Design and Implementation of Multi-VLAN Campus Network Architecture with Raspberry Pi Routing and LuCi Management

Gabriel Minda y Diego Ruiz

Faculty of Technical Sciences, International University of Ecuador

Network Information Communication Technology

Steven Vinueza, M.Sc.

December 14th, 2025

Table of Contents

Table of Tables

Abstract

This academic report details the design, implementation, and verification of a Multi-VLAN Campus Network that uses a Raspberry Pi as the central Core Router, managed through the LuCi web interface. The main objective was to achieve logical segmentation of critical services: microservices (VLAN 10), streaming (VLAN 20), email (VLAN 30), and gaming (VLAN 40) within a Layer 2 switching infrastructure. Address planning was based on the efficient variable length subnet mask (VLSM) method over the 10.10.0.0/16 space. For Layer 2 resilience, etherChannel link aggregation was implemented, combining the PAgP and LACP protocols. The Raspberry Pi was configured under the router-on-a-stick model, with NAT masquerading and strict firewall policies to control inter-VLAN traffic flow. Verification results confirmed full functionality: the Raspberry Pi firewall selectively allowed the required communication while blocking unauthorized traffic. EtherChannel redundancy tests were successful, and the operability of application layer services (FastAPI, aiosmtpd, VLC, Counter-Strike) validated the robustness of the routing and security implemented. It is concluded that the Raspberry Pi, managed through LuCi, is a viable and economical platform for implementing advanced network architectures.

Keywords: Raspberry Pi, VLAN, Router-on-a-Stick, LuCi, VLSM, EtherChannel, PAgP, LACP, NAT, Firewall, Campus Network, Inter-VLAN Routing.

Introduction

The evolution of modern networks, particularly in campus and enterprise environments, requires an architecture that combines high availability with strict security segmentation. The central problem addressed in this project lies in the need to logically isolate disparate services, from latency-sensitive microservice traffic to high-bandwidth multimedia streams, within a shared physical infrastructure, while maintaining a centralized and securely managed access point to the wide area network (WAN). Traditionally, implementing such designs has relied on expensive specialized routing hardware, presenting a significant financial barrier for educational or research projects with limited budgets (George, 2025).

This study proposes and evaluates an alternative solution: the use of a Raspberry Pi as a layer 3 routing device, capable of handling complex networking functions such as inter-VLAN routing, NAT, and packet filtering (firewall). The main objective of the project was to demonstrate the technical feasibility and cost efficiency of this platform by integrating it as the core of a four-switch multi-VLAN campus network. The implementation methodology is characterized by the strategic use of the LuCi interface for configuring network services on the Pi, minimizing the operational complexity associated with the command line in managing VLAN subinterfaces and Netfilter rules.

The network infrastructure was designed according to principles of optimization and resilience. Layer 2 was configured to maximize availability through the implementation of EtherChannel, using a mixed PAgP and LACP scheme for trunk link redundancy. At Layer 3, planning was guided by the VLSM scheme for efficient IP address space distribution. The implementation methodology is characterized by the strategic use of the LuCi interface for Raspberry Pi management, simplifying the configuration of VLAN subinterfaces and Netfilter

rules. The rigor of the project was validated by integrating four critical Application Layer services, each segregated into its own VLAN, whose required communications (e.g., SMTP traffic between VLAN 10 and VLAN 30) are explicitly governed by Core Router Pi policies.

The subsequent sections of this report will detail the theoretical framework underpinning each component, the step-by-step implementation methodology, the results obtained from connectivity and service verification tests, and finally, a critical discussion on the performance of the architecture and its implications for future deployments.

Objectives

General Objective

Design and implement a secure, segmented, high-availability campus network architecture using a Raspberry Pi as the core router to centralize inter-VLAN routing and security policies, and validate the full operability of Layer 7 services, demonstrating the viability of advanced, cost-effective networking solutions.

Specific Objectives

- Configure the Raspberry Pi as a Router-on-a-Stick with VLAN subinterfaces and VLSM addressing, enabling NAT for WAN connectivity.
- Implement EtherChannel with PAgP and LACP for trunk redundancy and configure the Pi's firewall (via LuCi) to apply minimum privilege inter-VLAN access rules.
- Verify the correct operation of Layer 7 services (SMTP, Streaming, Game Server), ensuring that critical communications operate in accordance with security policies.

