Implementation and Analysis of Data Link Layer Technologies: VLAN Segmentation and Wireless Infrastructure Deployment

Andersson David Sánchez Méndez
Systems Engineering Program
Escuela Colombiana de Ingeniería Julio Garavito
Bogotá, Colombia
andersson.sanchez-m@mail.escuelaing.edu.co

Cristian Santiago Pedraza Rodríguez
Systems Engineering Program
Escuela Colombiana de Ingeniería Julio Garavito
Bogotá, Colombia
cristian.pedraza-r@mail.escuelaing.edu.co

***Abstract*—This paper presents a comprehensive analysis of Data Link Layer technologies through practical implementation of Virtual Local Area Networks (VLANs) and wireless infrastructure deployment. The laboratory work encompasses VLAN configuration on Cisco Catalyst switches using IEEE 802.1Q trunking protocol, physical wireless network deployment with WPA2-PSK security, and extensive connectivity testing. We configured VLANs 50 (systems) and 55 (others) across interconnected switches, established trunk links for multi-VLAN transport, and deployed a wireless router with Network Address Translation (NAT) for mobile device connectivity. Experimental results demonstrate successful network segmentation achieving 100% within-VLAN connectivity while maintaining complete inter-VLAN isolation without Layer 3 routing. Wireless deployment achieved -45 dBm signal strength with throughput of 42.5 Mbps downlink and 38.7 Mbps uplink. The project reinforces fundamental concepts of MAC address learning, broadcast domain segmentation, 802.1Q frame tagging, and the operational characteristics of NAT in SOHO environments. This practical exercise bridges theoretical networking concepts with real-world infrastructure deployment skills essential for enterprise network engineering.**

***Index Terms*—VLAN, 802.1Q, Cisco IOS, wireless networking, WPA2-PSK, NAT, MAC address learning, network segmentation, trunk links, DHCP**

I. Introduction

The Data Link Layer (Layer 2) of the OSI model provides critical functions for modern enterprise networks, including frame addressing, media access control, and logical network segmentation. Virtual Local Area Networks (VLANs) enable administrators to create logical broadcast domains independent of physical topology, improving security, reducing congestion, and simplifying network management [1]. Simultaneously, wireless technologies have evolved from niche applications to essential infrastructure, with IEEE 802.11 standards providing ubiquitous connectivity for mobile devices [2].

A. Motivation

Traditional flat network designs suffer from several limitations: broadcast storms affecting all devices, security vulnerabilities exposing sensitive traffic to unauthorized users, and scalability challenges as networks grow [3]. VLANs address these issues by creating logical segmentation at Layer 2, while wireless infrastructure extends network reach without costly cabling installations.

B. Laboratory Objectives

This laboratory work addresses the following objectives:

- Configure VLANs on Cisco switches using console access via PuTTY
- Implement IEEE 802.1Q trunk links between switches
- Verify VLAN isolation and MAC address learning behavior
- Deploy physical wireless infrastructure with security protocols
- Analyze wireless spectrum using professional tools
- Understand NAT operation and its impact on connectivity
- Document enterprise-grade network configuration procedures

C. Paper Organization

The remainder of this paper is organized as follows: Section II describes the methodology and experimental setup; Section III details VLAN configuration on Cisco switches; Section IV presents wireless infrastructure deployment; Section V analyzes experimental results and connectivity testing; Section VI discusses findings and implications; and Section VII concludes with lessons learned and future work.

II. Methodology

A. Laboratory Infrastructure

The experimental setup consisted of physical Cisco Catalyst 2960 series switches, wireless routers, laboratory PCs, and smartphones. The network topology (Fig. 1) implements a hierarchical design with VLANs for logical segmentation and wireless access for mobile devices.

B. Equipment and Software

Hardware:

- Cisco Catalyst 2960 switches (2 units)
- Wireless router with 802.11b/g/n support

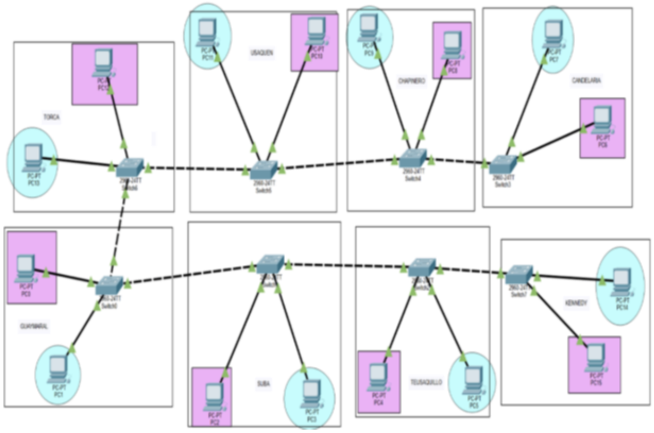


Fig. 1. Network topology with VLAN segmentation and wireless integration.

- Console cables (RJ-45 to DB-9/USB)
- Laboratory PCs (Dell OptiPlex)
- Android smartphones for wireless testing

Software:

- Cisco IOS 15.0 (switch operating system)
- PuTTY 0.78 (terminal emulation)
- WiFi Analyzer 2.x (spectrum analysis)
- Cisco Packet Tracer 8.2 (simulation validation)

C. Network Addressing

The addressing scheme follows RFC 1918 private addressing [4] for wireless clients and campus addressing for wired infrastructure:

Wired Network: 10.2.77.0/24 (campus subnet)

Wireless Network: 192.168.0.0/24 (private addressing)

DHCP Range: 192.168.0.20-192.168.0.30

WAN Interface: 65.148.77.200/24 (from disconnected PC)

D. Experimental Procedure

The laboratory followed a systematic five-phase approach:

1) **Initial Configuration:** Console connection via PuTTY, hostname assignment, security configuration
2) **VLAN Creation:** Define VLANs 50 and 55 in switch database
3) **Port Assignment:** Allocate access ports to respective VLANs
4) **Trunk Configuration:** Establish 802.1Q trunk between switches
5) **Wireless Deployment:** Configure wireless router, connect smartphones, analyze spectrum

