Loyola University

Computer Networks

FINAL PROJECT

Authors:
Martyna Baran
Zuzanna Jarlaczynska

November 27, 2023

Contents

1 Network Requirements

Our goal is to design Loyola University's IT Network, including Sewilla, Cordoba and Granada campus. The projects needs to fulfill following requirements:

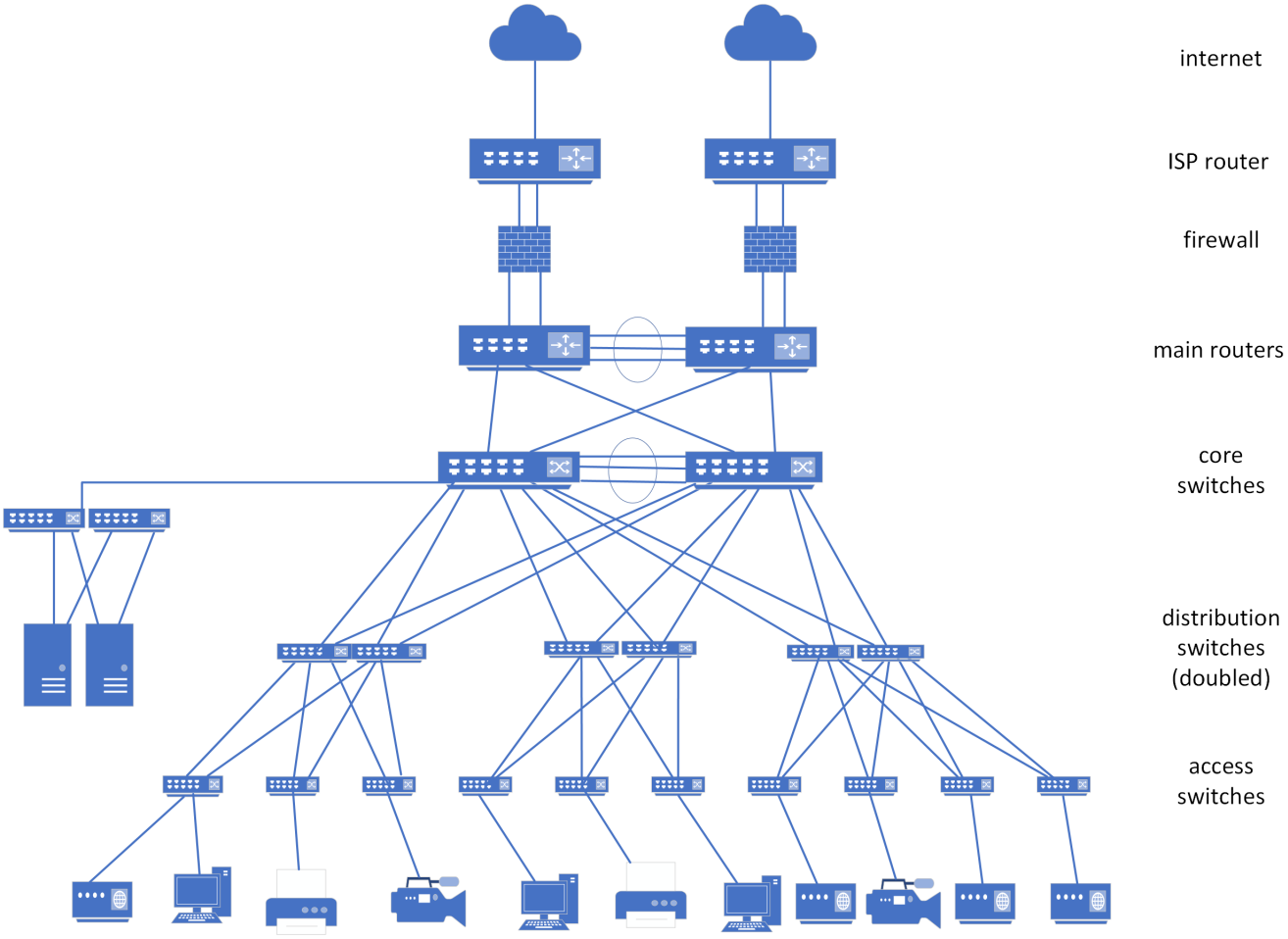
Feature	Sevilla	Cordoba	Granada
No of buildings	4	4	3
No of students	3000	2000	200
No of professors	350	250	25
No of staff	100	100	20
Area (m2)	29000	11286	9000