Theoretical Framework

Principles of Network Segmentation Using VLANs

The implementation of VLANs arises from the modern demand for logical isolation and traffic governance within a physical network. By establishing broadcast limits (broadcast domains) at the switch level, VLANs mitigate network congestion and, fundamentally, strengthen security posture. In the present architecture, the division was made into four VLANs: VLAN 10 (Microservices and Clients), VLAN 20 (Streaming Server), VLAN 30 (Mail Server), and VLAN 40 (Game Server), ensuring that each service and its users operate within their own isolated domain, which is fundamental to the principle of separation of duties (De Luz, 2025).

Inter-VLAN Routing Model and Router-on-a-Stick

The Router-on-a-Stick was selected as the inter-VLAN routing paradigm, a highly economical solution in terms of Core Router physical port consumption. The operating principle is based on the router's ability to accept frames tagged with the IEEE 802.1Q standard through a single physical trunk interface. This interface (eth0 of the Raspberry Pi) is subdivided into multiple logical subinterfaces, each acting as the gateway for a specific VLAN. The router performs the function of decapsulating and encapsulating the tagged frames to route traffic from one VLAN to another (Academy, 2024).

Address Space Optimization Using VLSM

The Variable Length Subnet Mask (VLSM) technique was applied to perform a hierarchical and efficient allocation of the IP address space 10.10.0.0.0 VLSM allows the subnet mask size to vary according to the actual number of hosts required in each segment. Table 1 details the addressing plan, showing the drastic reduction in IP address waste through the assignment of the mask that best fits the needs of the hosts in each VLAN (CCNA, 2023).

Table 1

IP Addressing Plan and VLSM Assignment

VLAN	Name	Hosts	Mask	Subnet	Gateway
VLAN 30	Mail Server	50	/26	10.10.0.0/26	10.10.0.1
VLAN 20	Streaming	40	/26	10.10.0.64/26	10.10.0.65
VLAN 10	Microservices	30	/27	10.10.0.128/27	10.10.0.129
VLAN 40	Counter Strike	15	/27	10.10.0.160/27	10.10.0.161

Note. The table details the Variable Length Subnet Mask (VLSM) addressing scheme applied to the 10.10.0.0/16 block. It shows the network segmentation with the subnet size optimized for the specific host requirements of each VLAN, and the assignment of the first host of each subnet as the gateway configured in the subinterfaces of the Raspberry Pi router.

EtherChannel Integration

EtherChannel technology was fundamental to the switching matrix. By grouping several physical links into a single logical channel (Port Channel), Layer 2 load balancing and fault tolerance are achieved. The implementation was carried out using two protocols: PAgP (Port Aggregation Protocol) on the Switch0 to Switch1 link, and LACP (Link Aggregation Control Protocol), the industry standard (802.3ad), on the Switch1 to Switch2 link (CISCO, 2025).

Methodology

The implementation of the network infrastructure was carried out through a systematic configuration of the main router (Raspberry Pi) and the layer 2 switches. The use of the LuCi graphical interface for the Raspberry Pi accelerated the configuration of routing and security policies, minimizing common syntactic errors associated with command-line configuration.

Routing and Security Configuration

The Raspberry Pi configuration focused on defining interfaces, activating Network Address Translation (NAT), and applying detailed firewall policies.

Physical and Logical Interface Definition

Through the LuCi control panel, the **WAN** and the **Trunk LAN Interface (eth0)** were identified and configured. Subsequently, the logical sub-interfaces associated with eth0 were created to manage VLAN traffic. Each sub-interface was assigned its corresponding *VLAN ID* and the *Static Gateway* with its subnet mask, in accordance with the pre-established VLSM plan.

Network Address Translation (NAT)

The NAT Masquerading service was explicitly enabled within the *Firewall* and *Netfilter* rules for the WAN interface. This action ensures that internal traffic originating from local networks can access the Internet using a single public IP address.

Firewall Policy Implementation

Network security was based on the principle of least privilege, configuring explicit *forwarding rules* in the LuCi *Firewall* section. The established rules were as follows:

- **Email Access:** Explicit permission was granted for TCP/25 (SMTP) traffic, allowing communication from VLAN 10 to the specific address of the Mail Server, located in VLAN 30.

- **Streaming Media Access:** Multimedia traffic (UDP/TCP port ranges) was allowed from VLAN 10 to VLAN 20.
- **Gaming Communication:** Bi-directional permissions were implemented for API traffic (TCP) and game traffic (UDP) between VLAN 10 and VLAN 40.
- **Outgoing TLS Traffic:** All outgoing Internet traffic was authorized, specifically including TCP/587 for the use of TLS in communication with external mail servers.

