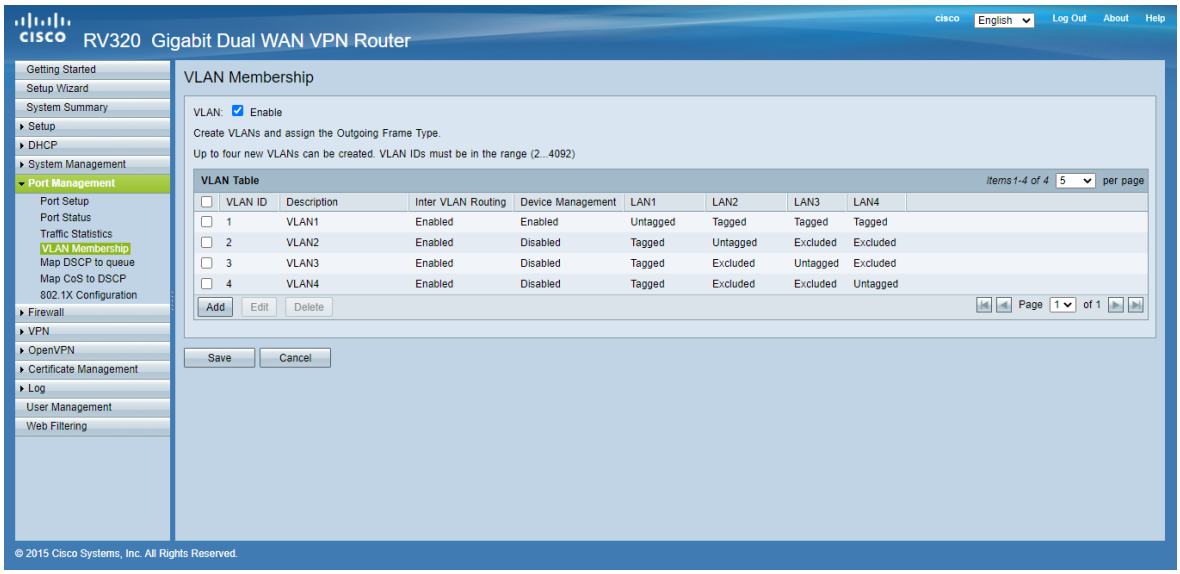


Figure 80. Vlan Membership

Next, the connectivity Vlan1 to Vlan2 will be checked. As can be seen in the figure below, communication from Vlan1 to Vlan2 is not allowed, as we have configured.

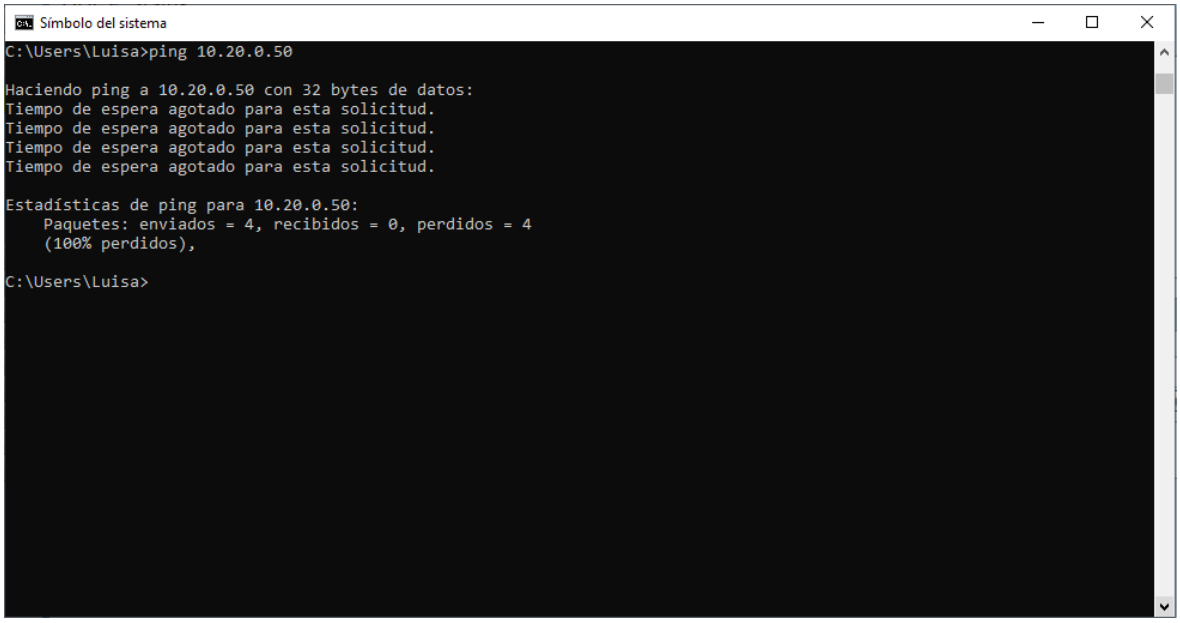


Figure 81. Vlan1 to Vlan2 connectivity

However, if Vlan2 to Vlan1 connectivity is verified, as can be seen in the figure below, it does allow communication from Vlan2 to Vlan1, as specified in the configuration.

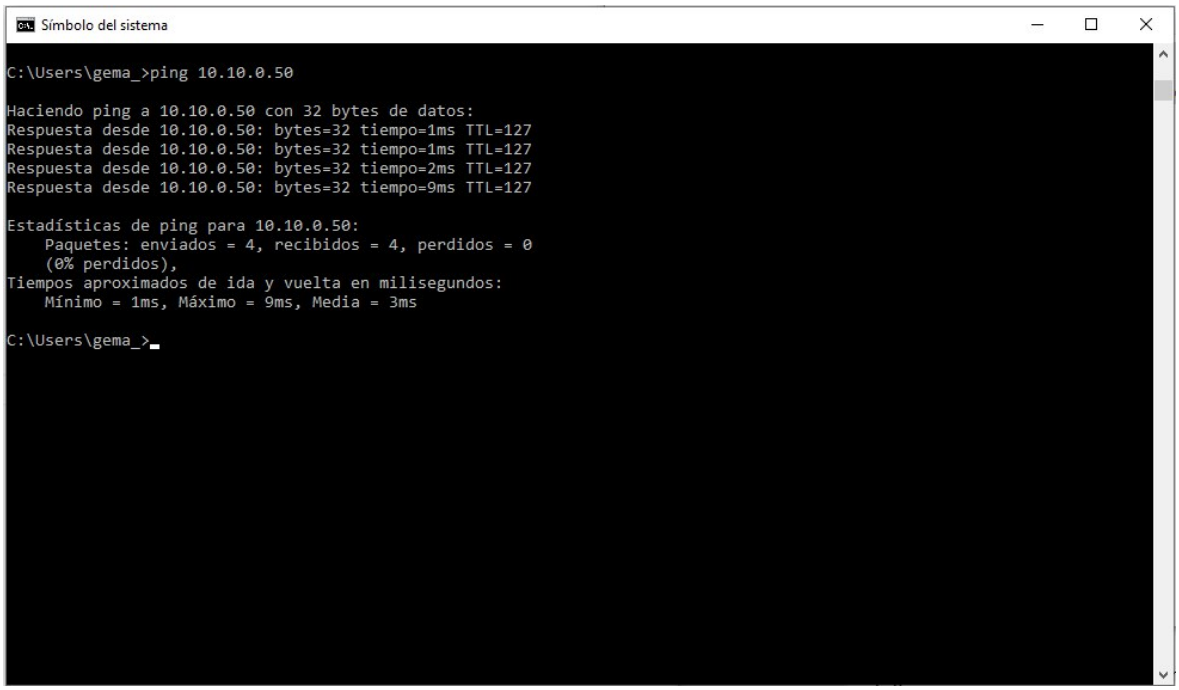


Figure 82. Vlan2 to Vlan1 connectivity

If the connectivity of Vlan1 is verified, with respect to Vlan3 and Vlan4, as seen in the subsequent figures, communication is not allowed.

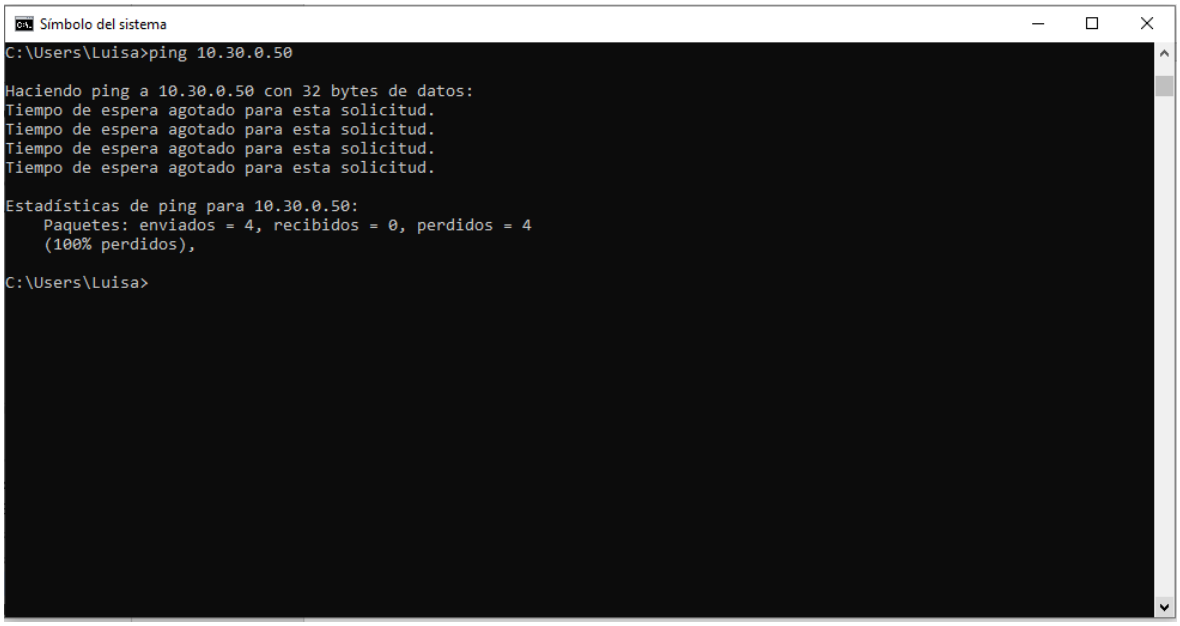


Figure 83. Vlan1 to Vlan3 connectivity

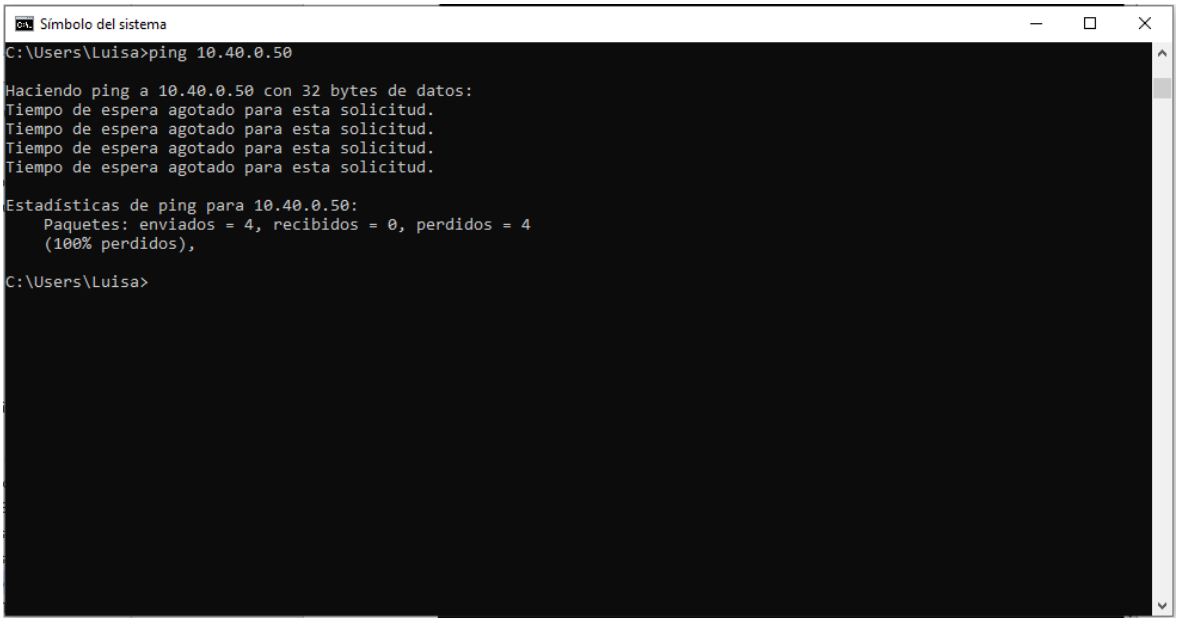


Figure 84. Vlan1 to Vlan4 connectivity

However, checking the connectivity from Vlan3 and Vlan4 to Vlan1, it does allow connectivity. Therefore, the Vlans configuration would be correct.