Our main aim is to handle network traffic, provide fast and reliable connection that will ensure security of users and the system. Thanks to a well structured network, we will provide required services and sufficient connection, reducing also the problem of non-reliability, non-availability and any other problem that may occur in campus network design. Important aspect of our work is to provide stable internet connection, keeping in mind the security of data transfer. Our major objective will be to make a secure system that is able to perform the following system functionalities:

- Quick and reliable communication
- Robustness to failure
- Network security and Quality of Service
- Efficient IP Address management
- Ease of implementation and base for future expansion of the network

In our work, we take into account the requirements of the users and the necessary technological solutions for their implementation. The network is expected to be cost effective and observe the information security rules of the CIA (confidentiality, integrity and availability). We assume that our building is already wired. We do not take into account the costs of power supply, maintenance, conservation etc.

2 Network Visualisation



3 Overview

The network is expected to have a hierarchical model that allows it to meet evolving needs. The modular design makes the network easy to scale, understand, and troubleshoot by promoting deterministic traffic patterns. Our model is an example of a server-based network, also known as a "client/server" networks. They rely on special-purpose computers called servers that provide centralized management, coordination and support to other computers, and resources on the network. In a server-based network, dedicated servers are installed for the purpose of providing network services such as: user logins, maintaining the authorized user accounts database, storing files, providing resources and shared applications to users, as well as network security. Server-based networks are scalable and allow for future network growth and expansion. These networks are robust and can support a large number of users depending on how the server is configured.
In the case of our university, the internet provider is Eduroam. The security of communication between the routers is ensured by the use of side-to-side VPN technology. The building block components for every campus are the access layer, the distribution layer, and the core (backbone)

layer, which will be discussed later. In a hierarchical design, the capacity features and functionality of a specific device are optimized for its position in the network and the role that it plays.
Each campus represents a local branch of our network and their structure is analogous, but only adapted to the specific requirements of the university. For this reason, we will present objectives of each layer and then indicate the detailed demands for each campus.

Servers

On the Seville campus, we also include a server room with the following servers:

- DNS (Domain Name Service) - is a key component of the Internet's structure. Its main purpose is to convert user-friendly domain names into corresponding IP addresses. This process enables communication between people and computers on the network, eliminating the need to remember and type in IP addresses. To improve performance, DNS servers can store (cache) information for a certain period of time. If a server has previously processed a query for a particular domain, it can respond directly instead of routing the query to the root servers.
- DHCP (Dynamic Host Configuration Protocol) - is a management protocol that plays a key role in the dynamic allocation of IP addresses to devices on a network. Its main purpose is to facilitate the communication of devices on the network by automatically assigning IP addresses, eliminating the need to manually configure each device. In the traditional approach, network administration would involve assigning static IP addresses to each device. DHCP introduces dynamic assignment, meaning that IP addresses are assigned to devices temporarily when they are needed and then released when they are no longer in use. New devices can automatically obtain an IP address without administrator intervention.
- EMAIL - is important in managing electronic correspondence for students and teachers, providing a reliable platform for communication and access to Loyola Online. Integration with Loyola Online enables users to access various online services and resources with a single set of credentials. The email server adheres to data protection regulations to safeguard the privacy of student and teacher information.

---

4 Hierarchical Design

Core Layer

The Core Layer serves as the robust backbone of our network infrastructure, playing a key role in ensuring seamless connectivity for all components within our system. Its significance lies in its speed and resilience, as every face of our network relies on it for uninterrupted connectivity.
At the heart of the Core Layer are innovative routers characterized by their exceptional speed and resilience. These switches, boasting the highest model numbers, are strategically positioned to merge geographically separated networks and facilitate the swift transfer of information across the entire network.