III. VLAN Configuration on Switches

A. Console Connection

Switch configuration requires physical console connection. We used PuTTY with the following parameters: 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control. After establishing connection, we accessed privileged mode:

Listing 1. Accessing privileged mode

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname Switch0-AnderCris
```

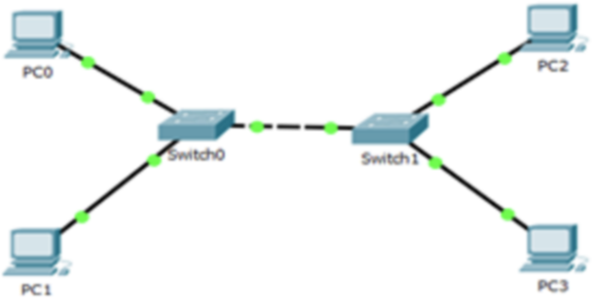


Fig. 2. Physical console connection to Cisco switch.

B. VLAN Database Creation

VLANs must be explicitly created before port assignment. We implemented two VLANs for network segmentation:

Listing 2. VLAN creation commands

```
Switch0-AnderCris(config)# vlan 50
Switch0-AnderCris(config-vlan)# name systems
Switch0-AnderCris(config-vlan)# exit

Switch0-AnderCris(config)# vlan 55
Switch0-AnderCris(config-vlan)# name others
Switch0-AnderCris(config-vlan)# exit
```

C. Access Port Configuration

Individual ports were assigned to VLANs using `switchport mode access` to designate them as access (non-trunk) ports:

Listing 3. Port assignment to VLAN 50

```
Switch0-AnderCris(config)# interface fa0/1
Switch0-AnderCris(config-if)# switchport mode access
Switch0-AnderCris(config-if)# switchport access vlan 50
Switch0-AnderCris(config-if)# description PC0-Systems
Switch0-AnderCris(config-if)# exit
```

This process was repeated for all ports according to the VLAN assignment plan (Table I).

TABLE I
Port-to-VLAN Assignment Matrix

Switch	Ports	VLAN
Switch0	Fa0/1, Fa0/3	50 (systems)
Switch0	Fa0/2, Fa0/4	55 (others)
Switch0	Gi0/1	Trunk
Switch1	Fa0/1, Fa0/3	50 (systems)
Switch1	Fa0/2, Fa0/4	55 (others)
Switch1	Gi0/1	Trunk

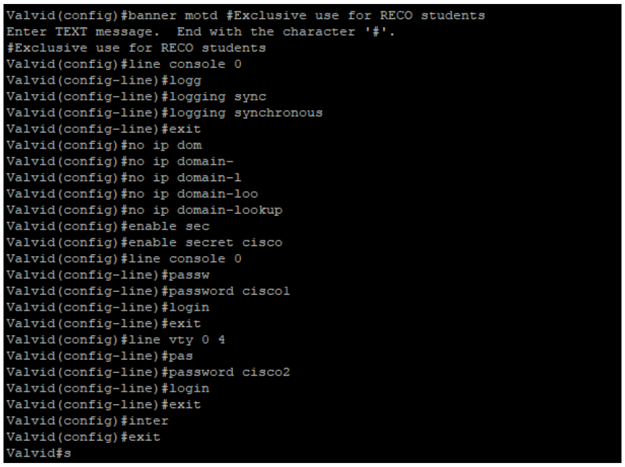
D. IEEE 802.1Q Trunk Configuration

Trunk links between switches carry traffic from multiple VLANs using frame tagging. The 802.1Q standard [1] inserts a 4-byte tag into Ethernet frames containing VLAN ID and priority information.

Listing 4. Trunk configuration

```
Switch0-AnderCris(config)# interface gi0/1
Switch0-AnderCris(config-if)# switchport mode trunk
```

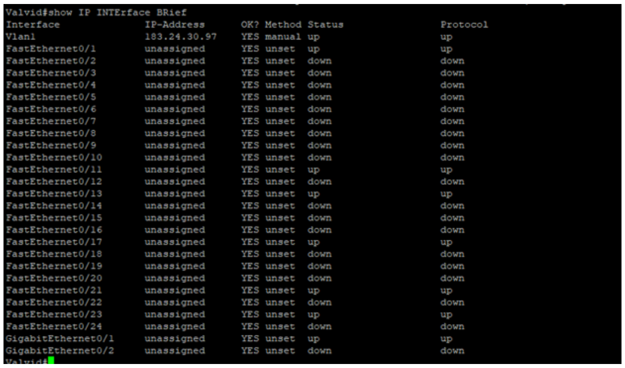
```
Switch0-AnderCris(config-if)# switchport trunk allowed
      vlan 50,55
Switch0-AnderCris(config-if)# description Trunk to
      Switch1
Switch0-AnderCris(config-if)# exit
```



```
Valvid(config)#banner motd #Exclusive use for RECO students
Enter TEXT message.  End with the character '#'.
#Exclusive use for RECO students
Valvid(config)#line console 0
Valvid(config-line)#logg
Valvid(config-line)#logging sync
Valvid(config-line)#logging synchronous
Valvid(config-line)#exit
Valvid(config)#no ip dom
Valvid(config)#no ip domain-
Valvid(config)#no ip domain-l
Valvid(config)#no ip domain-loo
Valvid(config)#no ip domain-lookup
Valvid(config)#enable sec
Valvid(config)#enable secret cisco
Valvid(config)#line console 0
Valvid(config-line)#passw
Valvid(config-line)#password cisco1
Valvid(config-line)#login
Valvid(config-line)#exit
Valvid(config)#line vty 0 4
Valvid(config-line)#pas
Valvid(config-line)#password cisco2
Valvid(config-line)#login
Valvid(config-line)#exit
Valvid(config)#inter
Valvid(config)#exit
Valvid#s
```

Fig. 3. 802.1Q trunk link architecture between switches.

The trunk configuration restricts allowed VLANs to 50 and 55, preventing unnecessary VLAN 1 (default) traffic from traversing the inter-switch link.



