2025

VLANs: From Theory to Packet-Level Analysis with GNS3 and Wireshark

From Theory to Packet-Level Reality Perfect for Real-World Engineers

Subash Subedi

Abstract

This hands-on guide provides a complete understanding of IEEE 802.1Q VLANs using a practical GNS3 topology with one Cisco Layer 2 switch and seven PCs. The document explains VLAN theory, switch configuration, tagging and untagging behavior, and packet-level verification using Wireshark.

A Local SPAN (Switched Port Analyzer) session is used to mirror VLAN traffic to a dedicated monitoring port. This allows accurate observation of 802.1Q header behavior on access ports, trunk ports, and native VLAN traffic.

By completing this lab, learners gain both theoretical and practical understanding required for CCNA and real-world network troubleshooting.

Table of Contents

1. Introduction 4

1.1. What is a VLAN? 4

1.2. Why VLANs Are Important 4

1.3. Benefits of VLANs in Modern Networks 5

2. VLAN Core Concepts 5

2.1. Broadcast Domains & Network Segmentation 5

2.2. Tagged vs Untagged Traffic 6

2.3. IEEE 802.1Q Standard Overview 6

2.4. The Native VLAN Concept 6

2.5. VLAN IDs and Ranges 7

3. VLAN Types 7

3.1. Static VLANs (Port-Based) 7

3.2. Dynamic VLANs 7

3.3. Voice VLAN (Auto & Manual) 7

3.4. Management VLAN & SVI 8

3.5. Default VLAN (VLAN 1) 8

3.6. Private VLANs 8

4. Switch Port Modes 9

4.1. Access Port 9

4.2. Trunk Port (ISLCisco & IEEE 802.1Q) 9

4.3. Dynamic Auto / Dynamic Desirable (DTP Modes Table) 9

4.4. How Switches Decide: Tagging vs Untagging Rules (Decision Matrix) 10

5. Hands-On Lab: VLAN Implementation in GNS3 11

5.1. Lab Objectives 11

5.2. Lab Topology Overview 11

5.3. Devices and Software Used 11

5.4. VLAN & IP Allocation Table 11

5.5. Step-by-Step Switch Configuration 12

5.5.1. Creating VLANs 12

5.5.2. Configuring Access Ports 13

6. SPAN (Switched Port Analyzer) Configuration 17

6.1. Why Use SPAN in VLAN Labs 17

6.2. Updated Topology with Monitoring Port 17

6.3. Complete SPAN Configuration 17

6.4. Verifying SPAN Session 18

6.5. What You Should See in Wireshark 18

6.6. Tag Behavior Summary Table 18

7. Traffic Capture & VLAN Tag Analysis 19

7.1. Access-Port Traffic --> Untagged 19

7.2. Trunk Traffic --> Tagged (VLAN 10) 19

7.3. 802.1Q Header Breakdown in Wireshark 19

7.4. Native VLAN Traffic --> Untagged on Trunk 19

7.5. Sample Packet Capture 20

8. Key Observations & Learning Outcomes 20

9. Best Practices & Security Recommendations 20

10. Troubleshooting VLAN Issues 20

10.1. Top 5 VLAN Problems on the Exam 20

10.2. Native VLAN Mismatch Symptoms 21

10.3. Must-Know Commands + Expected Output 21

11. Conclusion 21

1. Introduction

1.1. What is a VLAN?

A Virtual LAN (VLAN) is a logical grouping of devices within a switched network that allows them to communicate as if they were on the same physical segment, even if they are connected to different switches or located on different floors.

VLANs rely on logical connections rather than physical ones. Devices in the same VLAN share a broadcast domain, meaning that unicast, broadcast, and multicast traffic are restricted to that VLAN. Devices in different VLANs cannot communicate directly at Layer 2; communication between VLANs requires a Layer 3 device, such as a router.

Example: In a three-floor office, IT, HR, and Sales departments may each have their own VLAN (VLAN 2, 3, and 4). These VLANs span all floors, allowing devices to communicate logically while remaining physically connected to different switches.

1.2. Why VLANs Are Important

VLANs are essential because they:

Segment networks logically by function, department, or application, regardless of physical location.

Reduce broadcast domains, preventing unnecessary traffic from reaching all devices and improving performance.

Contain broadcast traffic within each VLAN, improving **efficiency and scalability**.

Enhance security and access control by isolating sensitive users or departments (e.g., HR, IT) from general users (e.g., Guests, Students).

Enable flexible network design, allowing devices to be moved or added without rewiring or creating new physical networks.

1.3. Benefits of VLANs in Modern Networks

The main advantages of VLAN implementation include:

Improved Performance

Smaller broadcast domains reduce unnecessary traffic and increase network efficiency.

Enhanced Security

Logical isolation prevents unauthorized access between VLANs, protecting sensitive departments.

Better Organization and Flexibility

Devices can be grouped by role or function rather than physical location, simplifying moves and expansions.

Simplified Network Management

Supports hierarchical IP addressing, making administration and troubleshooting easier.

Cost Efficiency

Reduces the need for multiple physical networks and equipment while maintaining logical separation.

Policy Enforcement

Access control and traffic rules can be applied per VLAN, such as restricting Guest VLANs to internet-only access.

2. VLAN Core Concepts

2.1. Broadcast Domains & Network Segmentation

A broadcast domain is a set of devices that receive a Layer 2 broadcast frame.