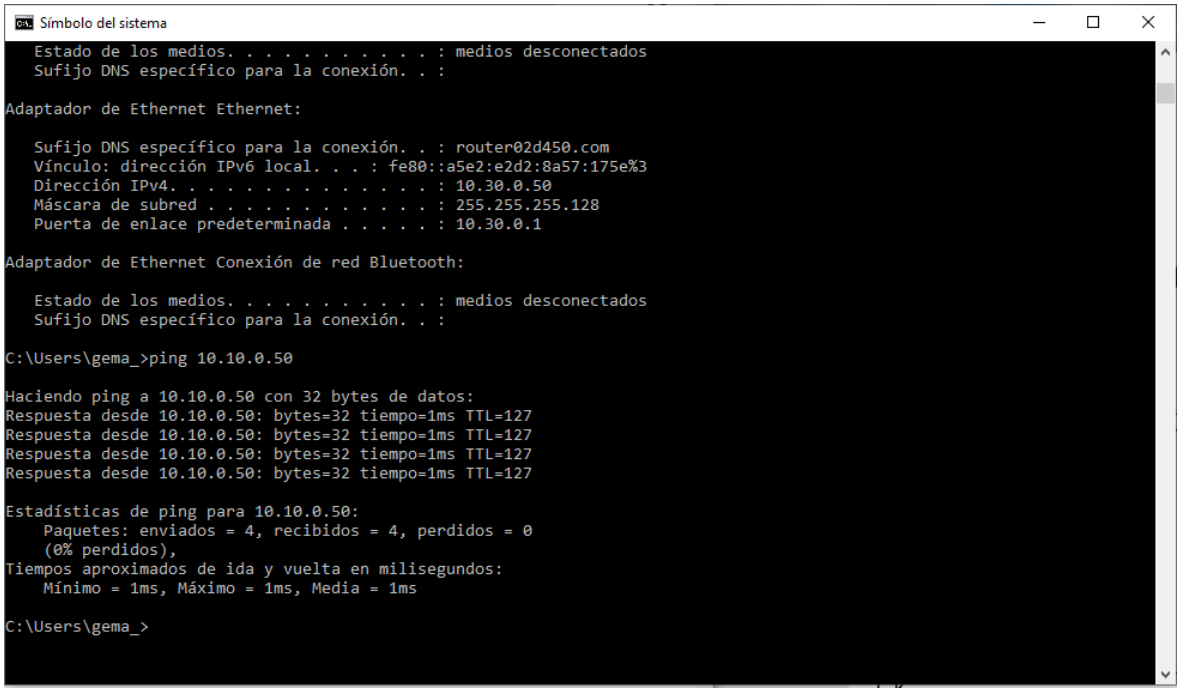


Figure 85. Vlan3 to Vlan1 connectivity

Figure 86. Vlan4 to Vlan1 connectivity

6.3 VPN CLIENTE-GATEWAY

6.3.1 *VPN configuration on RV320 router*

A VPN is to be made between a remote client and the router. To do this, using the side menu, click on VPN -> Client to Gateway and select TUNNEL.

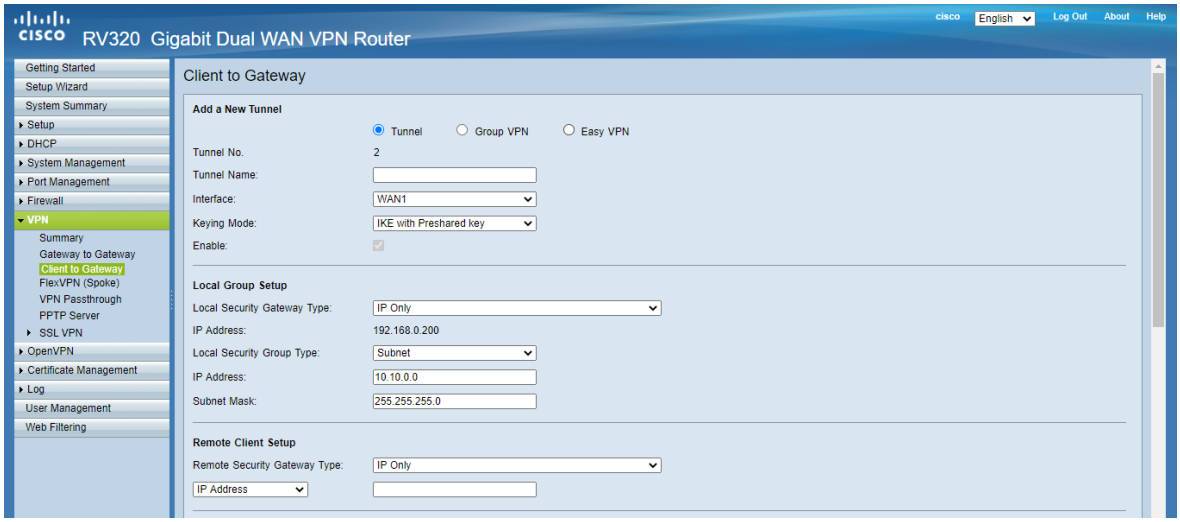


Figure 87. Add VPN

The name is added to the tunnel, in this case, for the name of the VPN, TEST has been chosen.

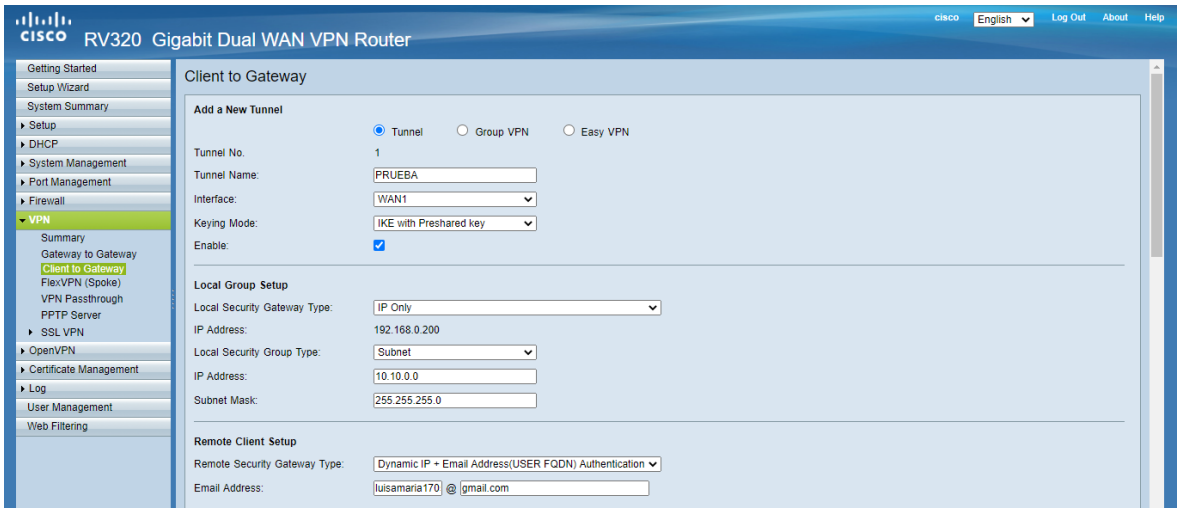


Figure 88. Add VPN

As input interface, WAN1 has been chosen and as Keying mode, IKE with preshared key has been chosen.

For this VPN, you will only be given access to the 10.10.0.0/25 network. And the phase 1 and phase 2 values shown in the image below will be used.

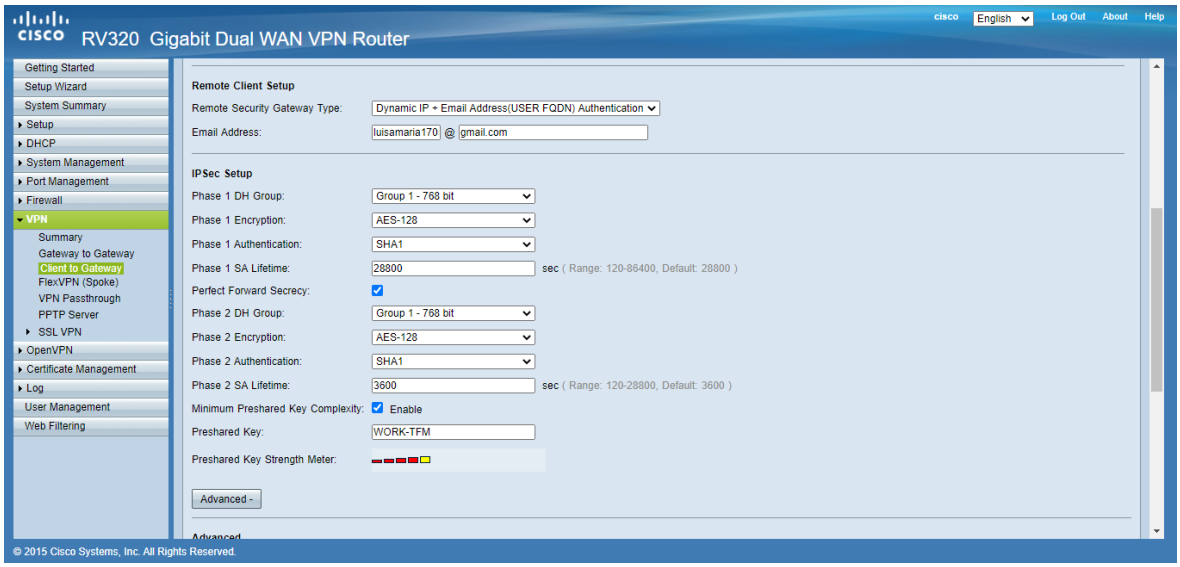


Figure 89. Phase 1 and phase 2 values

In the advanced parameters, the fields shown in the following image are selected, and in the authentication we will select a user who is registered in the device.

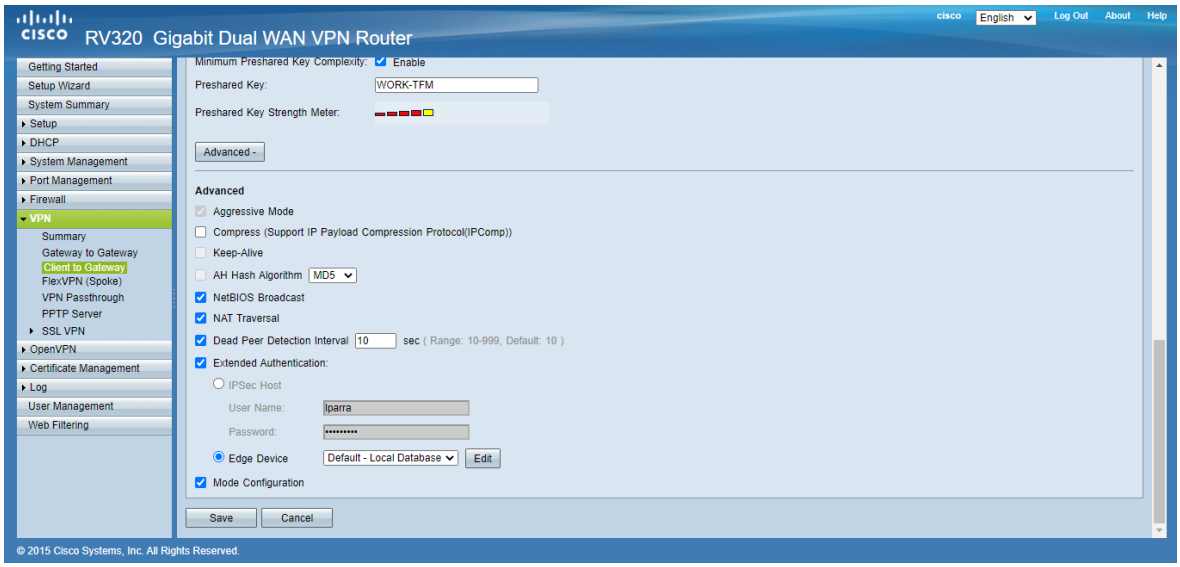


Figure 90. Advanced VPN settings

Next, click on User Management and add the username and password so that the user can access the campus using the VPN.

In this case, the user lparra will be added with the password Parra-TFM.

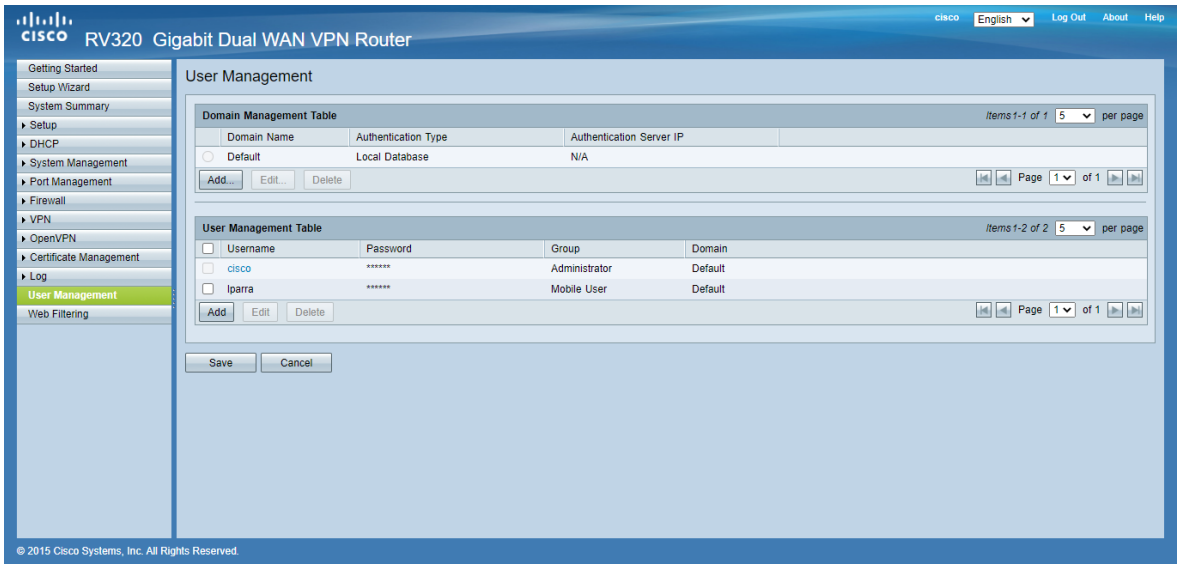


Figure 91. Add user VPN

6.3.2 VPN configuration on client

For the creation of the client, the free software ShrewSoft will be used.