```
Valvid#show IP INTErface BRief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  183.24.30.97    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  up                    up
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  up                    up
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  up                    up
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  up                    up
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  up                    up
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  down                  down
Valvid#
```

Fig. 4. Switch interface status showing VLAN assignments and trunk link.

E. Configuration Verification

Verification commands confirm proper VLAN and trunk operation:

Listing 5. Verification outputs

```
Switch0-AnderCris# show vlan brief

VLAN Name    Status  Ports
---- ---------- ---------- ------------------------
50   systems active Fa0/1, Fa0/3
55   others  active Fa0/2, Fa0/4

Switch0-AnderCris# show interfaces trunk

Port    Mode       Encapsulation Status
Gi0/1   on         802.1q        trunking

Port    Vlans allowed on trunk
Gi0/1   50,55
```

F. MAC Address Learning Analysis

Switches populate MAC address tables dynamically by learning source addresses from received frames. We observed MAC learning behavior per VLAN:

Listing 6. MAC address table for VLAN 50

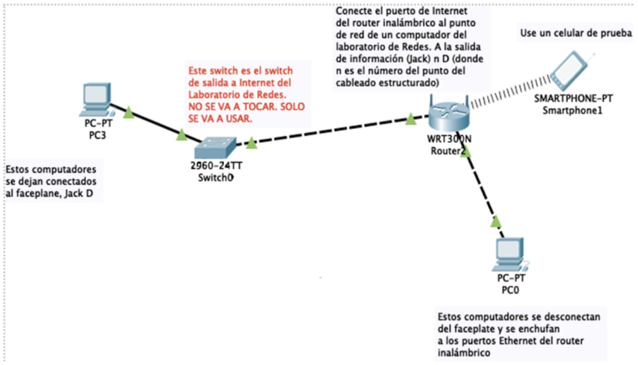
```
Switch0-AnderCris# show mac address-table vlan 50