Without VLANs: the entire switched network is one broadcast domain - any broadcast is sent to all devices, causing unnecessary traffic.

With VLANs: each VLAN forms a separate broadcast domain. Broadcasts are limited to devices in the same VLAN, even across different switches.

Result: smaller broadcast domains → improved network performance, scalability, and security.

2.2. Tagged vs Untagged Traffic

Untagged traffic: Standard Ethernet frames without VLAN information (from PCs or standard devices).

Tagged traffic: Frames with a 4-byte 802.1Q tag inserted between Source MAC and Type/Length fields, carrying the VLAN ID (VID).

Access ports: Send/receive untagged frames (single VLAN).

Trunk ports: Carry tagged frames for multiple VLANs.

Exception: Traffic in the native VLAN is sent untagged, even on trunks.

2.3. IEEE 802.1Q Standard Overview

IEEE 802.1Q is the industry-standard protocol for VLAN tagging on Ethernet networks.

It inserts a 4-byte tag into the original Ethernet frame header containing:

TPID (Tag Protocol Identifier): 2 bytes, value 0x8100

Priority (PRI): 3 bits for Class of Service (QoS)

CFI: 1 bit (legacy Token Ring support)

VID (VLAN ID): 12 bits, supporting up to 4096 VLANs (0–4095)

After tagging, the switch recalculates and updates the Frame Check Sequence (FCS). 802.1Q enables trunk links to transport traffic from multiple VLANs between switches and other devices.s.

2.4. The Native VLAN Concept

Each 802.1Q trunk has a native VLAN (default = VLAN 1).

Untagged frames received on a trunk are assigned to the native VLAN.

Frames for the native VLAN are sent untagged across the trunk.

Important points:

Cisco switches drop incoming tagged frames that match the native VLAN ID.

Control protocols (CDP, STP, VTP, DTP) typically use the native VLAN and are sent untagged.

Security best practice: Change the native VLAN to an unused VLAN (e.g., 999) and do not carry user traffic on it.

Native VLAN must match on both ends of the trunk; mismatch causes errors and warnings.

2.5. VLAN IDs and Ranges

Normal VLANs: 1–1005 (stored in vlan.dat, supported on all Cisco switches)

Extended VLANs: 1006–4094 (supported on modern switches in VTP transparent mode)

Reserved IDs: 0 and 4095 cannot be used

Total VLANs possible with 802.1Q: 4096 (12-bit VID field)

3. VLAN Types

3.1. Static VLANs (Port-Based)

The most common and recommended method.

Ports are manually assigned to a specific VLAN using switchport access vlan X command.

Reliable, secure, and easy to understand - this is the primary method tested in CCNA.

3.2. Dynamic VLANs

VLAN assignment is based on the device’s MAC address using a VLAN Membership Policy Server (VMPS).

Rarely used today and officially deprecated by Cisco - no longer part of CCNA but may appear in CCNP ENCOR.

3.3. Voice VLAN (Auto & Manual)

Allows a single switch port to support both a PC (data) and an IP phone (voice).

The port is configured with one data VLAN and one voice VLAN.

Cisco IP phones use CDP or LLDP to learn the voice VLAN and tag voice traffic accordingly.

Configuration example:

```
switchport mode access
switchport access vlan 20
switchport voice vlan 150
```

3.4. Management VLAN & SVI

A dedicated VLAN used for switch management (SSH, Telnet, SNMP, etc.).

Should not be VLAN 1 for security reasons.

A Switch Virtual Interface (SVI) is created using:

```
interface vlan 99
ip address 192.168.99.10 255.255.255.0
```

This provides Layer 3 access to the switch.

3.5. Default VLAN (VLAN 1)

All switch ports belong to VLAN 1 by default.

VLAN 1 cannot be deleted or renamed.

Carries all control plane traffic (CDP, STP, VTP, DTP, etc.).

Best security practice:

Do not use VLAN 1 for user or management traffic

Change the native VLAN on trunks

Create separate management and user VLANs

3.6. Private VLANs

Advanced feature for further Layer 2 isolation within a single VLAN.

Used in service provider or multi-tenant environments.

Types of ports:

Isolated: Can only communicate with promiscuous ports

Community: Can communicate with other members of the same community and promiscuous ports

Promiscuous: Typically connected to router/firewall

4. Switch Port Modes

4.1. Access Port

Belongs to exactly one VLAN.

Sends and receives only untagged frames.

Used for end devices (PCs, printers, IP phones).

Configuration:

```
switchport mode access
switchport access vlan X
```

Strongly recommended to explicitly configure mode access (security).

4.2. Trunk Port (ISLCisco & IEEE 802.1Q)

Carries traffic for multiple VLANs.

Uses tagging to identify VLAN membership.

ISL (Cisco proprietary) - deprecated.

802.1Q (IEEE standard) - current standard used everywhere.