The following images show the client configuration to establish the VPN with the campus.

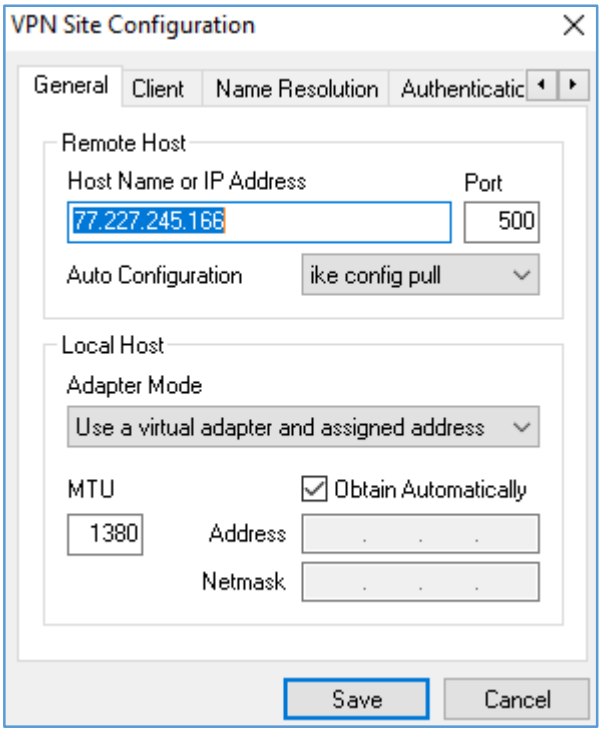


Figure 92. Client configuration Part1

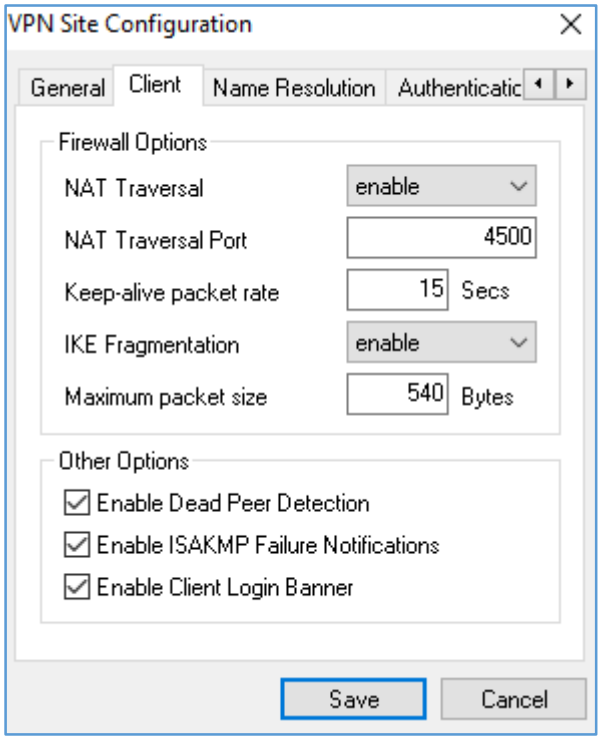


Figure 93. Client configuration Part2

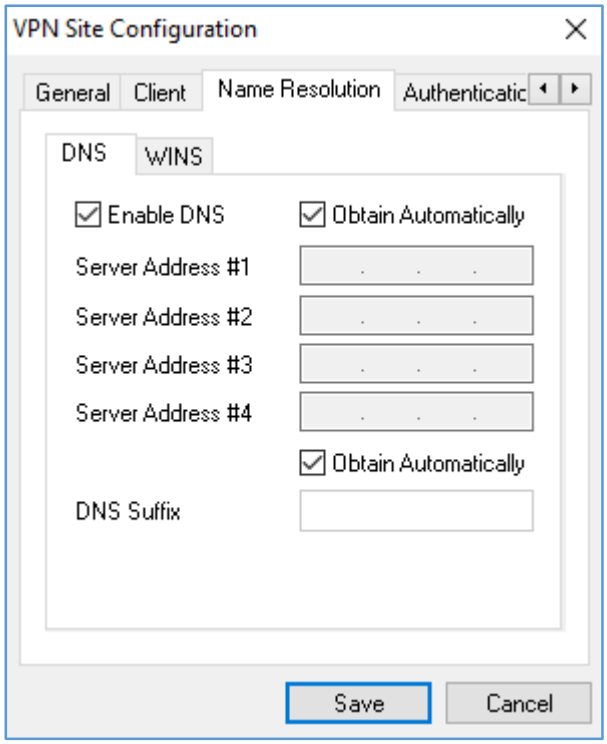


Figure 94. Client configuration Part3

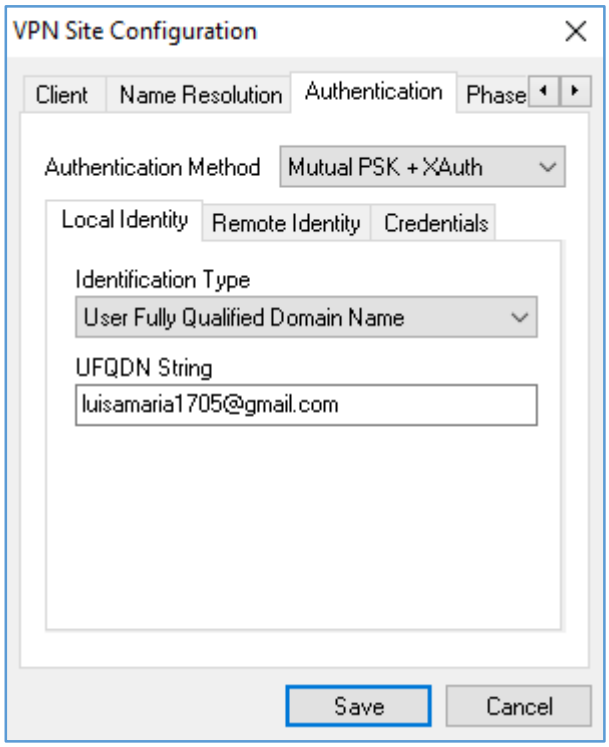


Figure 95. Client configuration Part4

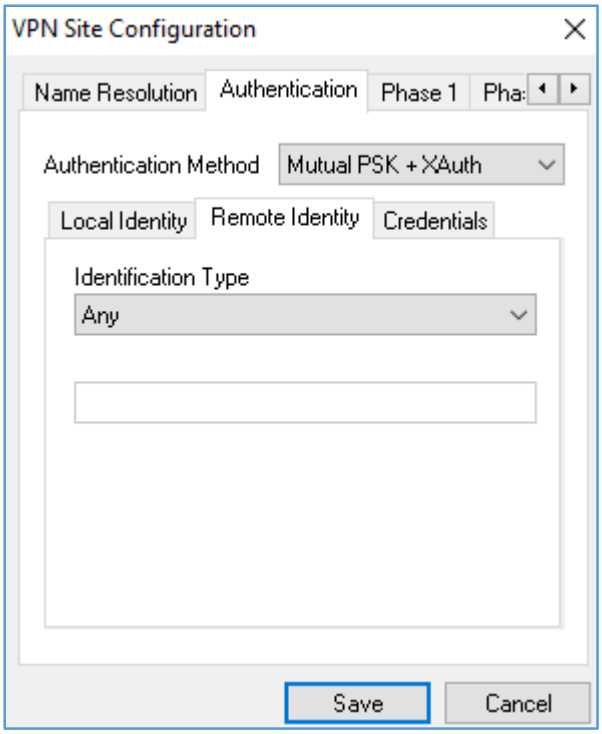


Figure 96. Client configuration Part5

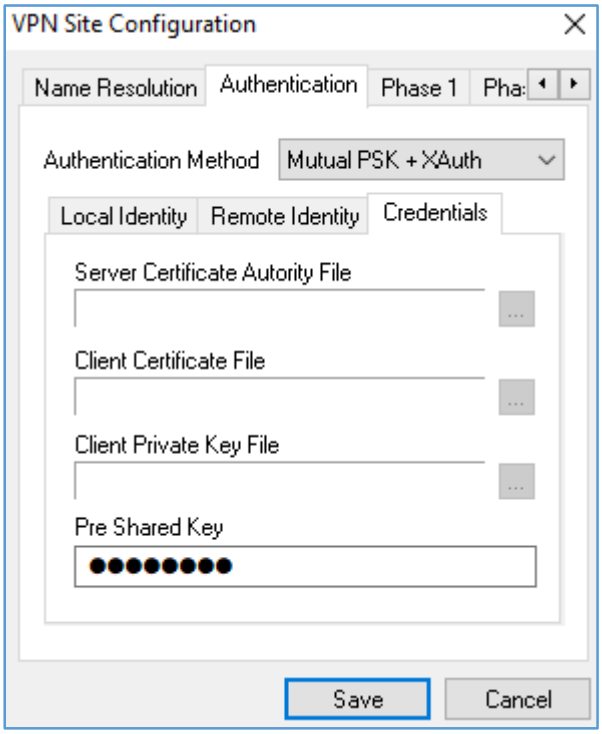


Figure 97. Client configuration Part6

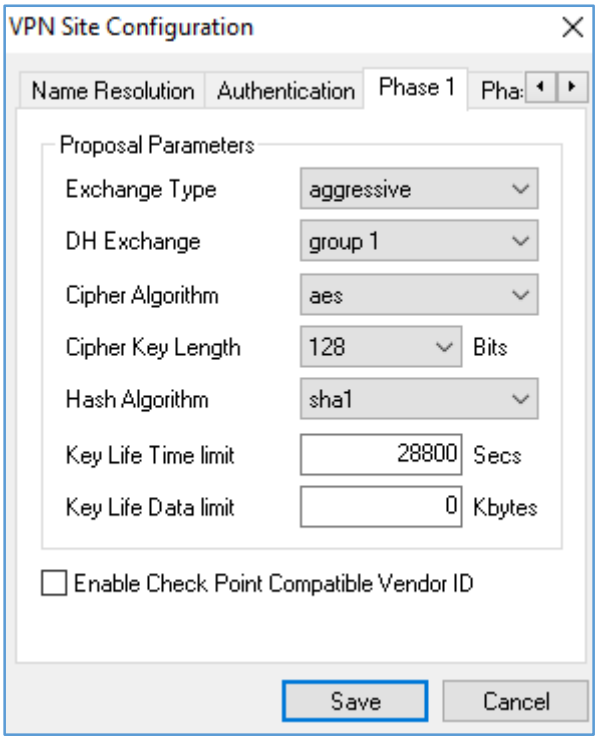


Figure 98. Client configuration Part7

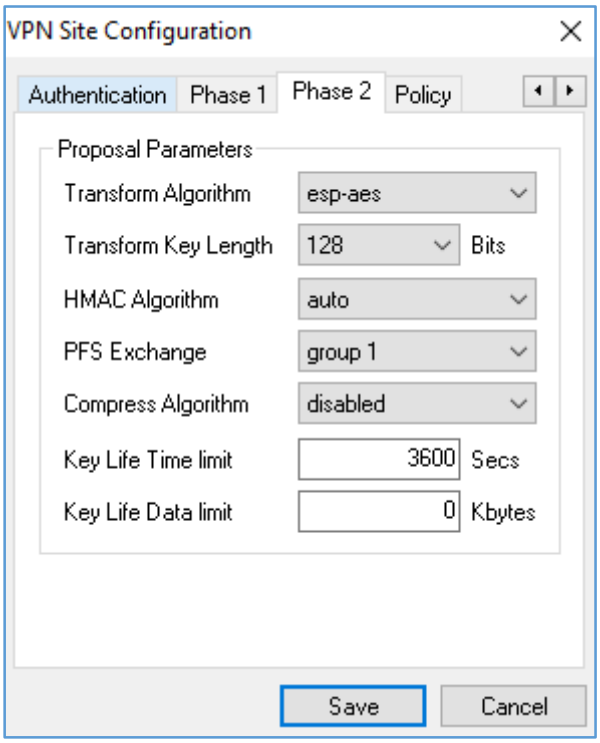


Figure 99. Client configuration Part8

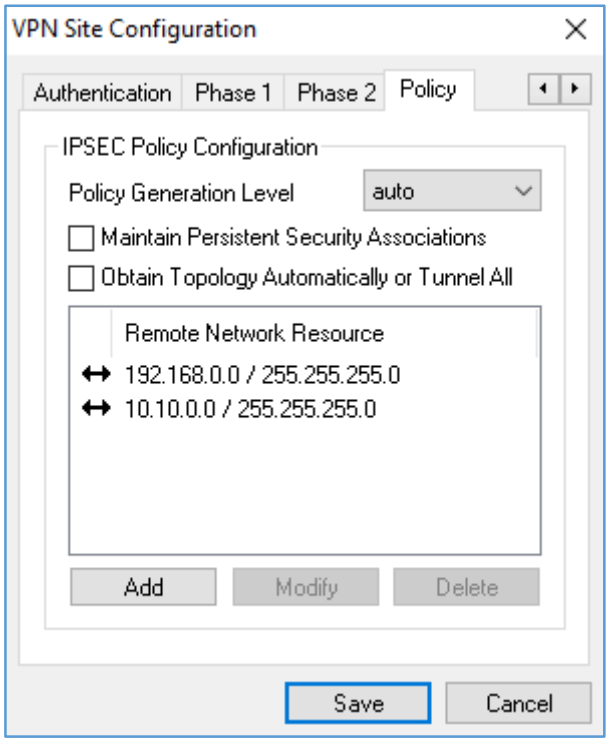


Figure 100. Client configuration Part9

6.4 VPN Gateway to Gateway

6.4.1 VPN configuration on Router A

A VPN will be made that connects the two company campus, for this, using the side menu, click on VPN -> Gateway to Gateway.