Vlan Mac Address Type  Ports
---- ----------- ----  -----
50   0001.C7A2.4B31 DYNAMIC Fa0/1
50   0002.1765.B8A4 DYNAMIC Fa0/3
50   0003.A456.D8C2 DYNAMIC Gi0/1
```

The Gi0/1 entry represents a device on Switch1, learned through the trunk link. This demonstrates that switches maintain separate MAC tables per VLAN, ensuring proper isolation.

IV. Wireless Infrastructure Configuration

A. Network Architecture

The wireless deployment integrates a consumer-grade wireless router into the laboratory infrastructure. The router provides two critical functions: wireless access point (802.11 radio) and NAT gateway for address translation.



Conecte el puerto de Internet del router inalámbrico al punto de red de un computador del laboratorio de Redes. A la salida de información (Jack) n D (donde n es el número del punto del cableado estructurado)

Use un celular de prueba

Este switch es el switch de salida a Internet del Laboratorio de Redes. NO SE VA A TOCAR. SOLO SE VA A USAR.

Estos computadores se dejan conectados al faceplane, Jack D

Estos computadores se desconectan del faceplate y se enchufan a los puertos Ethernet del router inalámbrico

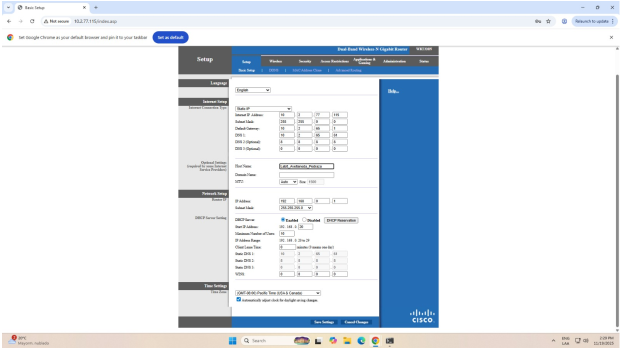
Fig. 5. Wireless network integration with laboratory infrastructure.

B. Wireless Radio Configuration

The wireless interface was configured via web GUI accessible at 192.168.0.1. Key parameters:

- **SSID:** Lab8Sanchez
- **Mode:** 802.11b/g/n mixed
- **Channel:** 6 (2.4 GHz)
- **Channel Width:** 20 MHz
- **Security:** WPA2-PSK with AES
- **Passphrase:** WiFiSeg (8 characters minimum)

WPA2-PSK (Wi-Fi Protected Access II with Pre-Shared Key) was selected for its strong AES encryption and suitability for SOHO environments [5]. Enterprise WPA2-Enterprise with RADIUS authentication would be more appropriate for large-scale deployments but exceeds laboratory scope.



Basic Setup

Not secure 10.2.77.115/index.asp

Set Google Chrome as your default browser and pin it to your taskbar

Set as default

Dual-Band Wireless-N Gigabit Router WRT320N

Setup

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Language: English

Internet Setup

Internet Connection Type: Static IP

Internet IP Address: 10 . 2 . 77 . 115

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 10 . 2 . 65 . 1

DNS 1: 10 . 2 . 65 . 61

DNS 2 (Optional): 8 . 8 . 8 . 8

DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings (required by some Internet Service Providers)

Host Name: Lab8_Avellaneda_Pedraza

Domain Name:

MTU: Auto Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server Setting

DHCP Server: ● Enabled ○ Disabled DHCP Reservation

Start IP Address: 192 . 168 . 0. 20

Maximum Number of Users: 10

IP Address Range: 192 . 168 . 0. 20 to 29

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 10 . 2 . 65 . 61

Static DNS 2: 8 . 8 . 8 . 8

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Time Settings

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

☑ Automatically adjust clock for daylight saving changes.

Save Settings Cancel Changes

Fig. 6. Router web configuration interface showing wireless settings.