Switch Configuration

The configuration of the four Layer 2 switches (Cisco 2960-24TT) focused on network segmentation using VLANs, defining port modes, and implementing link aggregation (EtherChannel).

VLAN Definition and Access Ports

All four VLANs (10, 20, 30, and 40) were created on all switching devices. The access ports connected to the *end-devices* were statically configured in **Access** mode and assigned to their corresponding VLAN to ensure segmentation.

Trunk Port Configuration

The interconnection links (Switch-to-Switch and Switch-to-Router) were configured in Trunk mode, utilizing the IEEE 802.1Q encapsulation protocol. This configuration ensured that traffic from VLANs 10, 20, 30, and 40 could be transported across these links.

EtherChannel Implementation

Link aggregation was implemented to increase bandwidth and provide redundancy on the trunk links:

- **Switch0 and Switch1 (PAgP):** The links were grouped into a logical *Port-Channel*, and the physical interfaces were configured using the PAgP protocol. Switch0 was configured to actively initiate negotiation (*Desirable* mode).
- **Switch1 and Switch2 (LACP):** A separate *Port-Channel* was created. The physical interfaces were configured with the LACP protocol (in *Active* or *Passive* mode) to dynamically manage link aggregation.

Application Layer Integration

To validate Layer 7 connectivity, application services were deployed on their respective segmented hosts, including:

- **VLAN 10:** FastAPI Server, with the *Auth_Service* and *Notification Service* microservices.
- **VLAN 30:** Mail Server, using *aiosmtpd* and *SQLite* for mail management.
- **VLAN 20:** Streaming Server, based on VLC.
- **VLAN 40:** Gaming Server (*Counter-Strike Server*).

Connectivity and adherence to the firewall policies were verified through the functional testing of these services within the segmented environment. The complete configuration can be seen in Annex 1.

Results

The verification phase was executed with a rigorous methodology to ensure the comprehensive functionality of the network architecture, covering from Layer 1 up to Layer 7 of the OSI model.

Connectivity and VLSM Verification

Exhaustive ICMP (ping) connectivity tests were performed, which confirmed the success of both inter-VLAN communication and access to the external network (WAN). Path analysis (traceroute) from a client located in VLAN 10 to a server in VLAN 30 identified the Raspberry Pi's Gateway as the first Layer 3 hop, which validates the correct implementation of the Router-on-a-Stick model.

EtherChannel Stability

Verification commands confirmed that the Port-Channels configured using PAgP and LACP were correctly established and were operating efficiently in load-balancing mode. The simulation of a failure in one of the physical links aggregated in the channel did not cause any interruption in network connectivity, demonstrating the expected redundancy and resilience inherent in the EtherChannel implementation.

Functional Validation of the Application Layer

The most critical test was the validation of Layer 7 operability, which directly depended on the correct application of the firewall policies configured on the Raspberry Pi. The results of these tests are summarized below in Table 2.

Table 2

Operational Differences Between Unicast, Multicast, and Anycast

Required Communication Flow	Service Involved	Result	Validated Implication
VLAN 10 to VLAN 30	SMTP (TCP 25)	Successful	The Notification Service sent an email that was authorized by the *firewall* policy and correctly received by the *aiosmtpd* server.
VLAN 10 to VLAN 20	VLC Streaming	Successful	Clients were able to reproduce the video, validating correct inter-VLAN routing for multimedia traffic.
VLAN 10 to VLAN 40	Game/API	Successful	The client connected to the gaming session and the API reported results, proving the required bi-directional rule for game traffic.
All VLANs to WAN	TLS/External SMTP	Successful	Communication with external mail services (e.g., Gmail on port 587) was completed satisfactorily, validating the NAT service and the global outbound permission.

Note. The table details the Variable Length Subnet Mask (VLSM) addressing scheme applied to the 10.10.0.0/16 block. It shows the network segmentation with the subnet size optimized for the specific host requirements of each VLAN, and the assignment of the first host of each subnet as the gateway configured in the subinterfaces of the Raspberry Pi router.

Additionally, traffic analysis using Wireshark on the trunk ports confirmed the presence of the 802.1Q tags, verifying that the traffic reached the Raspberry Pi correctly tagged for logical routing.

Discussion

Evaluation of Raspberry Pi Performance

The performance of the Raspberry Pi as the Core Router in the multi-VLAN architecture proved to be functionally adequate and economically superior to traditional dedicated hardware solutions. However, this approach introduces critical considerations regarding performance and scalability. The Router-on-a-Stick operation centralizes the processing load on the eth0 interface, requiring the Pi's CPU to handle the decapsulation, routing decision, and re-encapsulation of every inter-VLAN packet, in addition to the inherent tasks of NAT and the Firewall (OpenWrt, 2024).