Next, the name of the tunnel is chosen, in this case it has been named as Campus 1 to Campus 2.

In the following two images, you can see the values for phase 1 and phase 2 of the VPN, as well as the subnets to which access is given with this VPN.

Figure 101. VPN Gateway Configuration - Gateway

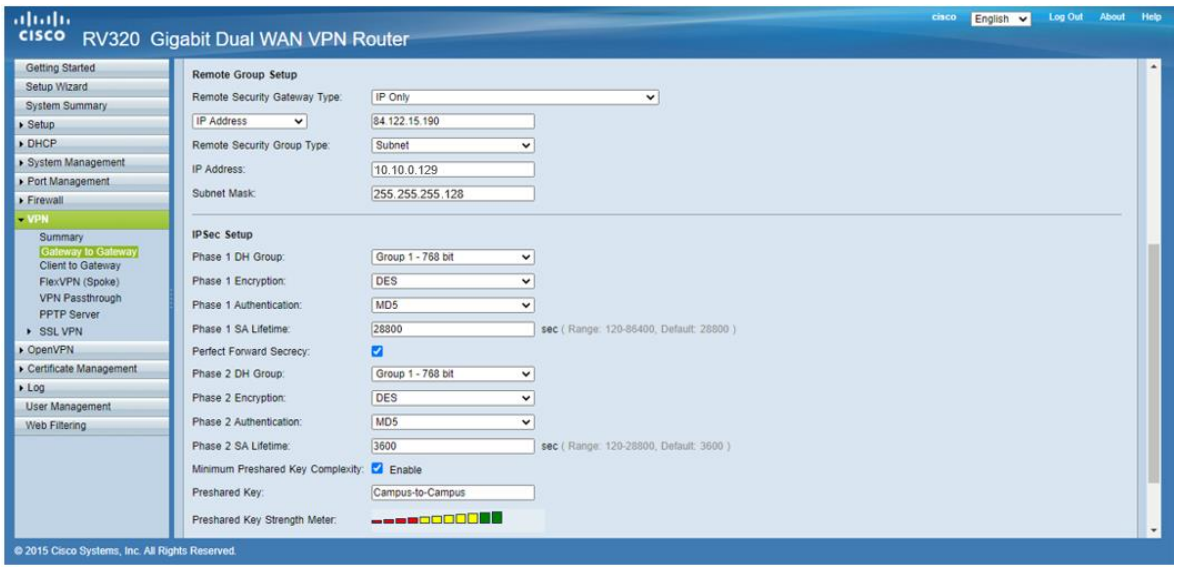


Figure 102. VPN Gateway Configuration - Gateway

6.5 QOS

Normally, in a network all traffic is managed in the same way and all data has the same probability of being delivered or not, therefore, we will proceed to manage the network traffic using the quality of service (QoS), which prioritizes specific network traffic while delivering the best performance to lower priority services.

To implement the Diffserv model in the RV320 route, use the left side menu and click on Port Management -> Map DSCP to Queue.

Next, the service corresponding to the DSCP is chosen and the desired priority level is selected from the respective list of Queue Priority.

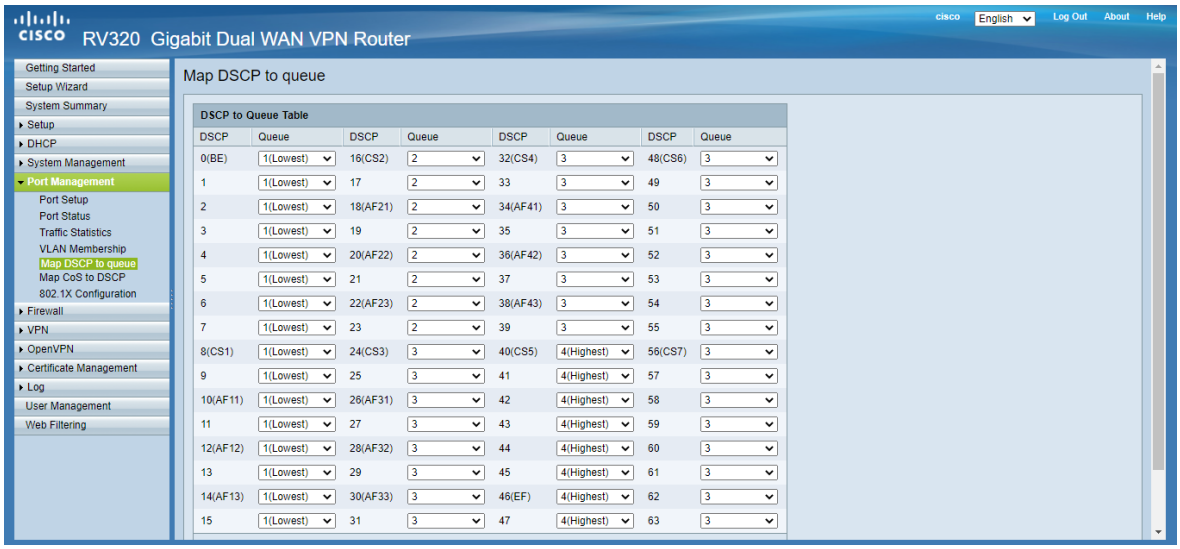


Figure 103. Map DSCP to queue

The DSCP to the queue table displays the following information:

- 0 to 7 - This range is assigned the traffic being treated ensuring a best effort to be delivered. It is the default type of service and is recommended for the traffic that is not in real time.
- 8 to 23 - Background. All traffic running as Background needs to be allocated in this range. This includes bulk transfers, games etc.
- 24 to 31 - Best effort. Best-effort data to be delivered with ordinary priority on the LAN. The network does not provide any guarantees on the output, but the data gets unspecified bit rate and delivery time based on the traffic. Most applications will use this option.
- 32 to 47 - All video traffic can be assigned in this range.
- 48 to 63 - This range is mainly used for voice traffic.
- Queue - Displays the outgoing queue to which the DSCP is associated. The queue uses the priority queue that ranges from 1 to 4, with 1 being the lowest priority and 4 the highest.

For the network being configured, real-time and VOIP traffic will be prioritized, so that video conferencing can be done smoothly and phone calls will work properly. Therefore, the range 19 to 23 will be marked as 3 and the range 48-54 will be marked as 4. The range 40-47, is used mainly for the video, so it will be marked as 4 so that it goes smoothly.

Figure 104. Map DSCP to queue

To verify that the configuration is correct, an iperf server has been installed on one of the computers in the local network, as well as an iperf client on another of the computers. Also, a video call will be made simultaneously with the 10.10.0.50 equipment to a non-network equipment, to verify that the video call is not interrupted, with the current configuration.

In the figure below, you can see the iperf server hosted on the local network computer with IP 10.10.0.50.

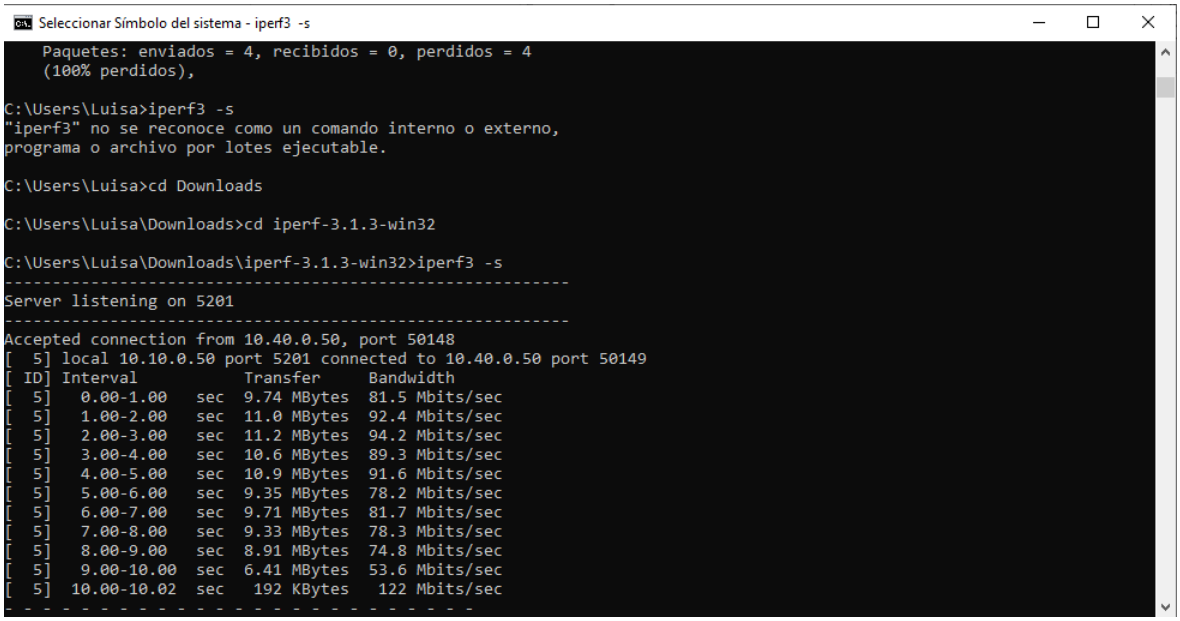


Figure 105. Iperf Server

While, in the following figure, you can see the client hosted on the computer with IP 10.40.0.50

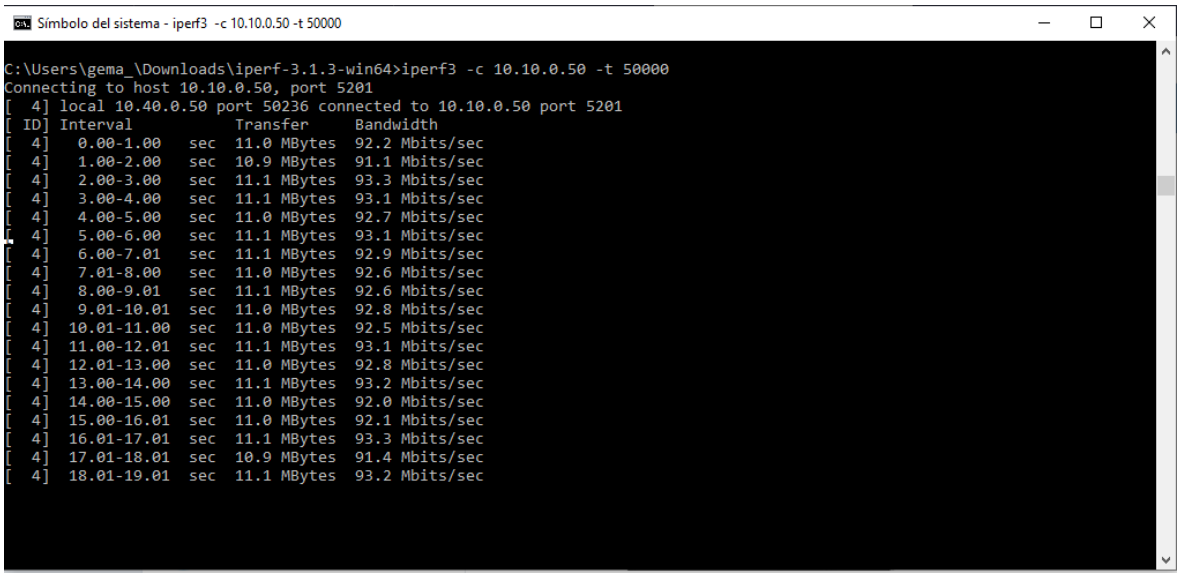


Figura 106. Iperf Client

Also, the network is being analyzed using wireshak from the 10.10.0.50 computer, verifying that while the video call is not established, there are no packet losses between the client and the iperf server.