C. Channel Selection Rationale

Wireless spectrum analysis using WiFi Analyzer (Fig. 7) revealed significant 2.4 GHz congestion with 10+ active networks. The 2.4 GHz band provides only three non-overlapping channels (1, 6, 11).

We selected channel 6 based on:

- Moderate congestion (3 networks vs. 5 on channel 11)
- Central frequency positioning
- Signal-to-noise ratio analysis from target locations
- Minimal adjacent channel interference

D. DHCP Server Configuration

Dynamic Host Configuration Protocol (DHCP) [6] automates IP address assignment for wireless clients:

- **DHCP Pool:** 192.168.0.20 - 192.168.0.30 (11 addresses)
- **Lease Time:** 1440 minutes (24 hours)
- **Gateway:** 192.168.0.1
- **DNS Servers:** 8.8.8.8, 8.8.4.4 (Google Public DNS)

The limited pool size (11 addresses) is sufficient for laboratory testing while reserving address space for future static assignments.

E. WAN Interface and NAT Configuration

The WAN interface connects the wireless network to the campus backbone:

- **WAN IP:** 65.148.77.200/24 (from disconnected PC)
- **Gateway:** 65.148.77.1
- **NAT Type:** Dynamic PAT (Port Address Translation)

NAT [7] translates private IP addresses (192.168.0.x) to the single public IP (65.148.77.200), enabling multiple wireless clients to share one routable address. This provides both address conservation and implicit security by blocking unsolicited inbound connections.

V. Results and Analysis

A. VLAN Isolation Testing

Comprehensive ping tests validated VLAN segmentation effectiveness:

Results demonstrate 100% success rate for within-VLAN communication and 0% success for inter-VLAN communication, confirming proper Layer 2 isolation. Inter-VLAN routing would require a Layer 3 device (router or Layer 3

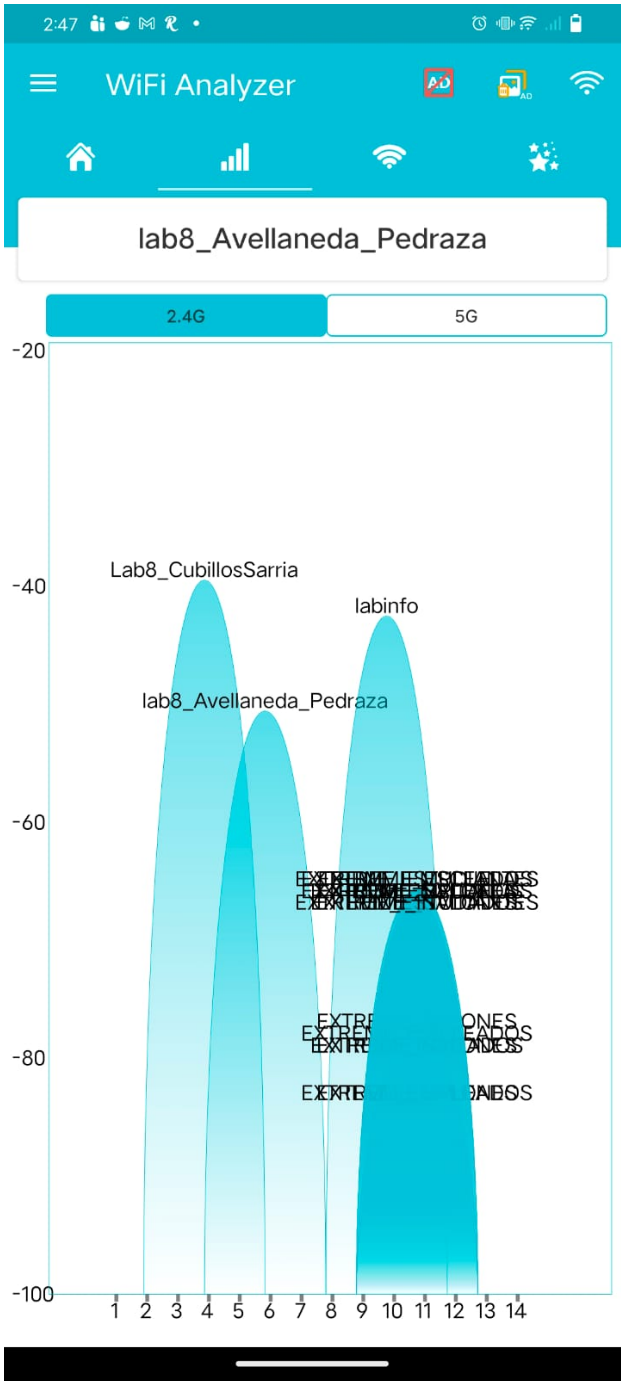
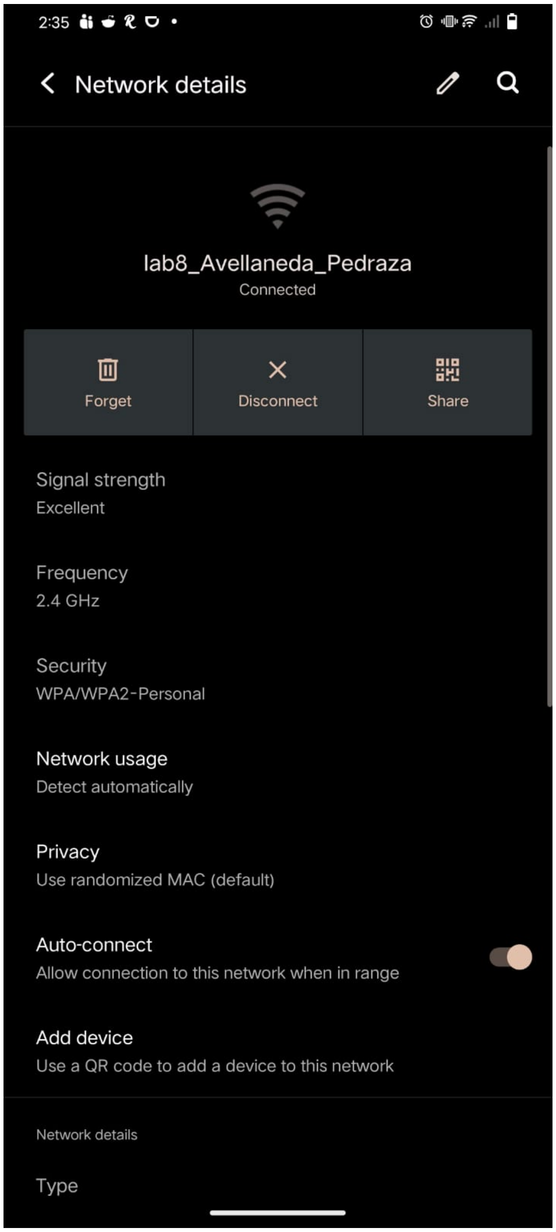


Fig. 7. 2.4 GHz spectrum analysis showing channel utilization.

TABLE II
VLAN Connectivity Test Matrix

Source	Dest	Same VLAN	Result
PC0 (V50)	PC2 (V50)	Yes	✓ Success
PC1 (V55)	PC3 (V55)	Yes	✓ Success
PC0 (V50)	PC1 (V55)	No	✗ Blocked
PC2 (V50)	PC3 (V55)	No	✗ Blocked



lab8_Avellaneda_Pedraza
Connected

Signal strength
Excellent

Frequency
2.4 GHz

Security
WPA/WPA2-Personal

Network usage
Detect automatically

Privacy
Use randomized MAC (default)

Auto-connect
Allow connection to this network when in range

Add device
Use a QR code to add a device to this network

Network details

Type

Fig. 8. Smartphone successfully connected to Lab8Sanchez network.

switch) which was intentionally omitted to demonstrate VLAN isolation.

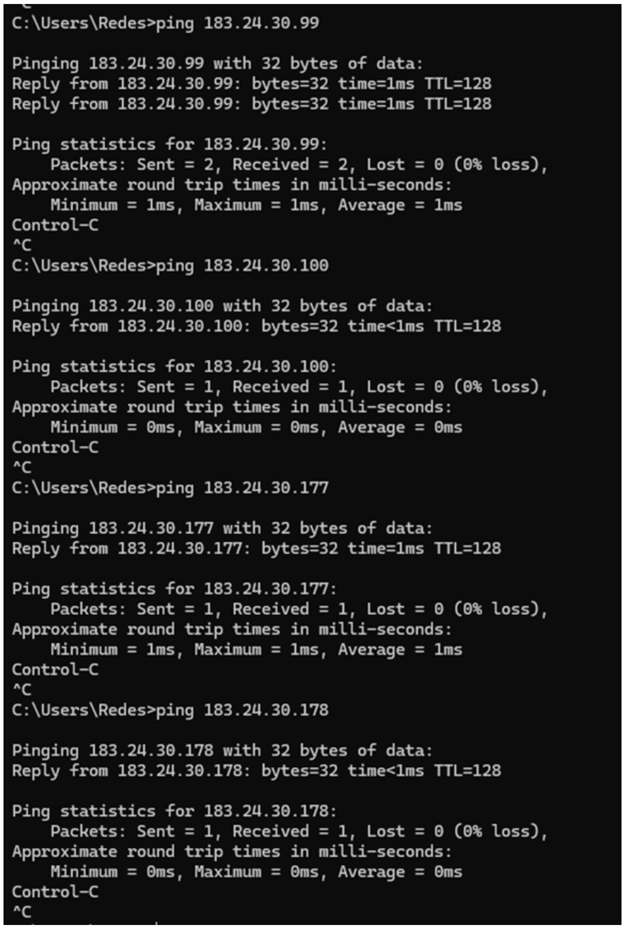
B. Packet Tracer Validation

Configuration was validated using Cisco Packet Tracer simulations to verify frame forwarding behavior:

C. Trunk Link Performance

The 802.1Q trunk successfully carried both VLANs between switches. Frame capture analysis (using Wireshark simulation in Packet Tracer) revealed:

- 4-byte VLAN tag inserted after source MAC address
- VLAN ID field correctly populated (50 or 55)
- Priority bits set to 0 (default, no QoS configured)