Configuration:

```
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30
```

4.3. Dynamic Auto / Dynamic Desirable (DTP Modes Table)

Dynamic Trunking Protocol (DTP) negotiates trunking:

dynamic desirable: Actively tries to form a trunk - trunks with trunk, desirable, or auto

dynamic auto: Passively waits - trunks only if partner is trunk or desirable

trunk: Permanently trunking

access: Permanently access (no trunking)

Best practice: Disable DTP with switchport nonegotiate

4.4. How Switches Decide: Tagging vs Untagging Rules (Decision Matrix)

When a frame enters a port:

Access port ---> untagged frame assigned to configured access VLAN

Trunk port ---> tagged frame forwarded based on VID

Trunk port ---> untagged frame assigned to native VLAN

When a frame exits a port:

Access port ---> always sent untagged

Trunk port ---> tagged (except native VLAN traffic → sent untagged)

Port Type	Incoming Frame	Switch Action	Outgoing Frame
Access	Any	Assign to access VLAN	Untagged
Trunk	Tagged	Forward by VLAN ID	Tagged
Trunk	Untagged	Assigned to native VLAN	Untagged
Trunk	Native VLAN	Forward	Untagged
Trunk	Other VLAN	Forward	Tagged

5. Hands-On Lab: VLAN Implementation in GNS3

5.1. Lab Objectives

Create VLAN 10 (IT), VLAN 20 (Finance), VLAN 30 (Sales)

Assign ports to correct VLANs

Configure Management VLAN

Use SPAN to capture frames and verify tagging behavior

5.2. Lab Topology Overview

One Cisco L2 switch

Six PCs across three VLANs

One monitoring PC for SPAN

5.3. Devices and Software Used

GNS3

Cisco vIOS-L2

Seven VPCS nodes

Wireshark

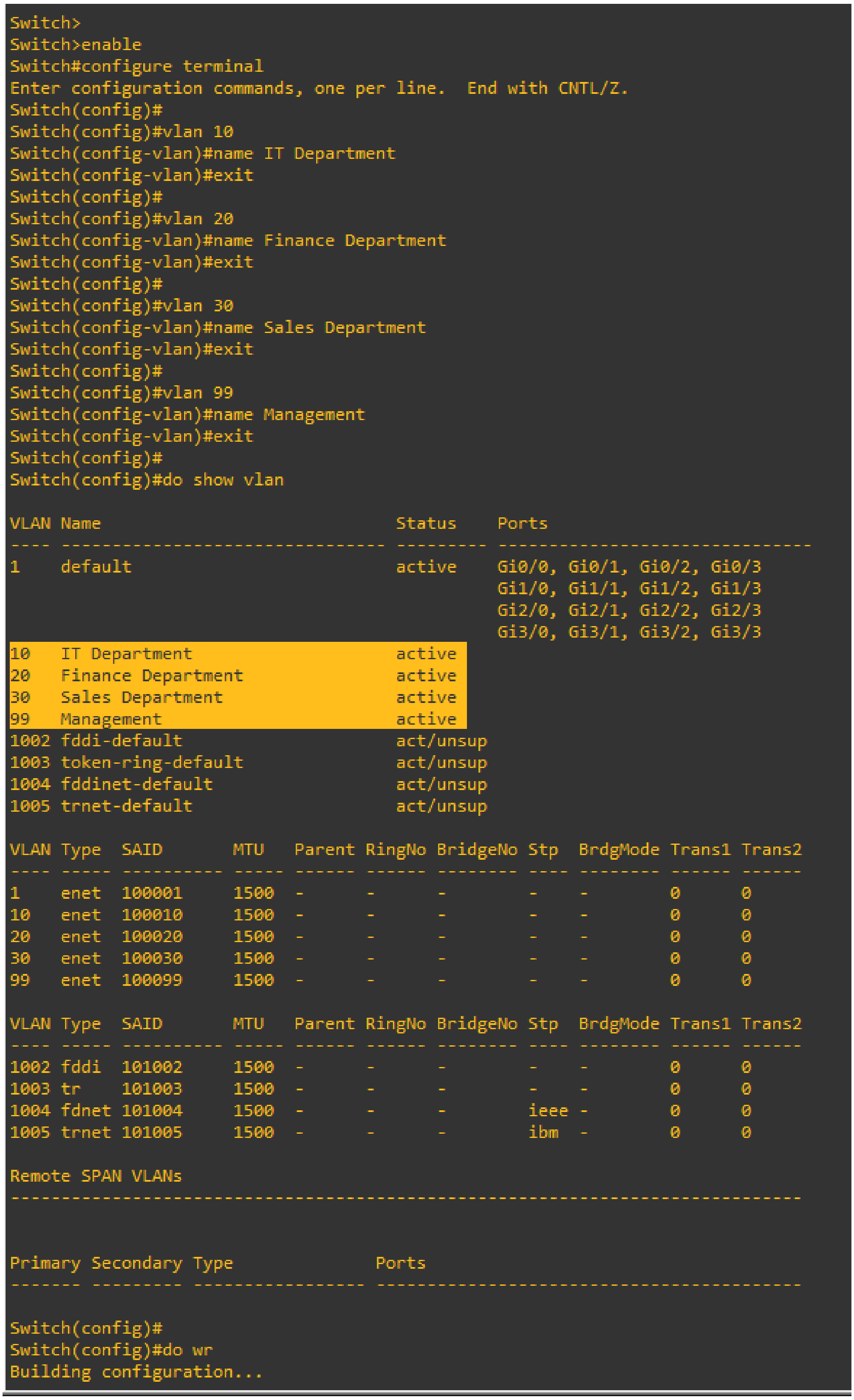
5.4. VLAN & IP Allocation Table

DEPARTMENT	VLAN	Name	IP Address
IT Department	VLAN 10	PC1-VLAN--10	192.168.1.2
		PC2-VLAN--10	192.168.1.3
Finance Department	VLAN 20	` PC3-VLAN--20	192.168.1.4
		PC4-VLAN--20	192.168.1.5
Sales Department	VLAN 30	PC5-VLAN--30	192.168.1.6
		PC6-VLAN--30	192.168.1.7
SPAN (Switched Port Analyzer) Management	VLAN 99	Switch SVI	192.168.1.1