No.	Time	Source	Destination	Protocol	Length	Info
182	0.018289	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=220461 Ack=1 Win=53248 Len=1460
183	0.018289	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=221921 Ack=1 Win=53248 Len=1460
184	0.018290	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=223381 Ack=1 Win=53248 Len=1460
185	0.018290	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=224841 Ack=1 Win=53248 Len=1460
186	0.018309	10.10.0.50	10.40.0.50	TCP	54	5201 → 50182 [ACK] Seq=1 Ack=226301 Win=64512 Len=0
187	0.019062	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=226301 Ack=1 Win=53248 Len=1460
188	0.019063	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=227761 Ack=1 Win=53248 Len=1460
189	0.019064	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=229221 Ack=1 Win=53248 Len=1460
190	0.019064	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=230681 Ack=1 Win=53248 Len=1460
191	0.019065	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=232141 Ack=1 Win=53248 Len=1460
192	0.019065	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=233601 Ack=1 Win=53248 Len=1460
193	0.019066	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=235061 Ack=1 Win=53248 Len=1460
194	0.019088	10.10.0.50	10.40.0.50	TCP	54	5201 → 50182 [ACK] Seq=1 Ack=236521 Win=64512 Len=0
195	0.019840	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=236521 Ack=1 Win=53248 Len=1460
196	0.019840	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=237981 Ack=1 Win=53248 Len=1460
197	0.019841	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=239441 Ack=1 Win=53248 Len=1460
198	0.019841	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=240901 Ack=1 Win=53248 Len=1460
199	0.019842	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=242361 Ack=1 Win=53248 Len=1460
200	0.019843	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=243821 Ack=1 Win=53248 Len=1460
201	0.019862	10.10.0.50	10.40.0.50	TCP	54	5201 → 50182 [ACK] Seq=1 Ack=245281 Win=64512 Len=0

Figure 107. Sequence of communication packets between iperf client and server

If a packet is entered, it can be verified that the traffic is marked as Diffserv, when the packet comes from IP 10.40.0.50 towards 10.10.0.50.

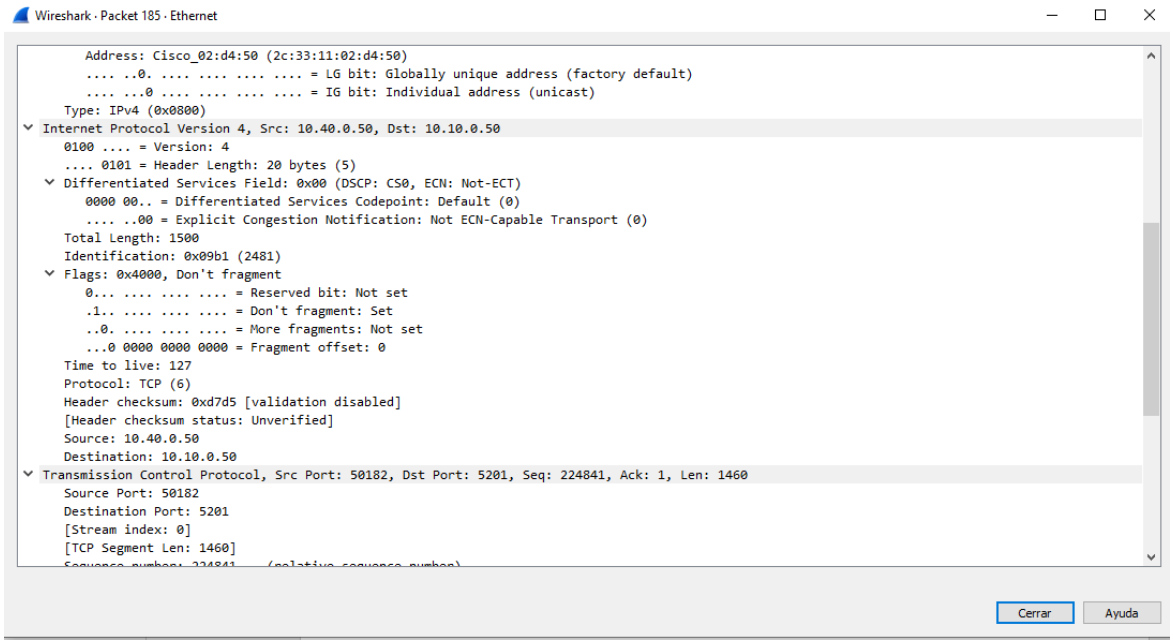
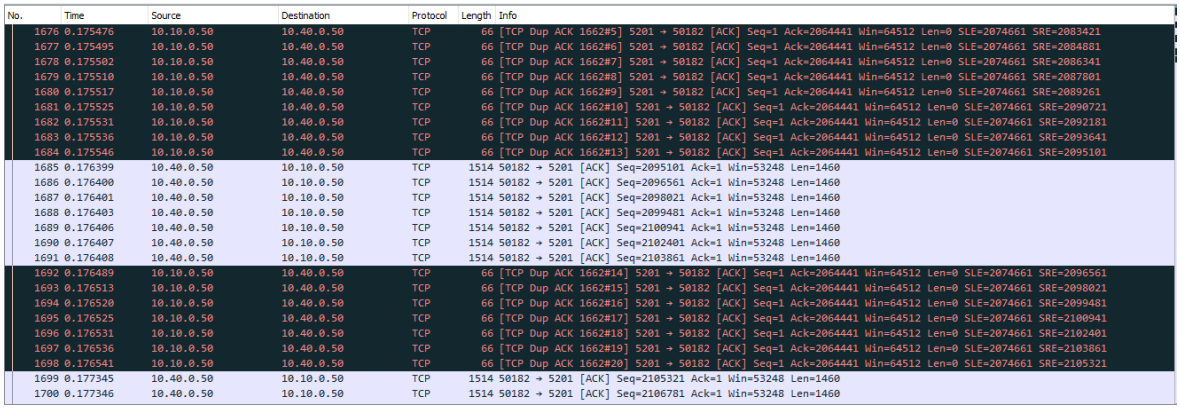


Figure 108. Package marked Diffserv

As seen previously, there was no packet loss between client and server while the video call was not in progress, however, once the video call starts, packets start to be discarded in the iperf communication, producing packet resendings.



No.	Time	Source	Destination	Protocol	Length	Info
1676	0.175476	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#5] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2083421
1677	0.175495	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#6] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2084881
1678	0.175502	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#7] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2086341
1679	0.175510	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#8] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2087801
1680	0.175517	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#9] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2089261
1681	0.175525	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#10] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2090721
1682	0.175531	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#11] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2092181
1683	0.175536	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#12] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2093641
1684	0.175546	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#13] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2095101
1685	0.176399	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2095101 Ack=1 Win=53248 Len=1460
1686	0.176400	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2096561 Ack=1 Win=53248 Len=1460
1687	0.176401	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2098021 Ack=1 Win=53248 Len=1460
1688	0.176403	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2099481 Ack=1 Win=53248 Len=1460
1689	0.176406	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2100941 Ack=1 Win=53248 Len=1460
1690	0.176407	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2102401 Ack=1 Win=53248 Len=1460
1691	0.176408	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2103861 Ack=1 Win=53248 Len=1460
1692	0.176489	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#14] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2096561
1693	0.176513	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#15] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2098021
1694	0.176520	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#16] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2099481
1695	0.176525	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#17] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2100941
1696	0.176531	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#18] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2102401
1697	0.176536	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#19] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2103861
1698	0.176541	10.10.0.50	10.40.0.50	TCP	66	[TCP Dup ACK 1662#20] 5201 → 50182 [ACK] Seq=1 Ack=2064441 Win=64512 Len=0 SLE=2074661 SRE=2105321
1699	0.177345	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2105321 Ack=1 Win=53248 Len=1460
1700	0.177346	10.40.0.50	10.10.0.50	TCP	1514	50182 → 5201 [ACK] Seq=2106781 Ack=1 Win=53248 Len=1460

Figure 109. Packet loss

If a packet is entered, it can be seen that it is a duplicate packet, which indicates that the receiver has seen a space between the numbers of the received transmission sequence, which implies the loss of one or more lost packets. The receiver, by sending so many DUP messages, is clearly indicating that the packets are being dropped.

However, the video call service has not experienced any cut, neither video nor sound, and wireshark, has not shown packet loss between ip 10.10.0.50 and the outside.

7.6. FIRMWARE UPDATE RV320

It has been decided to update the firmware version installed in the RV320 device, to solve a bug that presents version v1.3.1.12 when configuring inter Vlans on the device and when performing the VPN Gateway to Gateway. These problems are solved with the download and installation of version v1.3.2.02.

To do this, using the side menu, click on System Management -> Firmware Upgrade and load the new firmware version.

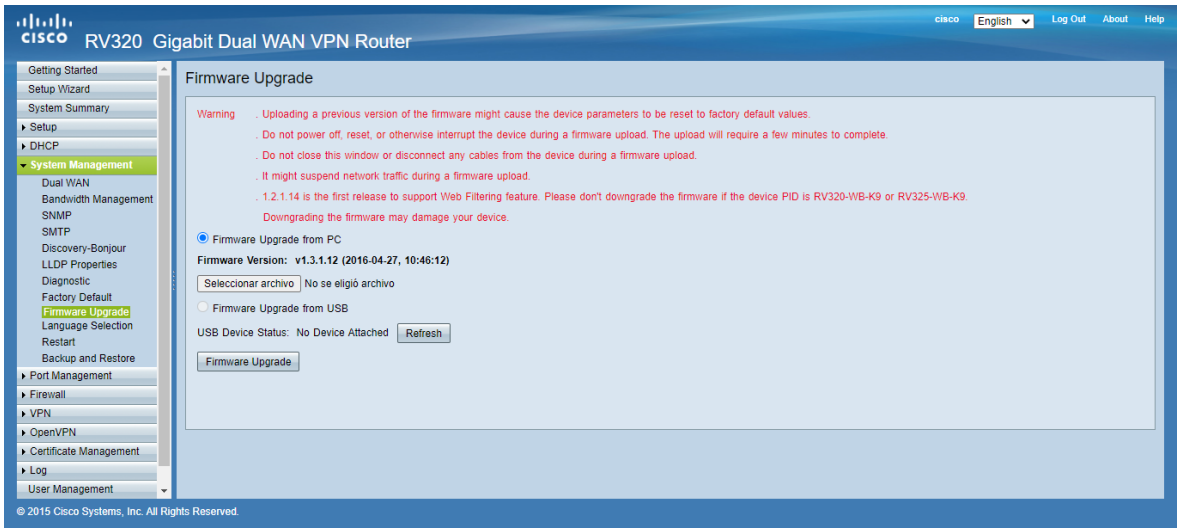


Figure 110. Upload new firmware

6.6 Router B Configuration

First, the Cisco RV320 Gigabit Dual WAN VPN router has been reset to the factory state. To do this, the Reset button has been held down for a few seconds, causing it to be reset and thus all the device's LEDs turn on for a few seconds.

When the device is in its initial state, it is assigned the IP 192.168.1.1. The IP address of the PC that is going to be used will be configured, for the access and subsequent configuration of the router, so that it takes an IP by DHCP, in this way the router will assign the equipment an IP within the range 192.168.1.x.

The web administrator of the device will be used to configure it, for this reason we will access the equipment through a web browser, entering the IP 192.168.1.1 in the address bar and we will change the access password to TFM-Luisa.

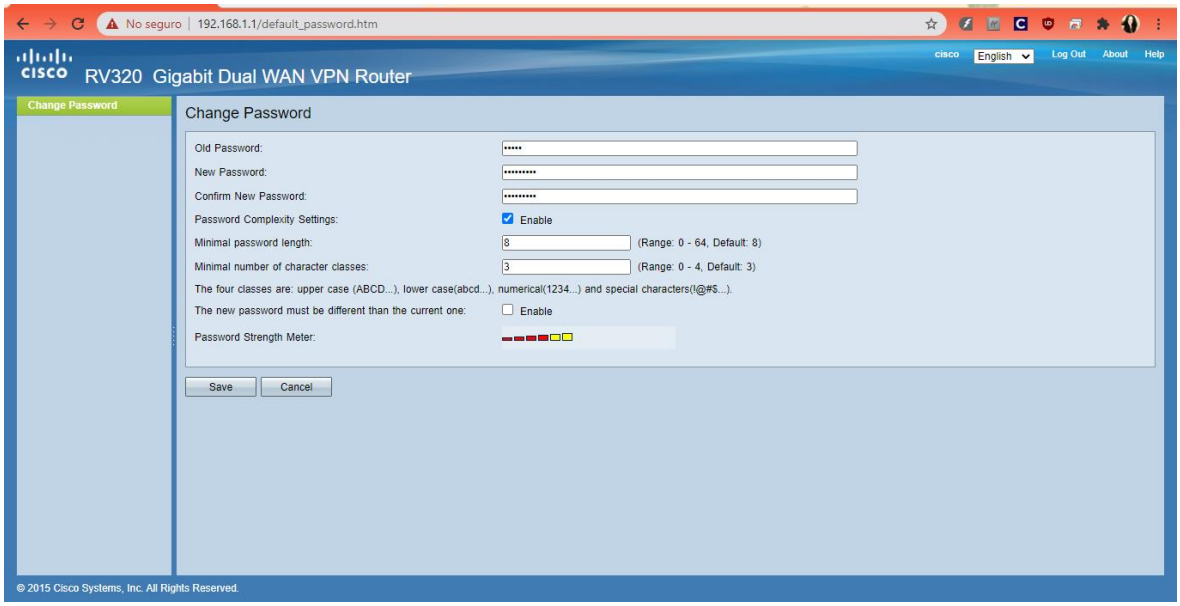


Figure 111. Router B password change

As in router A, we are going to start by configuring the VLANs and we are going to use the same ranges for the Vlan as in the other device.

In the following image, you can see the creation of Vlans 2, 3 and 4 and the permission table between Vlans.