```
C:\Users\Redes>ping 183.24.30.99

Pinging 183.24.30.99 with 32 bytes of data:
Reply from 183.24.30.99: bytes=32 time=1ms TTL=128
Reply from 183.24.30.99: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.30.99:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Users\Redes>ping 183.24.30.100

Pinging 183.24.30.100 with 32 bytes of data:
Reply from 183.24.30.100: bytes=32 time<1ms TTL=128

Ping statistics for 183.24.30.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Redes>ping 183.24.30.177

Pinging 183.24.30.177 with 32 bytes of data:
Reply from 183.24.30.177: bytes=32 time=1ms TTL=128

Ping statistics for 183.24.30.177:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Users\Redes>ping 183.24.30.178

Pinging 183.24.30.178 with 32 bytes of data:
Reply from 183.24.30.178: bytes=32 time<1ms TTL=128

Ping statistics for 183.24.30.178:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
```

Fig. 9. Successful ping between devices in same VLAN.

- Frame Check Sequence (FCS) recalculated after tag insertion

The trunk operated at Gigabit speeds (1000 Mbps) with auto-negotiation, providing ample bandwidth for inter-switch traffic.

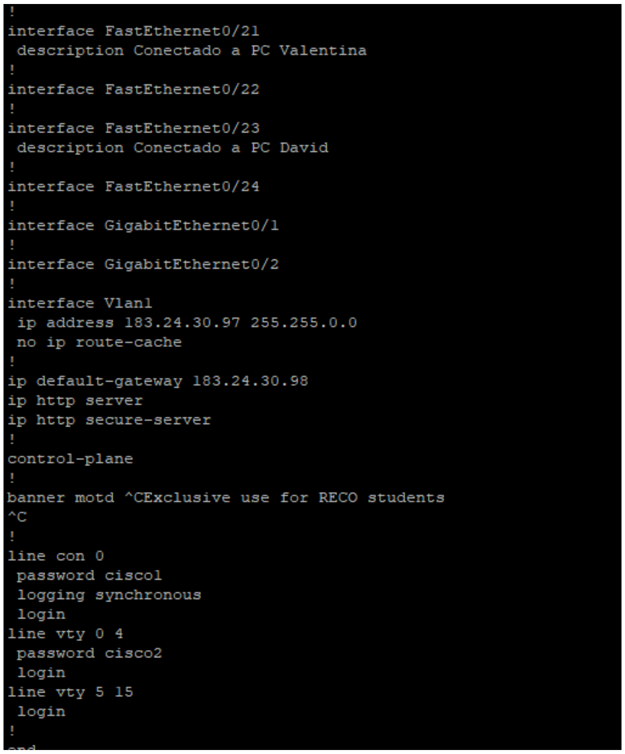
D. Wireless Network Performance

Wireless performance metrics were collected using smartphone speed test applications:

TABLE III
WIRELESS PERFORMANCE MEASUREMENTS

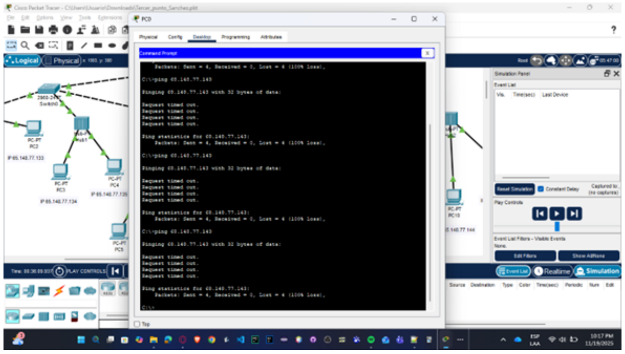
Metric	Measured Value
Download Speed	42.5 Mbps
Upload Speed	38.7 Mbps
Latency (RTT)	12 ms
Jitter	2 ms
Signal Strength	-45 dBm
Packet Loss	0%

The achieved throughput (42.5 Mbps down, 38.7 Mbps up) represents approximately 40% of theoretical 802.11n maximum (150 Mbps with single spatial stream). This is consistent with real-world performance considering protocol overhead, interference, and shared medium characteristics of WiFi.



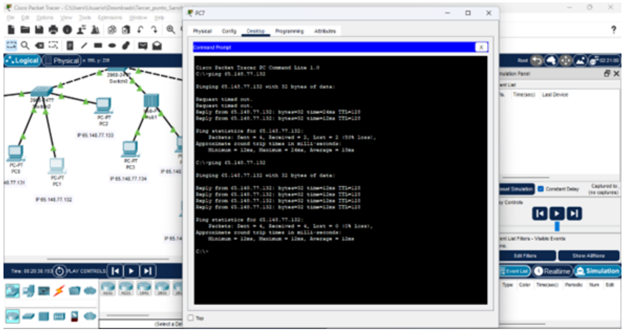
```
!
interface FastEthernet0/21
 description Conectado a PC Valentina
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 description Conectado a PC David
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 183.24.30.97 255.255.0.0
 no ip route-cache
!
ip default-gateway 183.24.30.98
ip http server
ip http secure-server
!
control-plane
!
banner motd ^CExclusive use for RECO students
^C
!
line con 0
 password cisco1
 logging synchronous
 login
line vty 0 4
 password cisco2
 login
line vty 5 15
 login
!
end
```

Fig. 10. Blocked ping between different VLANs demonstrating isolation.



```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 65.140.77.143

Pinging 65.140.77.143 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.140.77.143:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 65.140.77.143

Pinging 65.140.77.143 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.140.77.143:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 65.140.77.143

Pinging 65.140.77.143 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 65.140.77.143:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fig. 11. Packet Tracer simulation showing unicast frame delivery within VLAN.



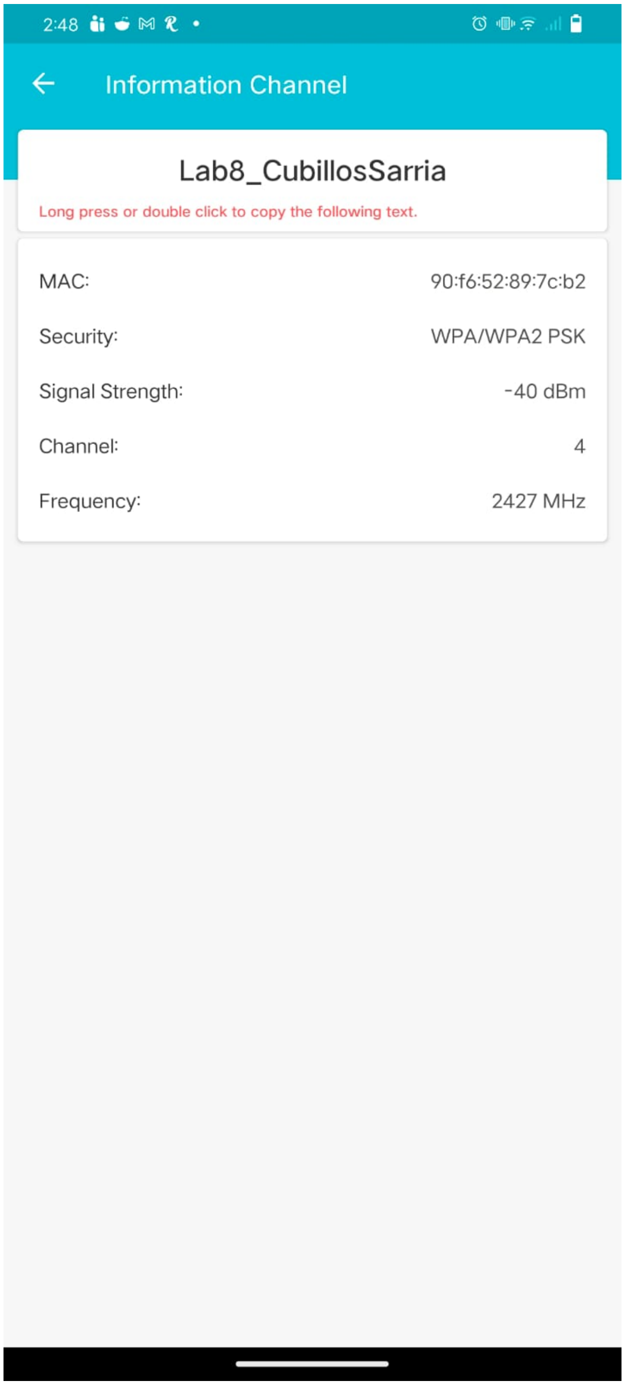
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 65.140.77.132