Distribution Layer

In a large LAN environment, there often arises a need for the deployment of multiple Distribution Layer switches to address specific architectural and performance considerations. The strategic placement of distribution layer switches becomes imperative, especially in scenarios where access layer switches are distributed across geographically disparate buildings. One compelling reason for the deployment of multiple distribution layer switches is the optimization of fiber-optic runs between buildings. By siting a distribution layer switch in each building where access layer switches are located, we mitigate the need for costly and extensive fiber-optic cabling, enhancing both efficiency and cost-effectiveness.
Moreover, the distribution layer serves as a critical aggregation point for nodes from the access layer, effectively shielding the core from the potential strain of high-density peering. This architectural decision contributes not only to improved network performance but also to the scalability and resilience of our overall network infrastructure.
A key attribute of the distribution layer is its role as a fault boundary, creating a logical isolation point in the event of a failure originating in the access layer. This intrinsic fault tolerance enhances the network's reliability by containing and mitigating those issues.

Access Layer

The access layer is the point at which user-controlled and user-accessible devices are connected to the network. The access layer provides both wired and wireless connectivity and contains features and services that ensure security and resiliency for the entire network. End devices, representing the diverse array of user-controlled hardware, establish their connection with the Access Layer through the utilization of fast Ethernet and 802.11 (Wi-Fi) technology. This strategic choice is informed by the dual advantages of speed and cost-effectiveness inherent in these technologies. Emphasizing accessibility and user-friendly connections, the Access Layer aligns with our commitment to providing a network environment that is both intuitive and adaptable to the diverse needs of end-users. The deployment of this layer not only supports the varied connectivity requirements of end devices but also establishes a solid foundation for the entire network infrastructure.

---

5 Network structure

At the very top of the structure is the connection to the Internet Service Providers - ISPs. In this case, they provide two routers, which are the base of the Internet connection. Subsequently, these routers establish connections with the pair of routers procured by the university. To fortify the network against potential threats, a firewall is strategically positioned between these two layers to act as a protective barrier. Its continuous monitoring and filtering capabilities not only bolster our defense against potential threats but also contribute to the overall reliability and speed of our network. Consequently, our network stands as a fast, reliable, and secure gateway, ensuring safe and uninterrupted access to the Internet for all users.
Critical to the seamless operation of this infrastructure are the cable connections interconnecting various devices. In order for the system to be able to cope with the amount of information that

will flow through it, it is necessary to introduce aggregation, i.e. multiple cable connections, which provides our system with redundancy. In this way, the security of the network will also increase, as it will not rely solely on single cable connections.
Next, we have opted for a dual-switch configuration in the Core Layer, acknowledging the associated costs but prioritizing heightened reliability. This redundancy ensures continuous connectivity even in the event of a failure in one of the switches. There will be several links provided between them and also between the upper layer.
We have decided to install two distribution layer switches for each building on the campus. Additionally, we assume that in the main building of each campus, there is a server room, where Internet Service Provider (ISP) routers, main routers, core layer switches, Wifi controller and servers will be housed. To prevent network overload due to the volume of information flowing through these connections, this room will be equipped with two additional distribution layer switches. These switches will be connected between each other and have several links to the Core Layer. This design choice is expected to contribute significantly to load balancing, Quality of Service (QoS), and streamlined provisioning – key considerations for an efficient and high-performance distribution layer in our network architecture. As we move forward with the implementation, this distribution layer design will play a crucial role in optimizing network resources, enhancing fault tolerance, and providing the necessary scalability to meet the performance goals of our network.
Considering the access layer, on each floor we plan to deploy three switches for cameras (approximately 35 per floor), Access Points (15 per floor), and printers. In addition, rooms for secretarial staff, support staff, and teachers will be equipped with separate access switches. Therefore, the number of devices per floor may vary, but we always anticipate a 30% provision in the number of available ports. The libraries, due to the limited number of devices, will not receive dedicated distribution layer switches. Instead, the connection will be consolidated with 2 access switches, which will be used by all end devices and access points.