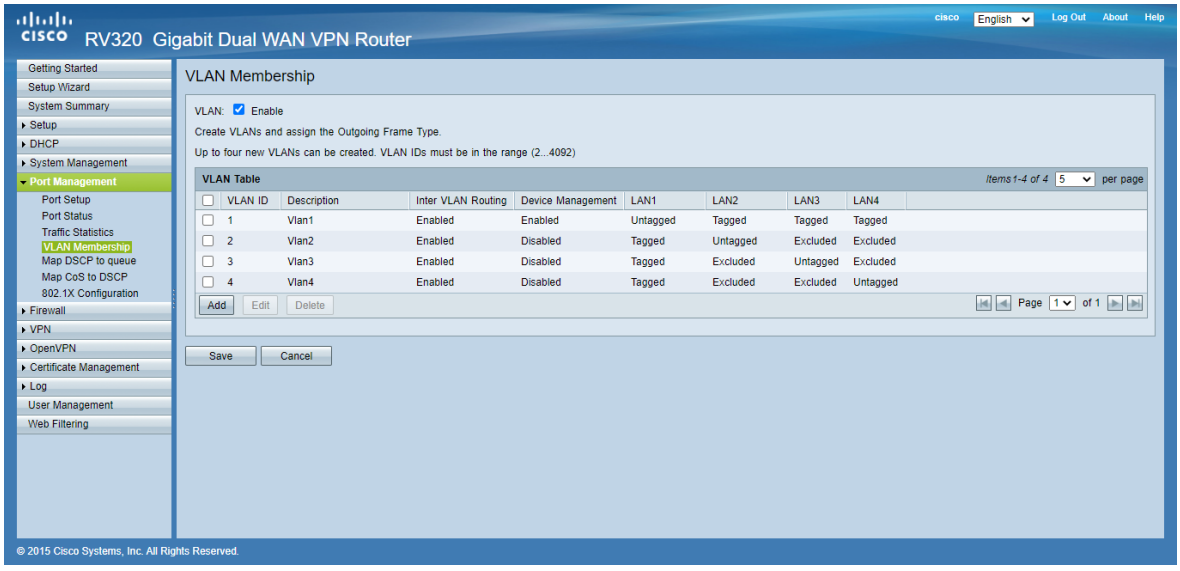


Figure 112. Add Vlan y Vlan Membership

Next, DHCP servers are created for each Vlan created. In the following images, you can see the DHCP configuration of the different VLANs.

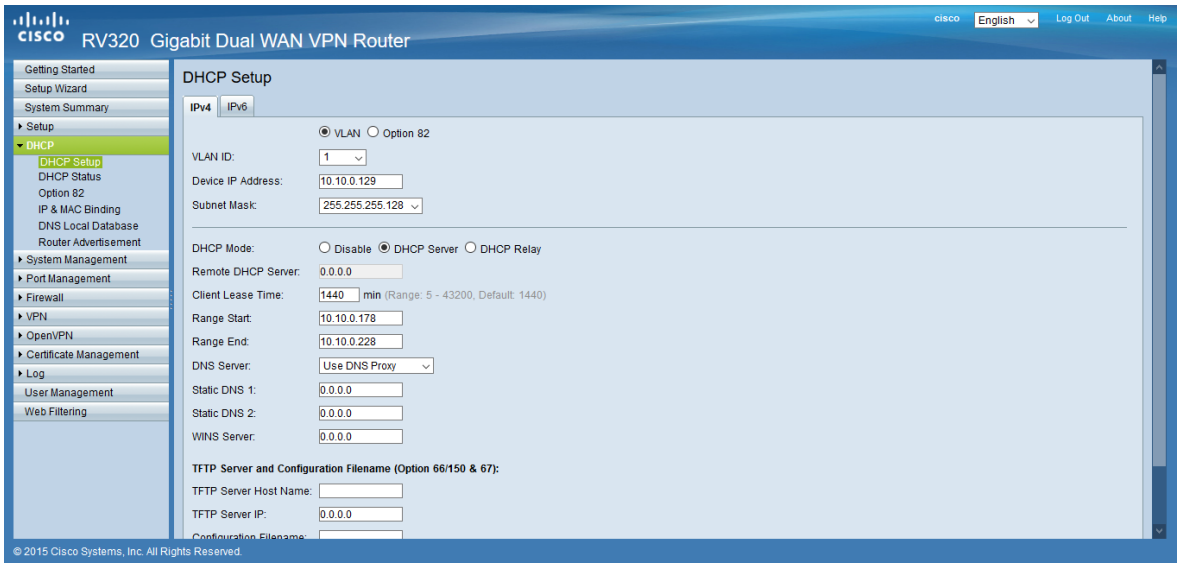


Figure 113. DHCP Vlan 1

Figure 114. DHCP Vlan 2

Figure 115. DHCP Vlan 3

Figure 116. DHCP Vlan 4

Now, the architecture connected to the router will be equipped with the internet. To do this, you will connect a network cable from the router of the internet access company to wan 1 of the device.

In this case, an IP will be assigned to the WAN using pppoe, since the router at headquarters 2 is from Movistar and allows its configuration as a single station.

To do this, in Network -> Wan1, configure the movistar pppoe parameters.

Figure 117. WAN configuration with pppoe

In the figure below, you can see how WAN 1 has established the ppeo connection and obtained a public IP address.

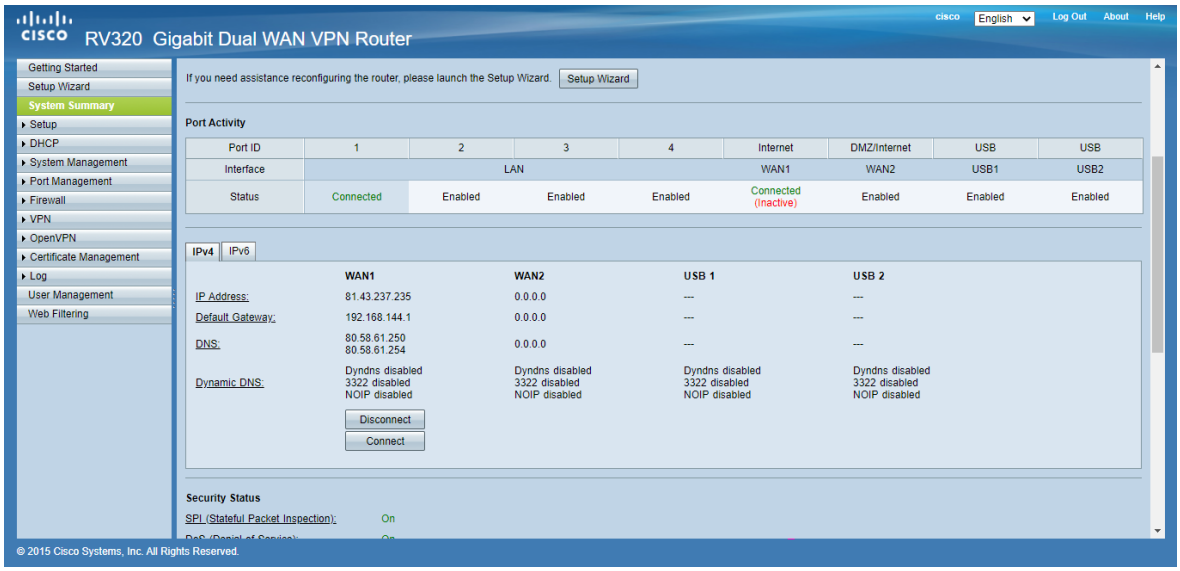


Figure 118. IP WAN 1

In this case, the internet provider of campus 2 is Movistar, so it allows you to configure your internet access router as a single-user station and in this way that you can configure the RV320 router through PPPOE.

To configure the Movistar router as a single-user, you had to access the telephone operator's router and select the single-user option from the options menu.

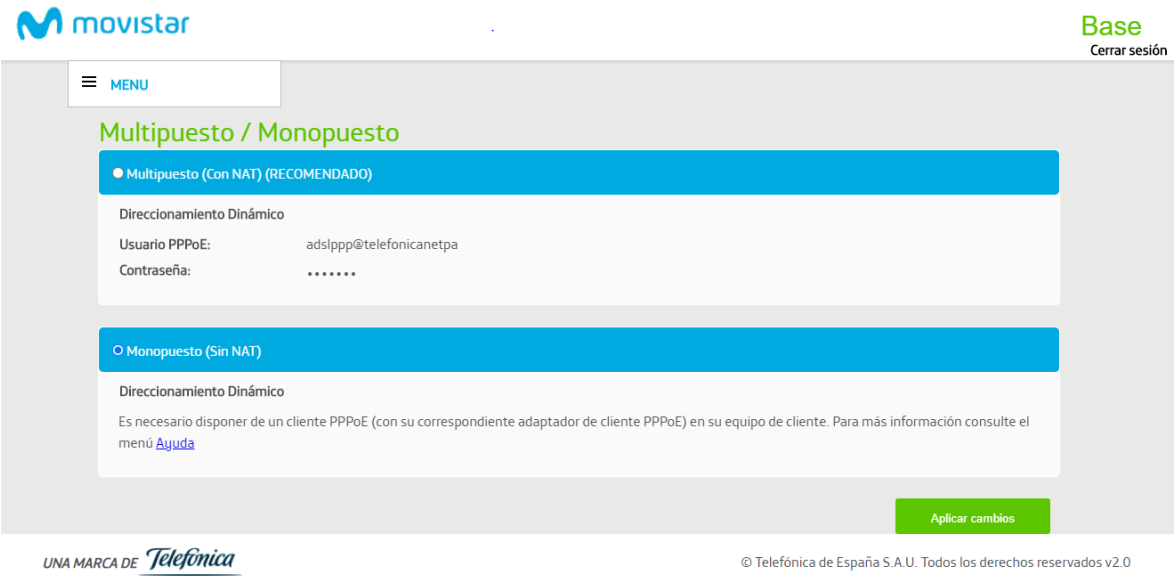


Figure 119. Single-user configuration

6.7 VPN Gateway to Gateway

6.7.1 VPN configuration on Router B

A VPN is going to be created to connect the two company sites. To do so, using the side menu, click on VPN -> Gateway to Gateway.

Next, choose the name of the tunnel, in this case it has been named Campus 1 to Campus 2.

In the following two images, you can see the values for phase 1 and phase 2 of the VPN, as well as the subnets to which access is given with this VPN.

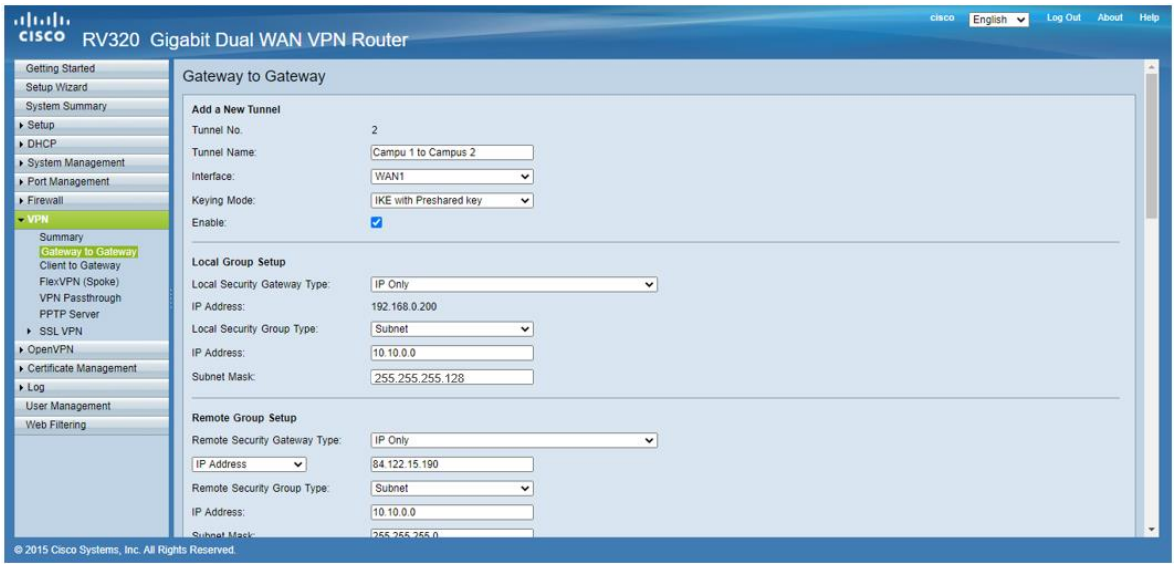


Figure 120. VPN Gateway Configuration - Gateway

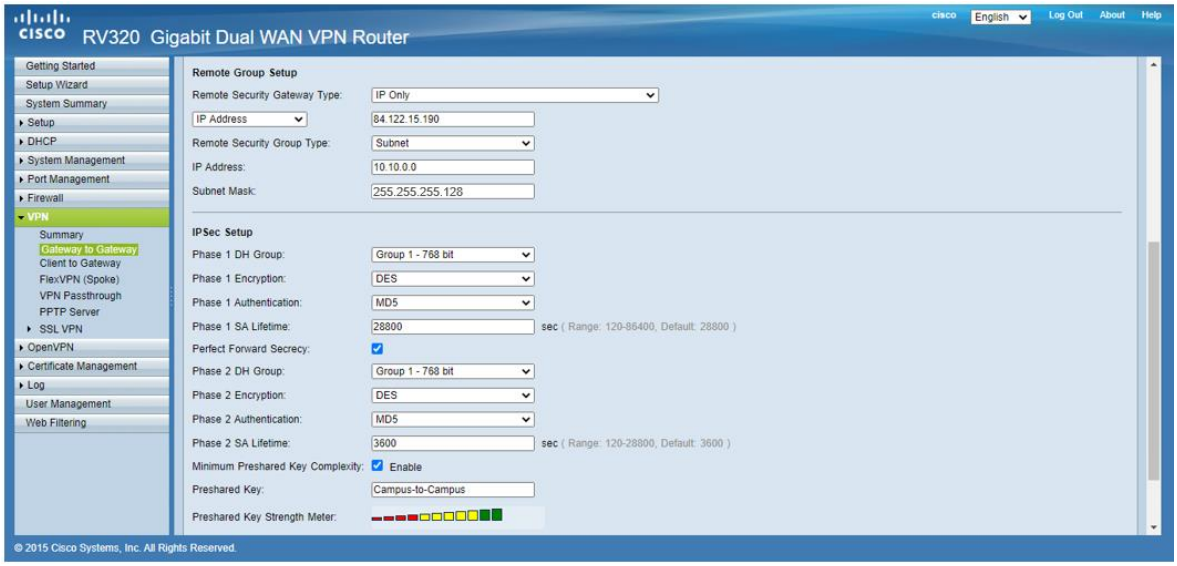


Figure 121. VPN Gateway Configuration - Gateway

7 PLANNING

In this section, we will detail the different phases of the project, as well as its duration in time.