5.5. Step-by-Step Switch Configuration

5.5.1. Creating VLANs

```
enable
configure terminal

vlan 10
name IT Department
exit

vlan 20
name Finance Department
exit

vlan 30
name Sales Department
exit

vlan 99
name Management
exit

do show vlan
do wr
```



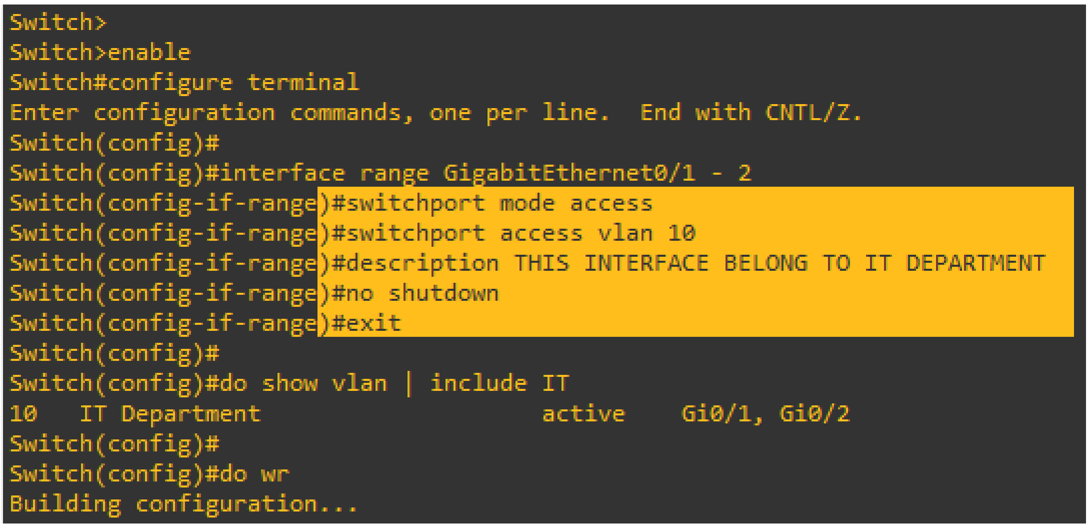
```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name IT Department
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 20
Switch(config-vlan)#name Finance Department
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 30
Switch(config-vlan)#name Sales Department
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 99
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#do show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                                Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                                Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                                Gi3/0, Gi3/1, Gi3/2, Gi3/3
10   IT Department                    active
20   Finance Department               active
30   Sales Department                 active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch(config)#
Switch(config)#do wr
Building configuration...
```

5.5.2. Configuring Access Ports

VLAN 10

```
enable
```

```
configure terminal


interface range GigabitEthernet0/0 - 3
switchport mode access
switchport access vlan 10
description THIS INTERFACE BELONG TO IT DEPARTMENT
no shutdown
exit


do show vlan | include IT
```

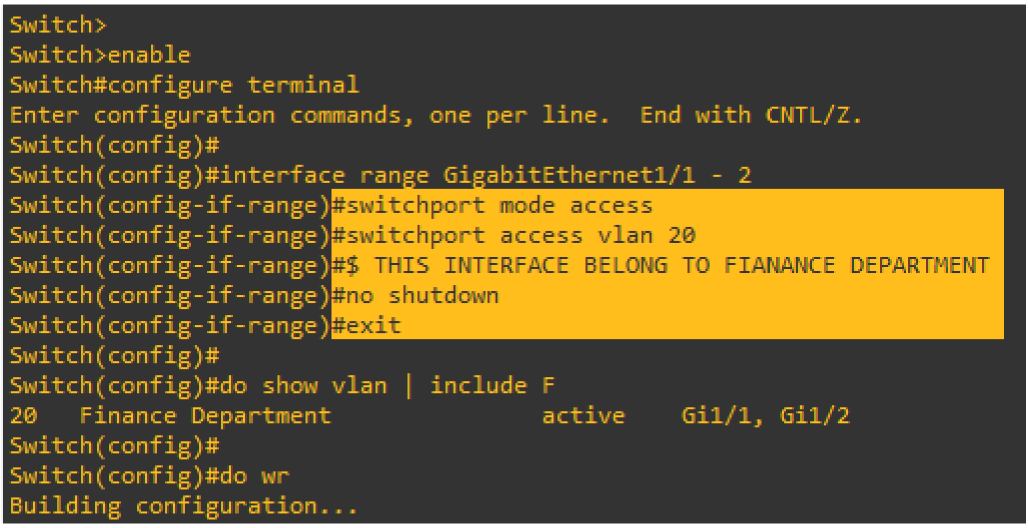


```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface range GigabitEthernet0/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#description THIS INTERFACE BELONG TO IT DEPARTMENT
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do show vlan | include IT
10   IT Department                    active    Gi0/1, Gi0/2
Switch(config)#
Switch(config)#do wr
Building configuration...
```