While the LuCi interface dramatically simplified the implementation of complex Netfilter rules and VLAN sub-interface configuration, it must be acknowledged that in a production environment with a significantly higher volume of burst traffic (e.g., multiple simultaneous multimedia streams or massive upload/download traffic), the throughput performance could be limited. Latency, while acceptable in gaming tests (VLAN 40), could become a bottleneck if deep packet inspection (DPI) is required or if the number of firewall rules increases considerably, negatively impacting time-sensitive services (OpenWrt, 2024).

Analysis of Layer 2 and Layer 3

The implementation of EtherChannel link aggregation was crucial for Layer 2 resilience. The ability to operate with mixed protocols, PAgP and LACP, in the same infrastructure not only proved interoperability but also ensured fault tolerance and rudimentary load balancing on critical switch-to-switch links.

However, the design suffers from a single point of failure at Layer 3: the Raspberry Pi itself and its single trunk interface. This risk is unacceptable in mission-critical environments.

Although the *Router-on-a-Stick* model optimizes port usage, a future architectural evolution would require migrating to an active/passive or active/active Gateway redundancy design, utilizing protocols such as VRRP (*Virtual Router Redundancy Protocol*) or HSRP (*Hot Standby Router Protocol*) (CISCO, 2024).

Regarding security, the principle of least privilege strategy applied in the Firewall was a success. Table 3 details the strict correspondence between the functional requirement and the security rule.

Table 3

Inter-VLAN Firewall Policy Verification Matrix

Source	Destination	Protocol/Port	Required Function	Rule Status (LuCi)
VLAN 10	VLAN 30	TCP 25 (SMTP)	Email Sending	Explicitly Allowed
VLAN 10	VLAN 40	UDP/TCP (Game)	Gaming and API Traffic	Bi-directionally Allowed
VLAN 10	VLAN 20	TCP/UDP (Range)	Streaming Playback	Explicitly Allowed
Remaining Inter-VLANs	All	ALL	User Traffic	Denied by Default

Note. The table demonstrates the direct mapping between the communication requirements of Layer 7 services and the security rules implemented in the Raspberry Pi Firewall, confirming the effective application of the principle of least privilege in inter-VLAN routing.

VLSM Addressing and IP Resource Management

The rigorous application of VLSM (Variable Length Subnet Masking) on the $10.10.0.0/16$ block proved to be responsible engineering practice. By sizing the subnets precisely to the host needs, high allocation efficiency was achieved, preserving valuable address ranges for future network growth. The success of the Layer 7 service validation, reflected in Table 4, confirms that the correct VLSM segmentation and sub-interface routing integrated perfectly with the application protocol needs.

Table 4

Verification of Application Service Operability

Verified Service	Source → Destination (VLAN)	Key Protocol	Functional Status
Authentication/Notification	VLAN 10 to VLAN 30	SMTP (TCP 25)	Functional
Game Connection	VLAN 10 to VLAN 40	UDP/TCP	Functional
Multimedia Streaming	VLAN 10 to VLAN 20	UDP/TCP	Functional
Access to Updates	All to WAN	HTTP/HTTPS	Functional

Note. This table summarizes the functional test results of the application services, confirming that inter-VLAN routing and Firewall rules allowed the transit of the specific protocols necessary for the operation of the segmented systems.

Conclusion

The present project has successfully validated the fundamental premise that a low-cost, embedded computing device, such as the Raspberry Pi, can be integrated with sufficient technical capability to assume the role of Core Router in a multi-VLAN campus network architecture. Compliance with the general objective has been rigorously proven, establishing a secure, segmented, and cost-efficient infrastructure. The implementation of the Router-on-a-Stick model was crucial for centralizing inter-VLAN routing and security policy management. Likewise, it was confirmed that the VLSM addressing plan provided the appropriate logical segmentation for each of the services, tangibly optimizing the utilization of the IP address space. The Layer 2 switching matrix demonstrated the necessary robustness, achieving the required resilience and bandwidth increase thanks to the verified and operational implementation of EtherChannel, with the successful coexistence of the PAgP and LACP protocols.