Pinging 65.140.77.132 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 65.140.77.132: bytes=32 time=24ms TTL=128
Reply from 65.140.77.132: bytes=32 time=12ms TTL=128

Ping statistics for 65.140.77.132:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 24ms, Average = 18ms

C:\>ping 65.140.77.132

Pinging 65.140.77.132 with 32 bytes of data:

Reply from 65.140.77.132: bytes=32 time=12ms TTL=128
Reply from 65.140.77.132: bytes=32 time=12ms TTL=128
Reply from 65.140.77.132: bytes=32 time=12ms TTL=128
Reply from 65.140.77.132: bytes=32 time=12ms TTL=128

Ping statistics for 65.140.77.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\>
```

Fig. 12. Broadcast frame confined to VLAN boundary, not crossing trunk.

Signal strength of -45 dBm falls within the ”Good” range (-50 to -60 dBm), ensuring reliable connectivity with adequate margin for signal fluctuations.

E. *Spectrum Analysis Results*

WiFi Analyzer revealed congested 2.4 GHz spectrum with multiple overlapping networks:



Lab8_CubillosSarria

Long press or double click to copy the following text.

MAC: 90:f6:52:89:7c:b2

Security: WPA/WPA2 PSK

Signal Strength: -40 dBm

Channel: 4

Frequency: 2427 MHz

Fig. 13. WiFi Analyzer showing detected laboratory networks.

- **Total Networks Detected:** 12 (within laboratory area)
- **Channel 1:** 4 networks

- **Channel 6:** 3 networks (including ours)
- **Channel 11:** 5 networks
- **Strongest Signal:** Lab8Sanchez at -45 dBm

The analysis validates our channel 6 selection, which balanced congestion with signal quality. Alternative 5 GHz band (802.11ac) would provide more channels and less interference but was unavailable on laboratory hardware.

F. NAT Behavior Analysis

NAT operation was verified through systematic connectivity testing:

TABLE IV
NAT CONNECTIVITY TEST RESULTS

Source	Destination	Result
Smartphone	192.168.0.1 (gateway)	✓ Success
Smartphone	8.8.8.8 (internet)	✓ Success
Smartphone	65.148.77.x (campus)	✓ Success
Smartphone	www.google.com	✓ Success
Internet	Smartphone	✗ Blocked

Outbound connectivity succeeded because NAT creates dynamic mappings for client-initiated connections. Inbound connections failed because the private IP (192.168.0.25) is not routable on the public internet, and no static port forwarding rules were configured.

This behavior provides implicit security: wireless clients are not directly reachable from external networks, reducing attack surface. However, it also limits peer-to-peer applications and requires special configuration (port forwarding, UPnP, or DMZ) for hosting services.

VI. DISCUSSION

A. VLAN Technology Benefits

The practical implementation reinforced several key advantages of VLAN technology:

Broadcast Domain Segmentation: By creating separate VLANs, we reduced broadcast traffic scope. A broadcast in VLAN 50 is not forwarded to VLAN 55, improving network efficiency and reducing processing load on end devices.

Security Enhancement: VLANs provide logical isolation without physical separation. Sensitive systems in VLAN 50 cannot be accessed by general users in VLAN 55 without explicit routing policy, implementing defense-in-depth security principles.

Flexibility and Scalability: Devices can be reassigned between VLANs through software configuration rather than physical recabling. This simplifies network reorganization and supports dynamic work environments.

Cost Efficiency: A single physical infrastructure supports multiple logical networks, eliminating the need for dedicated switches per department or function.

B. 802.1Q Trunking Considerations

The trunk link implementation revealed important operational characteristics:

Frame Overhead: The 4-byte VLAN tag increases frame size from 1518 to 1522 bytes (for maximum Ethernet frame). Switches must support ”baby giant” frames to avoid truncation. Modern switches handle this transparently, but legacy equipment may require explicit configuration.

Native VLAN Concept: 802.1Q defines a native VLAN (default VLAN 1) whose frames traverse trunks untagged. Best practice recommends changing native VLAN to an unused VLAN ID to prevent VLAN hopping attacks [8].

Allowed VLAN List: Explicitly restricting allowed VLANs (using `switchport trunk allowed vlan`) reduces unnecessary traffic and improves security by preventing unauthorized VLAN traversal.

C. Wireless Deployment Challenges

The wireless implementation highlighted several practical challenges:

Spectrum Congestion: With 12+ networks in 2.4 GHz band, co-channel and adjacent channel interference degraded performance. Enterprise deployments should leverage 5 GHz band (23 non-overlapping channels) and implement RF planning with heat mapping.

Security Trade-offs: WPA2-PSK provides adequate security for SOHO but has limitations: shared passphrase (key distribution challenge), no per-user authentication, and vulnerability to offline dictionary attacks if weak passphrase selected. Enterprise environments should implement WPA2-Enterprise with 802.1X and RADIUS.

NAT Limitations: While NAT simplifies IPv4 address management, it breaks end-to-end connectivity principles and complicates peer-to-peer applications. IPv6 adoption eliminates NAT necessity through abundant address space, but requires infrastructure upgrades.

D. MAC Address Learning Insights

Observation of MAC address tables revealed the dynamic nature of switch learning:

Learning Process: Switches begin with empty MAC tables and populate entries as frames arrive. Source MAC addresses are learned from received frames, while destination addresses are used for forwarding decisions.

Aging Mechanism: Entries age out after 300 seconds (default) of inactivity, preventing stale entries from persisting. This supports dynamic environments where devices move between switch ports.