VLAN 20

```
enable
configure terminal


interface range GigabitEthernet1/0 - 3
switchport mode access
switchport access vlan 20
description THIS INTERFACE BELONG TO FIANANCE DEPARTMENT
no shutdown
exit
```

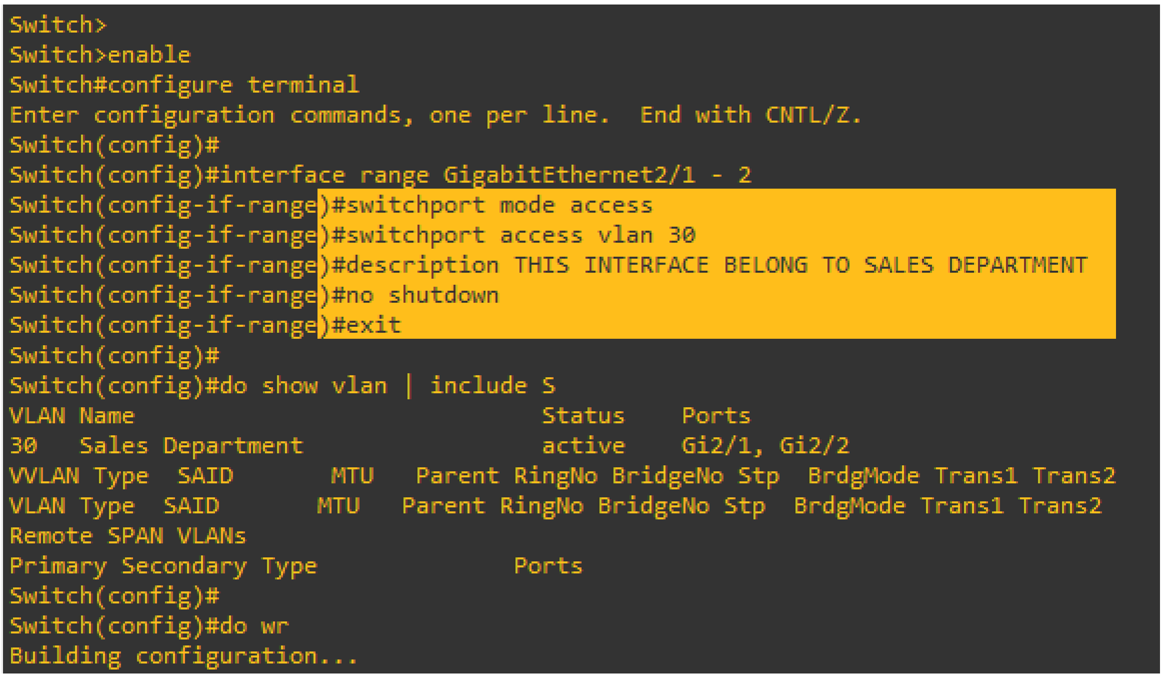
```
do show vlan | include Fi
```



```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface range GigabitEthernet1/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#$ THIS INTERFACE BELONG TO FIANANCE DEPARTMENT
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do show vlan | include F
20   Finance Department               active    Gi1/1, Gi1/2
Switch(config)#
Switch(config)#do wr
Building configuration...
```

VLAN 30

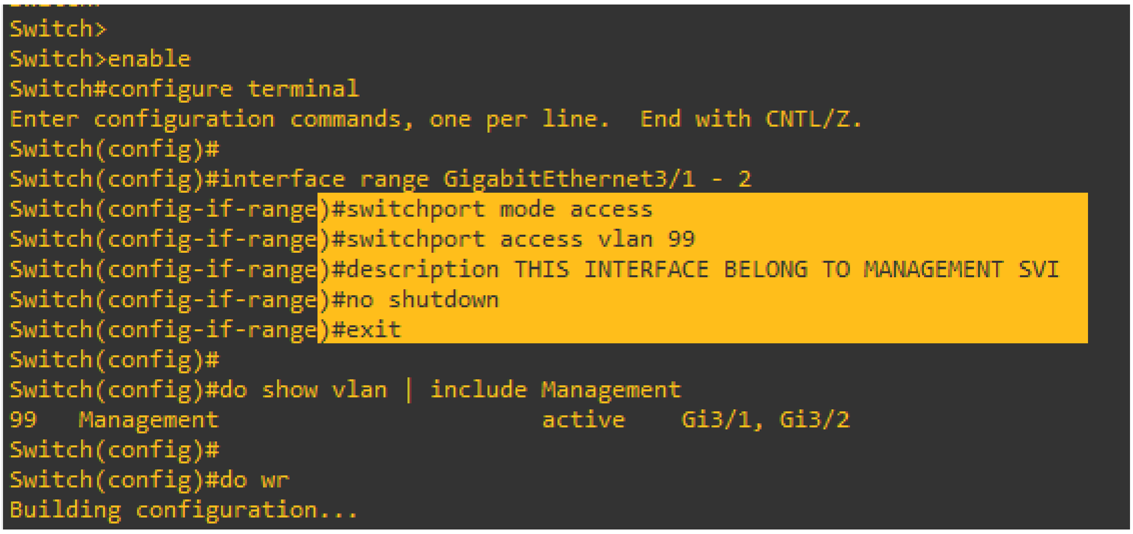
```
enable
configure terminal

interface range GigabitEthernet2/0 - 3
switchport mode access
switchport access vlan 30
description THIS INTERFACE BELONG TO SALES DEPARTMENT
no shutdown
exit

do show vlan | include Sales
```



```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface range GigabitEthernet2/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#description THIS INTERFACE BELONG TO SALES DEPARTMENT
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do show vlan | include S
VLAN Name                             Status    Ports
30   Sales Department                 active    Gi2/1, Gi2/2
VVLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
Remote SPAN VLANs
Primary Secondary Type              Ports
Switch(config)#
Switch(config)#do wr
Building configuration...
```