In the following table, you can see all the tasks to be developed during the project:

Nombre de tarea	Duración	Predecesoras	Nombres de los recursos
Design and implementation of a company's communications	**91 días**		
Desing of the network	31 días		Engineering department
Stockpiles of material	30 días	2	purchasing department
Electronic network configuration	15 días	3	Engineering department
Electronic network installation	10 días	4	Installation operators
Start Up	5 días	5	Engineering department

Table 3. Tasks of the department

In the following image, you can see the course of the tasks by means of a Gantt chart.

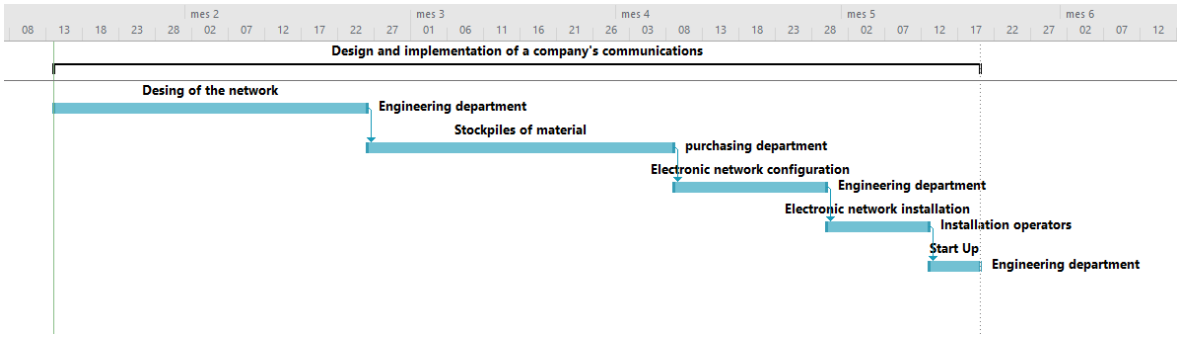


Figure 122. Gantt Diagram

As can be seen in both the Gantt chart and the task table, the project would have a duration of 91 days, which could be halved if twice as many resources were assigned to the Electronic network configuration and Electronic network installation tasks, resulting in a duration of 78.5 days.

8 COST ESTIMATION

In the following pages, we can see the cost estimate for the implementation of a company's communications infrastructure.

ESTIMATE BREAKDOWN AND TAKE-OFF LINES

TFM

CODE	DESCRIPTION	QUANTITY	PRICE	AMOUNT
E19	**TELECOMMUNICATIONS AND COMPUTERS**			
E19R	**DATA NETWORK**			
E19RE	**LOCAL AREA NETWORKS (LAN)**			
E19RES	**SWITCH**			
E19RES030	**u SWITCH 48 PORTS LAYER 2**			
	Switch installation of 48 ports compatible with 10/100/1000 Mbps auto-sensing, 19 "rack size not including and included, manageable power supply and a fiber optic port SC compatible with 1000Base-LX (1000Mbps). maximum distance of 10 km, wavelength of 1300nm, SC single-mode (SM) Installed and connected.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*1,270*	*19,25*	*24,45*
	O01OB224 h Telecommunication Installer Assistant	*0,400*	*17,28*	*6,91*
	P22RES030 u Cisco SG300-52 52-Port Gigabit Managed Switch	*16,000*	*2.202,54*	*35.240,64*
	Lump total quantities	1,00		
		1,00	35.272,00	35.272,00
E19RES050	**u SWITCH 48 PORTS LAYER 3**			
	Installation of Switch of 48 ports with 10/100/1000 Mbps, layer 3 with two ports of 2 Gbps, for multimedia applications, 19 "rack size not included and power supply included. Installed and connected.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*1,710*	*19,25*	*32,92*
	O01OB224 h Telecommunication Installer Assistant	*0,600*	*17,28*	*10,37*
	P22RES050 u Catalyst 3750, 48 GbE PoE Ports, 4 SFP Ports,IPS Software	*3,000*	*6.906,05*	*20.718,15*
	Lump total quantities	1,00		
		1,00	20.761,44	20.761,44
	TOTAL E19RES			**56.033,44**
E19RER	**ROUTERS**			
E19RER010	**u ROUTER**			
	Installation of Router and Firewall for Internet access and perimetral security.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,430*	*19,25*	*8,28*
	O01OB224 h Telecommunication Installer Assistant	*0,250*	*17,28*	*4,32*
	P22RER010 u Cisco RV320 Gigabit Dual WAN VPN	*2,000*	*311,59*	*623,18*
	P01DW090 u FirePower 2110	*2,000*	*9.071,16*	*18.142,32*
	Lump total quantities	1,00		
		1,00	18.778,10	18.778,10
	TOTAL E19RER			**18.778,10**
	TOTAL E19RE			**74.811,54**
E19RI	**WIRELESS LOCAL AREA NETWORKS (WLAN)**			
E19RIA	**WIRELESS ACCESS POINT (AP)**			

TFM

CODE	DESCRIPTION	QUANTITY	PRICE	AMOUNT
E19RIA010	u Access Point			
	Installation of a wireless access point the ZoneFlex R500 is the industry's best-performing 2x2 802.11ac indoor WLAN access point, combining Ruckus-patented RF technologies with the new IEEE 802.11ac standard to provide outstanding WiFi performance. The R500 features dual radios, capable of concurrent operation. It features a 5 GHz 802.11a/n/ac radio in a 2x2:2 spatial stream configuration, capable of physical layer rates of up to 867 Mbps. A 2.4GHz 802.11b/g/n radio in a 2x2:2 spatial stream configuration offers an additional 300 Mbps of physical layer throughput. Installed and connected.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*1,300*	*19,25*	*25,03*
	P22RIA010 u , Ruckus ZoneFlex R500 Dual-Band 802.11ac 2X2	*1,000*	*500,00*	*500,00*
	Lump total quantities	20,00		
		20,00	525,03	10.500,60
E19RIA020	u Controller			
	Controller Virtual SmartZone Essentials (Vsz-E), for manage R500 APs			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*3,000*	*19,25*	*57,75*
	P22RIA020 u Virtual SmartZone Essentials (Vsz-E)	*1,000*	*1.240,00*	*1.240,00*
	Lump total quantities	1,00		
		1,00	1.297,75	1.297,75
	TOTAL E19RIA			**11.798,35**
	TOTAL E19RI			**11.798,35**
	TOTAL E19R			**86.609,89**
E19I	**STRUCTURED WIRING SYSTEM**			
E19IC	**CHANNELS AND CABINETS**			
E19IC010	m CHANNEL PVC 60x190 mm			
	Channeling planned to support the SCE, made with PVC channel with 60x190 mm inner cover with p.p. of accessories and register boxes, fully finished.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,180*	*19,25*	*3,47*
	O01OB224 h Telecommunication Installer Assistant	*0,060*	*17,28*	*1,04*
	P15GF120 m PVC gutter cover ext. 60x190 mm	*1,000*	*26,69*	*26,69*
	P15GT100 u Canal.t.ext accessories. 60x190 mm	*0,200*	*5,39*	*1,08*
	Lump total quantities	400,00		
		400,00	32,28	12.912,00
E19IC020	m CHANNEL FOR PERFABRICATED SHEET 100x35 mm TRAY			
	Channeling designed to support the SCE, made with a 100x35 mm galvanized perforated sheet tray, including p.p. of register boxes, fully finished.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,235*	*19,25*	*4,52*
	O01OB224 h Telecommunication Installer Assistant	*0,073*	*17,28*	*1,26*
	P15GH010 m Perforated sheet metal tray 100x35	*1,000*	*7,12*	*7,12*
	P15AH430 u Small material for installation	*0,200*	*1,40*	*0,28*
	Lump total quantities	100,00		
		100,00	13,18	1.318,00

ESTIMATE BREAKDOWN AND TAKE-OFF LINES

TFM

CODE	DESCRIPTION			QUANTITY	PRICE	AMOUNT
E19IC030	**m CHANNELING OF PERFABRICATED SHEET TRAY 100x60 mm**					
	Channeling designed to support the SCE, made with a 100x60 mm galvanized perforated sheet tray, including p.p. of register boxes, fully finished.					
	Breakdown					
	O01OB222	*h*	*Official 1st Telecommunication Installer*	*0,235*	*19,25*	*4,52*
	O01OB224	*h*	*Telecommunication Installer Assistant*	*0,073*	*17,28*	*1,26*
	P15GH050	*m*	*Perforated sheet metal tray 100x60*	*1,000*	*9,91*	*9,91*
	P15AH430	*u*	*Small material for installation*	*0,200*	*1,40*	*0,28*
	Lump total quantities			70,00		
				70,00	15,97	1.117,90
E19IC040	**m PERFABRICATED PVC TRAY CHANNEL 60x75 mm**					
	Channeling to support the SCE, made with a 60x75mm perforated PVC tray, including p.p. of register boxes, fully finished.					
	Breakdown					
	O01OB222	*h*	*Official 1st Telecommunication Installer*	*0,170*	*19,25*	*3,27*
	O01OB224	*h*	*Telecommunication Installer Assistant*	*0,070*	*17,28*	*1,21*
	P15GP020	*m*	*Perforated PVC tray 60x75 mm*	*1,000*	*8,18*	*8,18*
	P15GP140	*m*	*PVC tray cover 75 mm*	*1,000*	*5,35*	*5,35*
	P15AH430	*u*	*Small material for installation*	*0,100*	*1,40*	*0,14*
	Lump total quantities			50,00		
				50,00	18,15	907,50
E19IC050	**m PERFABRICATED PVC TRAY CHANNEL 100x300 mm**					
	Channeling planned to support the SCE made with perforated PVC tray, 100x300 mm, including p.p. of register boxes, fully finished.					
	Breakdown					
	O01OB222	*h*	*Official 1st Telecommunication Installer*	*0,230*	*19,25*	*4,43*
	O01OB224	*h*	*Telecommunication Installer Assistant*	*0,090*	*17,28*	*1,56*
	P15GP100	*m*	*Perforated PVC tray 100x300 mm*	*1,000*	*33,60*	*33,60*
	P15GP080	*m*	*Perforated PVC tray 60x300 mm*	*1,000*	*25,10*	*25,10*
	P15AH430	*u*	*Small material for installation*	*0,100*	*1,40*	*0,14*
	Lump total quantities			50,00		
				50,00	64,83	3.241,50
E19IC110	**u FLOOR RACK CABINET 19 "42 U 2000x600x600 mm**					
	Rack cabinet installed on the 19 "floor of 2000x600x600 mm of sheet steel and glass door, equipped with a lock, with passive ventilation through ventilation slots, rear panel prepared to house a fan, with a capacity of 42 U, including 4 profiles 19 ". Fully assembled and installed.					
	Breakdown					
	O01OB222	*h*	*Official 1st Telecommunication Installer*	*0,250*	*19,25*	*4,81*
	O01OB224	*h*	*Telecommunication Installer Assistant*	*0,250*	*17,28*	*4,32*
	P22IA070	*u*	*Floor rack 19 "42 U 2000x600x600 mm w / door, side and 4 19" profiles*	*1,000*	*810,74*	*810,74*
	P15AH430	*u*	*Small material for installation*	*1,000*	*1,40*	*1,40*
	Lump total quantities			2,00		
				2,00	821,27	1.642,54
			TOTAL E19IC			**21.139,44**