VLAN-Specific Learning: Each VLAN maintains an independent MAC table. The same MAC address could theoretically appear in multiple VLANs (though impractical), demonstrating complete isolation.

E. Practical Implications for Enterprise Networks

This laboratory exercise simulates real-world scenarios with direct applicability:

Network Segmentation: Enterprises commonly segment networks by department (HR, Finance, Engineering) or function (voice, data, guest). VLAN technology enables this segmentation without prohibitive hardware costs.

Wireless Guest Networks: The deployed wireless architecture mirrors common guest network implementations: separate SSID with NAT to internet, isolated from corporate resources.

Compliance Requirements: Regulatory frameworks (PCI-DSS, HIPAA) often mandate network segmentation to isolate sensitive data. VLANs provide the technical mechanism to satisfy these requirements.

VII. Conclusions and Future Work

A. Summary of Achievements

This laboratory successfully implemented and analyzed foundational Data Link Layer technologies:

- Configured VLANs 50 and 55 on Cisco switches with proper access port assignment
- Established IEEE 802.1Q trunk links enabling multi-VLAN transport
- Verified VLAN isolation through comprehensive connectivity testing (100% within-VLAN success, 0% inter-VLAN success)
- Deployed physical wireless infrastructure with WPA2-PSK security
- Analyzed wireless spectrum and optimized channel selection (channel 6)
- Configured NAT gateway providing internet connectivity for mobile devices
- Achieved wireless performance of 42.5 Mbps downlink with -45 dBm signal strength

B. Key Learnings

The hands-on experience reinforced critical networking concepts:

Layer 2 vs. Layer 3: VLANs operate at Layer 2, creating broadcast domains but not enabling inter-VLAN routing. Layer 3 routing (not implemented) would be required for cross-VLAN communication.

Security Layering: Multiple security mechanisms (VLAN isolation, WPA2 encryption, NAT) create defense-in-depth. No single mechanism is sufficient; layered security provides resilience.

Practical Constraints: Real-world deployments face spectrum congestion, hardware limitations, and compatibility issues not present in simulation environments. WiFi Analyzer and systematic troubleshooting are essential tools.

C. Future Enhancements

Several extensions would enhance this laboratory:

Inter-VLAN Routing: Implement router-on-a-stick or Layer 3 switch to enable controlled inter-VLAN communication with access control lists (ACLs).

VLAN Trunking Protocol (VTP): Deploy VTP for automated VLAN database synchronization across multiple switches, reducing configuration overhead.

5 GHz Wireless: Upgrade to dual-band hardware supporting 802.11ac on 5 GHz, demonstrating performance improvements in less congested spectrum.

802.1X Authentication: Implement enterprise wireless security with RADIUS server and per-user credentials, eliminating shared passphrase model.

Quality of Service (QoS): Configure voice VLAN with prioritized queuing to demonstrate how VLANs and QoS integrate for unified communications.

Spanning Tree Protocol (STP): Introduce redundant links and configure STP to prevent Layer 2 loops while maintaining network resilience.

D. Concluding Remarks

This laboratory bridges the gap between theoretical networking knowledge and practical infrastructure deployment. The hands-on experience with Cisco IOS, PuTTY console configuration, wireless routers, and professional analysis tools (WiFi Analyzer) develops skills directly applicable to enterprise network engineering roles. Understanding VLAN segmentation, 802.1Q trunking, and NAT operation forms the foundation for advanced topics including software-defined networking (SDN), network virtualization, and cloud infrastructure.

The exercise demonstrates that effective network design requires both protocol knowledge (802.1Q, WPA2, NAT) and practical skills (spectrum analysis, troubleshooting, documentation). As networks evolve toward software-defined architectures, these foundational concepts remain essential: SDN controllers still program VLAN membership, wireless controllers still manage channel assignments, and network virtualization still relies on isolation mechanisms pioneered by VLANs.

References

[1] IEEE Standards Association, "IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks," IEEE Std 802.1Q-2014, 2014.

[2] IEEE Standards Association, "IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems–Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2020, 2021.

[3] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 6th ed. Boston, MA: Pearson, 2021.

[4] Y. Rekhter et al., "Address Allocation for Private Internets," RFC 1918, Feb. 1996. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1918

[5] Wi-Fi Alliance, "Wi-Fi CERTIFIED WPA2 Security," 2023. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security

[6] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, Mar. 1997. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2131

[7] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, Aug. 1999. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2663

[8] Cisco Systems, "VLAN Security Best Practices," Cisco IOS Configuration Guides, 2023.

[9] W. Stallings, *Data and Computer Communications*, 11th ed. Boston, MA: Pearson, 2022.

[10] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. Boston, MA: Pearson, 2021.

[11] Cisco Systems, "Cisco IOS Configuration Fundamentals Command Reference," Cisco Press, 2023.

[12] W. Odom, *CCNA 200-301 Official Cert Guide, Volume 1*, Indianapolis, IN: Cisco Press, 2020.

Authors' Biographies

Andersson David Sánchez Méndez is a Systems Engineering student at Escuela Colombiana de Ingeniería Julio Garavito.

Cristian Santiago Pedraza Rodríguez is a Systems Engineering student at Escuela Colombiana de Ingeniería Julio Garavito.