VLAN 99

```
enable
configure terminal


interface range GigabitEthernet3/0 - 3
switchport mode access
switchport access vlan 99
description THIS INTERFACE BELONG TO MANAGEMENT SVI
no shutdown
exit


do show vlan | include Management
```



```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface range GigabitEthernet3/1 - 2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#description THIS INTERFACE BELONG TO MANAGEMENT SVI
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#do show vlan | include Management
99   Management                       active    Gi3/1, Gi3/2
Switch(config)#
Switch(config)#do wr
Building configuration...
```

6. SPAN (Switched Port Analyzer) Configuration

6.1. Why Use SPAN in VLAN Labs

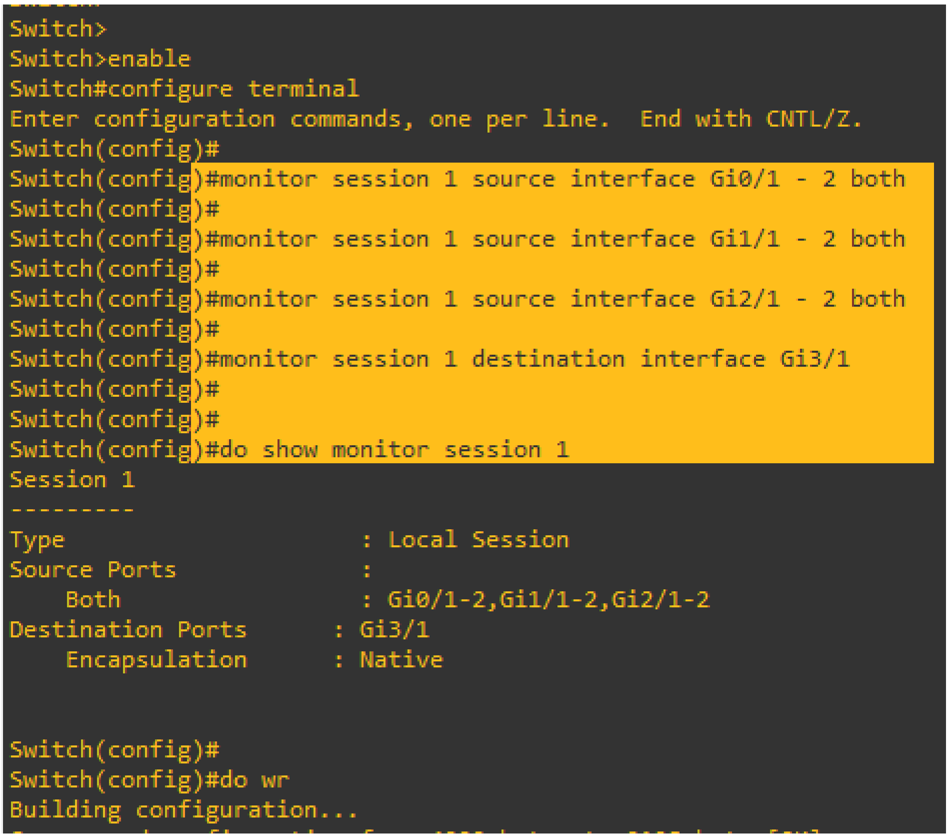
To see the truth - prove that access ports really send untagged frames.

6.2. Updated Topology with Monitoring Port

PC7 connected to Gi3/1 is used as the SPAN destination port --> receives mirrored traffic.

6.3. Complete SPAN Configuration

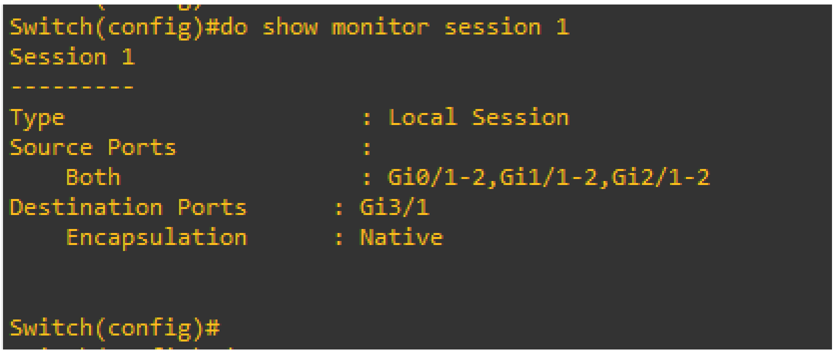
```
enable
configure terminal

monitor session 1 source interface Gi0/0 - 3 both

monitor session 1 source interface Gi1/0 - 3 both

monitor session 1 source interface Gi2/0 - 3 both

monitor session 1 destination interface Gi3/1
```



```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#monitor session 1 source interface Gi0/1 - 2 both
Switch(config)#
Switch(config)#monitor session 1 source interface Gi1/1 - 2 both
Switch(config)#
Switch(config)#monitor session 1 source interface Gi2/1 - 2 both
Switch(config)#
Switch(config)#monitor session 1 destination interface Gi3/1
Switch(config)#
Switch(config)#
Switch(config)#do show monitor session 1
Session 1
---------
Type                     : Local Session
Source Ports             :
    Both                 : Gi0/1-2,Gi1/1-2,Gi2/1-2
Destination Ports      : Gi3/1
    Encapsulation      : Native


Switch(config)#
Switch(config)#do wr
Building configuration...
```