---

6 Ways of Connecting Layers

In terms of connections between the layers of our project, we have adopted different approaches due to the specific requirements and characteristics of each layer.

1. **Connection between Core and ISPLayer, Core and Distribution Layer, Distribution and Access Layer**
   Fiber Optic Cable: We decided to use fiber optic cable for the connection between the mentioned layers. This choice is based on the speed and high reliability of this medium. Fiber optic cable perfectly meets the requirements for the connections in the layers that are crucial for the operation of the entire network. Each connection between core and distribution switches is made by two aggregated links using SFP+ transceiver (2x10Gbs).

2. **Connection between Access Layer and end devices**
   1000Base-T (Gigabit Ethernet) cable - UTP: For the connections between the Access Layer and end devices, we decided to use Gigabit Ethernet cables from the UTP (Unshielded Twisted Pair) category. This standard offers a bandwidth of 1 gigabit per second, which is sufficient

for connections at this stage of the network. It is also a cost-effective solution, which is important given the scale of the project.

In both cases, for the connections between the Core and Distribution Layer and between the Distribution and Access Layer, we are implementing redundancy solutions. This ensures that, if one connection fails, the system automatically switches to the other, ensuring continuity of the network.

---

7 VLAN and IP Addressing

7.1 VLAN

A VLAN (Virtual LAN) is a logically separate network of devices within another, larger physical network. The devices that make up a VLAN, irrespective of their physical location (the switch to which they are connected), can communicate freely with each other and at the same time are separated from other VLANs, which means that at the switch level, there is no possibility for devices belonging to two different VLANs to communicate with each other.
Taking these aspects into account, we decided to divide our network into the following VLANs:

- Administration
- Secretariat
- Professors
- Students (one for each lecture building)

Each VLAN with mask /22 can accommodate 1024 devices, which gives us sufficient resources to realise and expand our network. In order to transmit frames from different VLANs between switches via a single link, we must enable the transmission of frames within different VLANs on these links - the so-called trunk. This is necessary in our case, because not all devices in one VLAN will be connected to the same switch. As the structure of the university network is almost identical for each campus, we decided to show the division example for Sevilla.

VLANs for Sevilla campus

VLAN Name	Network Address	Subnet mask
Students 1	10.1.4.0/22	255.255.252.0
Students 2	10.1.8.0/22	255.255.252.0
Students 3	10.1.12.0/22	255.255.252.0
Professors	10.1.16.0/22	255.255.252.0
Secretariat	10.1.20.0/22	255.255.252.0
Administration	10.1.24.0/22	255.255.252.0
End devices	10.1.28.0/22	255.255.252.0
Security	10.1.32.0/22	255.255.252.0
Wifi access 1	10.1.36.0/22	255.255.252.0
Wifi access 2	10.1.40.0/22	255.255.252.0
Wifi access 3	10.1.44.0/22	255.255.252.0

7.2 Addressing

In our network we use both static and dynamic addressing. Dynamic addressing reduces the configuration tasks required to connect end systems to an internetwork. Dynamic addressing also supports users who change their localization and place of work. DHCP protocol minimizes the IP and system configuration tasks. On the other hand, static addresses are used for servers, routers, switches, printers and other devices that stay in the same place.

---

8 Cost Estimation

Role	Device	Number	Cost per unit (USD)	Total cost
Router	7613-S323B-8G-P Cisco 7613 Router	12	29,000.00	348,000.00
Core switch	Cisco Catalyst 9500 series, C9500-48X-A	6	18,386.00	110,300.00
Distribution Switch	Cisco Catalyst 9400 Series C9400-LC-48P	17	8,871.64	150,960.00
Access Switch	Cisco Catalyst 9200 C9200-48P	74	8,967.00	643.578.00
Access Point	Cisco Catalyst 9115AX	178	1,590.00	282,020.00
Server	Smart Selection PowerEdge R750 Rack Servidor	5	4,911.39	25,000.00
Wi-Fi Controller	Cisco Catalyst 9800-80 Wireless Controller	1	30,380.70	30,380
			SUM	1,600,000.00