ESTIMATE BREAKDOWN AND TAKE-OFF LINES

TFM

CODE	DESCRIPTION	QUANTITY	PRICE	AMOUNT
E19IB	**TWISTED PAIR WIRING**			
E19IB080	**m HORIZONTAL WIRING UTP CAT. 6 PVC**			
	Horizontal twisted-pair cabling, consisting of 4-pair UTP cable, category 6 PVC, in channel mounting, installed, mounting and connection.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,100*	*19,25*	*1,93*
	P22IB080 m Category 6 UTP horizontal cable (4 pairs) PVC	*1,000*	*0,52*	*0,52*
	P15AH430 u Small material for installation	*1,000*	*1,40*	*1,40*
	Lump total quantities	500,00		
		500,00	3,85	1.925,00
E19IB110	**m 1 m UTP / RJ-45 CAT.6PVC CORD**			
	UTP / RJ-45 patch cord, 1 meter PVC category 6 unit, for patching or PC connection, installed and connected.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,050*	*19,25*	*0,96*
	P22IB290 u UTP / RJ-45 Cable Category 6 PVC 1 m	*1,000*	*4,84*	*4,84*
	P15AH430 u Small material for installation	*1,000*	*1,40*	*1,40*
	Lump total quantities	200,00		
		200,00	7,20	1.440,00
	TOTAL E19IB			**3.365,00**
E19IP	**TWISTED PAIR CONNECTION PANELS**			
E19IP050	**u CONNECTION PANEL 24 PORTS CAT. 6**			
	Installation of a 24-port patch panel for category 6 UTP twisted-pair network cabling, fully equipped, installed and connected.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,400*	*19,25*	*7,70*
	P22IP020 u Connection panel 24 ports RJ-45 Category 6	*1,000*	*51,69*	*51,69*
	P22IM040 u RJ-45 C6 UTP socket connector	*24,000*	*8,03*	*192,72*
	P22IP060 u RJ45 port cover	*24,000*	*0,90*	*21,60*
	P22IP070 u Panel marking plate	*24,000*	*0,88*	*21,12*
	Lump total quantities	28,00		
		28,00	294,83	8.255,24
	TOTAL E19IP			**8.255,24**
E19IF	**OPTICAL WIRING**			
E19IF070	**u SINGLE-MODE ST-ST CORD 1m**			
	Single-mode ST-ST patch cord of 1 meter each, for patching or PC connection, installed and wired.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,050*	*19,25*	*0,96*
	P22IF070 u 1m ST -ST singlemode cord	*1,000*	*11,25*	*11,25*
	P15AH430 u Small material for installation	*1,000*	*1,40*	*1,40*
	Lump total quantities	12,00		
		12,00	13,61	163,32
	TOTAL E19IF			**163,32**

ESTIMATE BREAKDOWN AND TAKE-OFF LINES

TFM

CODE	DESCRIPTION	QUANTITY	PRICE	AMOUNT
E19IM	**JOB POSITIONS**			
E19IM060	**u RJ45 C6 UTP SOCKET**			
	Simple RJ45 category 6 STP socket (not including wiring), made with M 20 / gp5 corrugated PVC pipe conduit, recessed, assembled and installed.			
	Breakdown			
	O01OB222 h Official 1st Telecommunication Installer	*0,200*	*19,25*	*3,85*
	O01OB223 h Oficial 2ª Instalador telecomunicación	*0,200*	*18,01*	*3,60*
	P22IM060 u RJ-45 C6 UTP socket connector	*1,000*	*10,93*	*10,93*
	P22IM070 u Front 45x45 for 1RJ-45 C6 /C5e	*1,000*	*2,15*	*2,15*
	P22IM080 u Label for taking	*1,000*	*0,44*	*0,44*
	Lump total quantities	500,00		
		500,00	20,97	10.485,00
E19IM080	**u BUILT-IN BOX 3 MODULES WHITE**			
	Embedding box with IP4X of 3 modules composed of a frame with frames of 3 modules in white finish, 1 double Schuko base, 1 click cut-off terminal with LED, white finish, 1 Double Schuko base, 1-click cut terminal with LED, red finish , UPS line indicator and 2 Voice and Data flat plates with 1 RJ45 category 6A FTP connector, graphite finish. Manufactured in thermoplastic, self-extinguishing and halogen-free materials that guarantee the non-propagation of the flame by fire as well as low toxicity in the case of smoke emission. It incorporates a metal separating screen (grounded) between the electrical zone and the voice and data zone that ensures electromagnetic immunity, avoiding data transmission errors. Allows the incorporation of security elements in DIN rail format. Product design carried out under the Safety Requirements of Directive 2006/95 / CE (low voltage) through compliance with the UNE-EN-60.670-1: 2014 standard. Fully assembled and installed.			
	Breakdown			
	O01OA030 h First officer	*1,300*	*19,86*	*25,82*
	O01OA050 h Assistant	*0,600*	*17,68*	*10,61*
	P22IM610 u 3-module flush-mounting box without frame	*1,000*	*11,54*	*11,54*
	P22IM190 u Frame w / cover for flush-mounted box 3 modules snow white	*1,000*	*16,65*	*16,65*
	P22IM300 u Double Schuko snow white	*1,000*	*14,88*	*14,88*
	P22IM310 u Double red Schuko	*1,000*	*15,31*	*15,31*
	P22IM110 u V&D board 2 RJ45 cat.6 UTP connectors snow white	*1,000*	*28,32*	*28,32*
	P15AH430 u Small material for installation	*0,280*	*1,40*	*0,39*
	Lump total quantities	50,00		
		50,00	123,52	6.176,00

TFM

CODE	DESCRIPTION	QUANTITY	PRICE	AMOUNT
E19IM100	**u COMPLETE FLOOR BOX 3 RAISED FLOOR MODULES**			
	Complete floor box with 3 modules with IP4X for installation on raised floors (depth adjustable from 90 to 120) in gray finish consisting of 1 trim cover in gray finish, 1 mechanism-holder frame with 3 modules in snow white finish (included), 1 double Schuko socket with 1 click cut-off terminal block in snow white finish, 1 red double Schuko socket with 1-click cut terminal connection, SAI line indicator, both with voltage indicator light and 2 inclined Voice and Data plates with 1 RJ45 category 6 connector UTP in snow white finish. Manufactured in thermoplastic, self-extinguishing and halogen-free materials that guarantee the non-propagation of the flame by fire as well as low toxicity in the case of smoke emission. Product design carried out under the Safety Requirements of Directive 2006/95 / CE (Low Voltage) by means of compliance with the UNE-EN-60.670-1: 2006 standard, equivalent to the IEC-60670 standard. CE marked product. Fully assembled and installed.			
	Breakdown			
	O01OA030 h First officer	*2,000*	*19,86*	*39,72*
	O01OA050 h Assistant	*1,400*	*17,68*	*24,75*
	P22IM260 u Floor box 90 mm with 3 modules gray	*1,000*	*51,22*	*51,22*
	P22IM290 u Flush cover for floor box 3 mod gray	*1,000*	*6,80*	*6,80*
	P22IM300 u Double Schuko snow white	*1,000*	*14,88*	*14,88*
	P22IM310 u Double red Schuko	*1,000*	*15,31*	*15,31*
	P22IM180 u V&D inclined plate 2 RJ45 cat.6 UTP connectors snow white	*1,000*	*28,59*	*28,59*
	P15AH430 u Small material for installation	*0,280*	*1,40*	*0,39*
	Lump total quantities	400,00		
		400,00	181,66	72.664,00
	TOTAL E19IM			**89.325,00**
E19IS	**UNINTERRUPTED POWER SUPPLY SYSTEMS (UPS)**			
E19IS040	**u UPS SAFT (ON-LINE) 1250 VA**			
	Uninterruptible Power Supply (UPS), on-line operation, nominal power 1,250 VA, power supply 220 V +/- 1%, 50 Hz +/- 5%, zero switching time, sealed lead-acid battery, output signal 220 V . +/- 1% sinusoidal, capable of withstanding a permanent overload of 20%. Autonomy 15 minutes, manual static bypass, harmonic distortion less than 1.5%, with double-shielded isolation transformer, membrane keyboard, noise level less than 50 dB, operation by Pulse Width Modulation (PWM), with signaling optics and acoustics. Installed, including packaging, transportation, assembly and connection.			
	Breakdown			
	O01OB200 h 1st electrician officer	*2,500*	*19,25*	*48,13*
	P22IS050 u S.A.I. Saft (Off-Line) 1250 VA	*1,000*	*967,45*	*967,45*
	P15AH430 u Small material for installation	*10,000*	*1,40*	*14,00*
	Lump total quantities	4,00		
		4,00	1.029,58	4.118,32
	TOTAL E19IS			**4.118,32**
	TOTAL E19I			**126.366,32**
	TOTAL E19			**212.976,21**
	TOTAL			**212.976,21**

9 CONCLUSIONS

At this point in the memory of this final master's work and after carrying out all the dimensioning of the communications network and its securing, it can be said that:

- The guidelines offered by cisco, for the realization of a hierarchical network, help to dimension the communications infrastructure, as well as to be able to have a modular network, where the different functions can be separated, as well as a robust and flexible network to cover new technologies or infrastructure growth.
- The modularity of the network has made it possible to apply QoS techniques to the different services of the company, such as VoIP or video calls, thus ensuring that the services are fluid and that the network functions better.
- The workers of the fictitious company, the subject of this master's degree thesis, will be able to make use of a secure network, where it is tried to avoid attacks by malicious agents through layer 2 security functions such as DHCP Snooping, IP Source Guard or ARP Inspecction and perimeter security functions, such as the VPN or the DMZ zone.
- In addition, the workers of the company will have a wired network and also a Wi-Fi network that will allow them to move around the building.
- Thanks to the implementation of VPN, company workers will also be able to make use of teleworking, and access the same resources that they can physically access in the company.

10 LINES OF THE FUTURE

The fact of having created a modular, robust and flexible hierarchical network, as mentioned above, makes it possible to expand the infrastructure quite easily. Therefore, if the company needed more resources for its growth, it would only be necessary to expand the infrastructure already created initially.

The steps to follow would be very simple, firstly, the access layer would be covered and, if the size of the company was much higher than the current one, the distribution layer would also be expanded.

On the other hand, if the needs of the company changed and they decided to create a new physical headquarters, once the communications infrastructure was resized, another VPN Gateway to Gateway could be done without any problem to interconnect them and, in this way, the new headquarters could access all the company's services in a totally transparent way, as is currently the case with the two headquarters created in this Master's Thesis.

Apart from the growth of the company, and with it the infrastructure, it is proposed to carry out a monitoring system of the network equipment to detect possible drops, breaks or failures and, in this way, alleviate the problems caused by a network drop.

Thanks to the monitoring system, the people in charge of network maintenance will be able to monitor various aspects of the network and its operation, such as traffic, bandwidth use and activity time.

Through this monitoring of the network, you can obtain a clear image of all the devices that make up the network, as well as see the behavior of the data on the network and quickly identify and correct problems that may cause poor performance or cause failures. With this information, performance reports of network components can be made in a given period and, in this way, anticipate the needs of the company, being able to update or build a new infrastructure.

In addition, through monitoring, the normal state of the network will be known and in case of seeing an anomaly, such as an increase in traffic, it will be possible to identify if it is a threat to the security of the network.

11 BIBLIOGRAPHICAL REFERENCES

Cisco (2021, February 04). Cisco Catalyst 9300 Series Switches. Retrieved from https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/index.html

Address Resolution Protocol (ARP) Configuration on the 200/300 Series Managed Switches. (2019, May 09). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-200-series-smart-switches/smb87-address-resolution-protocol-arp-configuration-on-the-200-300.html

Backup and Restore the Configuration Files on RV320 and RV325 VPN Routers. (2019, April 24). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb4125-backup-and-restore-the-configuration-files-on-rv320-and-rv32.html

Bandwidth Management Configuration on RV320 and RV325 VPN Router Series. (2019, April 24). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb4165-bandwidth-management-configuration-on-rv320-and-rv325-vpn-ro.html

Cisco Firepower 2100 Series - Cisco Firepower 2100 Series. (2021, February 22). Retrieved from https://www.cisco.com/c/en/us/products/security/firepower-2100-series/index.html

Cisco - Guía de administración de Cisco RV320/RV325. Retrieved from https://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv320/administration/guide/es/rv32x_ag_es.pdf

Configuraciones de la habitación de la Seguridad en el Switches manejado 300 Series. (2019, May 09). Retrieved from https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb1076-security-suite-settings-on-300-series-managed-switches.html

Configuración de Seguridad de puerto en el Switches manejado 200/300 Series. (2019, May 09). Retrieved from https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-200-series-managed-switches/smb85-port-security-configuration-on-the-200-300-series-managed-sw.html

Configuración de Seguridad de puerto en el Switches manejado 300 Series. (2019, May 09). Retrieved from https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb4810-port-security-configuration-on-the-300-series-managed-switch.html

Configure QoS (Quality of Service) Queue Mapping on the RV320 and RV325 VPN Router Series. (2019, April 24). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb4261-configure-qos-quality-of-service-queue-mapping-on-the-rv320.html

Cuentas de usuario de la configuración para aumentar la Seguridad en Cisco Smart o Switch manejado. (2019, May 09). Retrieved from https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-250-series-smart-switches/smb4805-configure-user-accounts-to-enhance-security-on-a-cisco-smart.html

Gateway to Gateway Virtual Private Network (VPN) Configuration on RV320 and RV325 VPN Router Series. (2019, May 14). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb4270-gateway-to-gateway-virtual-private-network-vpn-configuration.html

Hierarchical Network Design: Cisco Hierarchical Model. (2019, November 12). Retrieved from https://ccnacompletecourse.blogspot.com/2019/11/hierarchical-network-design.html

Implementing Quality of Service Policies with DSCP. (2017, May 25). Retrieved from https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

Port Security Configuration on the 200/300 Series Managed Switches. (2019, May 09). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-

business-200-series-managed-switches/smb85-port-security-configuration-on-the-200-300-series-managed-sw.html

RADIUS Configuration on the 200/300 Series Managed Switches. (2019, May 09). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-200-series-managed-switches/smb102-radius-configuration-on-the-200-300-series-managed-switches.html

SG300-10 with Wireless Secured and Guest access. (2012, March 21). Retrieved from https://community.cisco.com/t5/small-business-switches/sg300-10-with-wireless-secured-and-guest-access/td-p/1923863

System Log Configuration on RV320 and RV325 VPN Router Series. (2019, April 24). Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb4221-system-log-configuration-on-rv320-and-rv325-vpn-router-serie.html