6.4. Verifying SPAN Session

```
show monitor session 1
```



```
Switch(config)#do show monitor session 1
Session 1
---------
Type                     : Local Session
Source Ports             :
    Both                 : Gi0/1-2,Gi1/1-2,Gi2/1-2
Destination Ports      : Gi3/1
    Encapsulation      : Native


Switch(config)#
```

6.5. What You Should See in Wireshark

Access port traffic appears untagged

VLAN tag (TPID 0x8100) appears only on trunk links

Native VLAN traffic remains untagged even on a trunk

6.6. Tag Behavior Summary Table

Port Type	VLAN Tagging Behavior

Access Port	Always untagged
Trunk Port (Native VLAN)	Untagged
Trunk Port (Non-Native VLANs)	Tagged

7. Traffic Capture & VLAN Tag Analysis

7.1. Access-Port Traffic --> Untagged

We will see normal Ethernet II frames - no “802.1Q Virtual LAN” line in Wireshark.

7.2. Trunk Traffic --> Tagged (VLAN 10)

For Trunk Traffics there we should add a second switch --> make link trunk --> we will instantly see TPID 0x8100.

7.3. 802.1Q Header Breakdown in Wireshark

Priority Code Point (PCP)

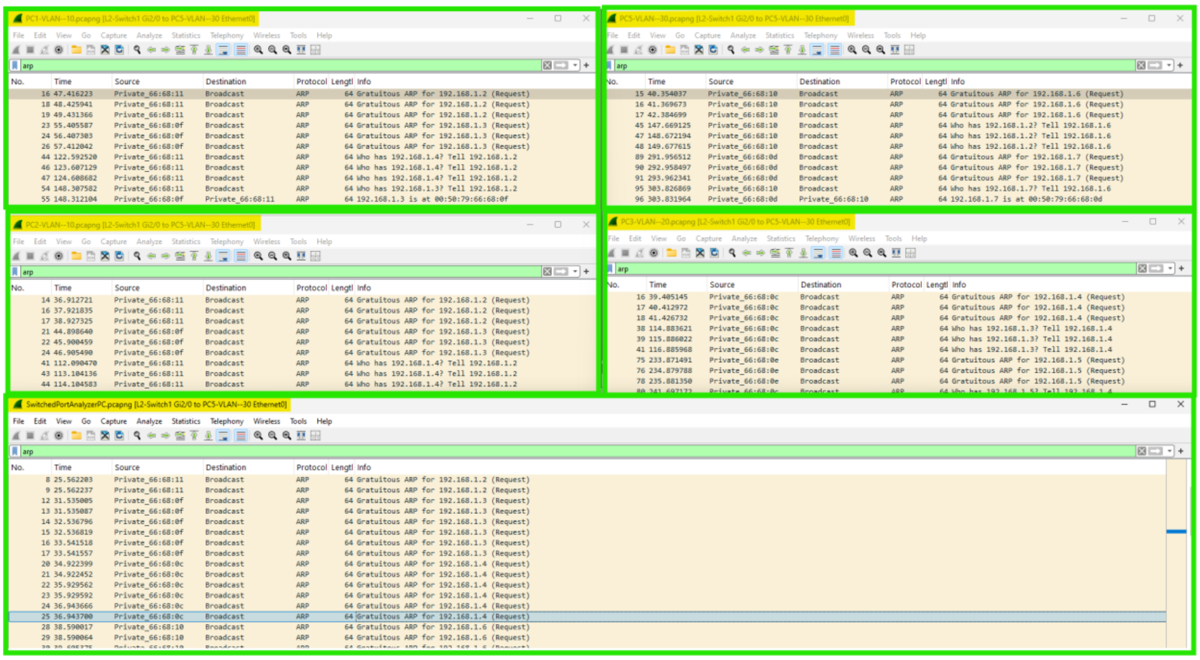
Drop Eligible Indicator (DEI)

VLAN Identifier (VID) → e.g., 10, 20, 30

7.4. Native VLAN Traffic --> Untagged on Trunk

Even on a trunk, native VLAN frames appear without tags.