9 Devices Specification

- MAIN ROUTER - **7613-S323B-8G-P Cisco 7613 Router**
  The 7613-S323B-8G-P Cisco 7613 Router is a high-performance router designed for deployment at the network edge where performance, IP services, redundancy and fault resiliency are critical requirements. It enables Carrier Ethernet service providers to deploy an advanced network infrastructure that supports a range of IP video and triple-play (voice, video, and data) system applications in both the residential and business services markets. The Cisco 7613 enables enterprises to deploy advanced WAN and metropolitan-area network (MAN) networking solutions necessary to succeed in demanding, high-traffic environments.

- CORE LAYER - **C9500-48X-A Catalyst 9500 48-port switch**
  The Cisco Catalyst 9500 Series Switches are the next generation of enterprise-class core and aggregation layer switches, supporting full programmability and serviceability. Based on an x86 CPU, the Catalyst 9500 Series is Cisco's lead purpose-built fixed core and aggregation enterprise switching platform, built for security, IoT, and cloud. The Catalyst 9500 Series is the industry's first purpose-built 40 Gigabit Ethernet line of switches targeted for the enterprise campus.

- DISTRIBUTION LAYER - **Cisco Catalyst C9400-LC-48P**
  Catalyst 9400 Series switches provide unparalleled investment protection with a chassis architecture that supports up to 9 Tbps of system bandwidth and unmatched power delivery with high density IEEE 802.3bt PoE (60W and 90W).

- ACCESS LAYER - **C9200-48P-A**
  C9200-48P-A is the Catalyst 9200 48-port PoE+ Switch, with Network Advantage software. Cisco Catalyst 9200 Series switches extend the power of intent-based networking and Catalyst 9000 hardware and software innovation to a broader set of deployments. With its family pedigree, Catalyst 9200 Series switches offer simplicity without compromise – it is secure, always on, and IT simplified. Important aspect of choosing an access layer switch is a PoE parameter. Power over Ethernet (PoE) is technology that passes electric power over twisted-pair Ethernet cable to powered devices (PD), such as wireless access points, IP cameras, and VoIP phones in addition to the data that cable usually carries. It enables one RJ45 cable to provide both data connection and electric power to PDs instead of having a separate cable for each.

- ACCESS POINTS - **Cisco Catalyst 9115AX**
  Cisco Catalyst 9115AX, one of the Cisco Catalyst 9000 family of products is the complete foundation for the modern intent-based network—it's simple to operate and has great potential to meet growing business demands. The new era of networking must be designed for wireless and at the forefront of the Wi-Fi 6 standard, along with the wired infrastructure needed to meet expectations.

- SERVER - **The Dell PowerEdge R750**
  The Dell PowerEdge R750, powered by the 3rd Generation Intel Xeon Scalable processors is a rack server to address application performance and acceleration. The PowerEdge R750, is a dual-socket/2U rack server that delivers outstanding performance for the most demanding workloads.

- Wi-Fi CONTROLLER - **Cisco Catalyst 9800-80 Wireless Controller**
  The Cisco Catalyst 9800-80 is a modular wireless controller with optional 100 Gigabit Ethernet (G) modular uplinks and seamless software updates for large enterprises and campuses. It is feature rich and enterprise ready to power your business-critical operations and transform end-customer experiences. It has a maximum number of 6000 access points which fulfills our demandings.

References

[1] University Loyola Andalucia. Available from World Wide Web: (https://www.uloyola.es/)

[2] Campus LAN and Wireless LAN Solution Design Guide. Available from World Wide Web: (https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide).

[3] Network Design Project Proposal- Part I. Available from World Wide Web: (https://www.academia.edu/NetworkDesign-Project-Proposal-Part-I)

[4] Plan, Design and Simulation of University Network", E. Longinus, M. Washington, N. Uchechukwu, C. Owuamanam