The functional validation of the Layer 7 services constituted the final proof of the design's precision. Critical applications, including controlled SMTP flow and low-latency gaming communications, operated uninterruptedly, which certifies that the Firewall policies configured through LuCi were granular enough to authorize necessary traffic flows while simultaneously maintaining security through the implicit denial of unauthorized traffic. Consequently, the project not only demonstrated the viability of alternative hardware in advanced networking but also established an implementation model that efficiently balances functionality, access control, and economics.

Future Perspectives

Despite the technical achievements demonstrated, a critical analysis of the architecture reveals essential avenues for its improvement and scalability to production environments. The most significant limitation identified resides in the single point of failure (SPOF) at Layer 3 inherent in the Router-on-a-Stick design, where the failure of the Raspberry Pi would result in the total interruption of inter-VLAN communication and WAN access. Therefore, future research must prioritize the implementation of gateway redundancy by integrating a second Raspberry Pi in an active/passive configuration, utilizing first-hop redundancy protocols (FHRP) such as VRRP or HSRP to ensure operational continuity. Additionally, a detailed exploration of the device's performance limits under maximum load is required. This would involve conducting exhaustive stress tests to determine the maximum sustainable *throughput* of the trunk interface under intensive NAT and Firewalling operations, and researching optimization techniques, such as offloading network functions to hardware or fine-tuning the Linux kernel, to ensure the platform can scale effectively without compromising latency or quality of service.

Annexes

Annex 1

Complete switch configuration

SW 0

```
en
conf t
hostname SW0
vlan 10
name Microservices
vlan 20
name Streaming
vlan 30
name MailServer
vlan 40
name Cs:Go
exit

interface range fastEthernet 0/1 -2
channel-group 1 mode desirable
exit
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40

interface range fastEthernet 0/7 -8
channel-group 4 mode desirable
exit
interface port-channel 4
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
ex

interface fastEthernet 0/10
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
ex

interface fastEthernet 0/9
switchport mode access
switchport access vlan 40
ex
```

SW 1

```
en
conf t
hostname SW1
vlan 10
name Microservices
vlan 20
name Streaming
vlan 30
name MailServer
vlan 40
name Cs:Go
exit

interface range fastEthernet 0/1 -2
channel-group 1 mode desirable
exit
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40

interface range fastEthernet 0/3 -4
channel-group 2 mode active
exit
interface port-channel 2
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
ex

interface fastEthernet 0/9
switchport mode access
switchport access vlan 30
ex
```

SW 2

```
en
conf t
hostname SW2
vlan 10
name Microservices
vlan 20
name Streaming
vlan 30
name MailServer
vlan 40
name Cs:Go
exit

interface range fastEthernet 0/3 -4
channel-group 2 mode passive
```

```
exit
interface port-channel 2
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40

interface range fastEthernet 0/5 -6
channel-group 3 mode on
exit
interface port-channel 3
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
ex

interface fastEthernet 0/9
switchport mode access
switchport access vlan 20
ex
SW 3
en
conf t
hostname SW3
vlan 10
name Microservices
vlan 20
name Streaming
vlan 30
name MailServer
vlan 40
name Cs:Go
exit

interface range fastEthernet 0/5 -6
channel-group 3 mode on
exit
interface port-channel 3
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40

interface range fastEthernet 0/7 -8
channel-group 4 mode desirable
exit
interface port-channel 4
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
ex

interface range fastEthernet 0/9 - 0/11
switchport mode access
switchport access vlan 10
ex
```

References

Academy, N. (2024). *Router on a stick (ROAS).* Retrieved from Network Academy : https://www.networkacademy.io/ccna/ethernet/router-on-a-stick

CCNA. (2023). *VLSM.* Retrieved from https://ccnadesdecero.es/vlsm-mascaras-subred-longitud-variable/#google_vignette

CISCO. (2024). *Hot Standby Router Protocol and Virtual Router.* Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_011110.pdf

CISCO. (2025). *EtherChannel.* Retrieved from https://www.cisco.com/c/es_mx/tech/lan-switching/etherchannel/index.html

De Luz, S. (2025, Agosto 16). *VLANs: Qué son, tipos y para qué sirven.* Retrieved from Rz redes zone: https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

George, S. (2025, April). *The Evolution of Data Center Networks: Strategies for Modern Infrastructure Design.* Retrieved from ReserchGate: https://www.researchgate.net/publication/391838417_The_Evolution_of_Data_Center_Networks_Strategies_for_Modern_Infrastructure_Design

OpenWrt. (2024). *Raspberry Pi.* Retrieved from https://openwrt.org/toh/raspberry_pi_foundation/raspberry_pi