7.5. Sample Packet Capture



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

PC1-VLAN--10.pcapng [L2-Switch1 Gi2/0 to PC5-VLAN--30 Ethernet0]

```
arp
No.   Time        Source              Destination         Protocol Lengtl Info
   16 47.416223   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   18 48.425941   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   19 49.431366   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   23 55.405587   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   24 56.407303   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   26 57.412042   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   44 122.592520  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.4? Tell 192.168.1.2
   46 123.607129  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.4? Tell 192.168.1.2
   47 124.608682  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.4? Tell 192.168.1.2
   54 148.307582  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.3? Tell 192.168.1.2
   55 148.312104  Private_66:68:0f    Private_66:68:11    ARP      64 192.168.1.3 is at 00:50:79:66:68:0f
```

PC5-VLAN--30.pcapng [L2-Switch1 Gi2/0 to PC5-VLAN--30 Ethernet0]

```
arp
No.   Time        Source              Destination         Protocol Lengtl Info
   15 40.354037   Private_66:68:10    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.6 (Request)
   16 41.369673   Private_66:68:10    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.6 (Request)
   17 42.384699   Private_66:68:10    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.6 (Request)
   45 147.669125  Private_66:68:10    Broadcast           ARP      64 Who has 192.168.1.2? Tell 192.168.1.6
   47 148.672194  Private_66:68:10    Broadcast           ARP      64 Who has 192.168.1.2? Tell 192.168.1.6
   48 149.677615  Private_66:68:10    Broadcast           ARP      64 Who has 192.168.1.2? Tell 192.168.1.6
   89 291.956512  Private_66:68:0d    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.7 (Request)
   90 292.958497  Private_66:68:0d    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.7 (Request)
   91 293.962341  Private_66:68:0d    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.7 (Request)
   95 303.826869  Private_66:68:10    Broadcast           ARP      64 Who has 192.168.1.7? Tell 192.168.1.6
   96 303.831964  Private_66:68:0d    Private_66:68:10    ARP      64 192.168.1.7 is at 00:50:79:66:68:0d
```

PC2-VLAN--10.pcapng [L2-Switch1 Gi2/0 to PC5-VLAN--30 Ethernet0]

```
arp
No.   Time        Source              Destination         Protocol Lengtl Info
   14 36.912721   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   16 37.921835   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   17 38.927325   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   21 44.898640   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   22 45.900459   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   24 46.905490   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   41 112.090470  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.4? Tell 192.168.1.2
   43 113.104136  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.4? Tell 192.168.1.2
   44 114.104583  Private_66:68:11    Broadcast           ARP      64 Who has 192.168.1.4? Tell 192.168.1.2
```

PC3-VLAN--20.pcapng [L2-Switch1 Gi2/0 to PC5-VLAN--30 Ethernet0]

```
arp
No.   Time        Source              Destination         Protocol Lengtl Info
   16 39.405145   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   17 40.412972   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   18 41.426732   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   38 114.883621  Private_66:68:0c    Broadcast           ARP      64 Who has 192.168.1.3? Tell 192.168.1.4
   39 115.886022  Private_66:68:0c    Broadcast           ARP      64 Who has 192.168.1.3? Tell 192.168.1.4
   41 116.885968  Private_66:68:0c    Broadcast           ARP      64 Who has 192.168.1.3? Tell 192.168.1.4
   75 233.871491  Private_66:68:0e    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.5 (Request)
   76 234.879788  Private_66:68:0e    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.5 (Request)
   78 235.881350  Private_66:68:0e    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.5 (Request)
   80 241.697172  Private_66:68:0c    Broadcast           ARP      64 Who has 192.168.1.5? Tell 192.168.1.4
```

SwitchedPortAnalyzerPC.pcapng [L2-Switch1 Gi2/0 to PC5-VLAN--30 Ethernet0]

```
arp
No.   Time        Source              Destination         Protocol Lengtl Info
    8 25.562203   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
    9 25.562237   Private_66:68:11    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.2 (Request)
   12 31.535005   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   13 31.535087   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   14 32.536796   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   15 32.536819   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   16 33.541518   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   17 33.541557   Private_66:68:0f    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.3 (Request)
   20 34.922399   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   21 34.922452   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   22 35.929562   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   23 35.929592   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   24 36.943666   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   25 36.943700   Private_66:68:0c    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.4 (Request)
   28 38.590017   Private_66:68:10    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.6 (Request)
   29 38.590064   Private_66:68:10    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.6 (Request)
   30 39.605375   Private_66:68:10    Broadcast           ARP      64 Gratuitous ARP for 192.168.1.6 (Request)
```

8. Key Observations & Learning Outcomes

Access ports always strip tags

Trunks preserve tags except for native VLAN

SPAN + Wireshark is the ultimate proof tool

Native VLAN mismatch = real production outages

9. Best Practices & Security Recommendations

Never use VLAN 1 for user traffic

Change native VLAN on all trunks (**switchport trunk native vlan 999**)

Disable DTP: **switchport nonegotiate**

Explicitly set **switchport mode access** or **trunk**

Use dedicated management VLAN (not 1)

10. Troubleshooting VLAN Issues

10.1. Top 5 VLAN Problems on the Exam

Native VLAN mismatch

Trunk not allowing required VLANs

Access port in wrong VLAN

DTP negotiation failure

Using VLAN 1 for user traffic

10.2. Native VLAN Mismatch Symptoms

%CDP-4-NATIVE_VLAN_MISMATCH logs

STP loops possible

10.3. Must-Know Commands + Expected Output

```
show vlan brief
show interfaces trunk
show interfaces switchport
show monitor session all
```

11. Conclusion

This document provides a complete understanding of VLAN configuration, 802.1Q tag behavior, native VLAN operation, and SPAN-based packet analysis. The combination of theory and hands-on practice in GNS3 allows accurate visualization of VLAN operations and prepares learners for both CCNA-level exams and real-world troubleshooting