VLANs

Virtual Local Area Networks

Cybersecurity AEC Program

What they are · How they are used · Tagging explained

The Problem: Flat Networks

What happens when there is no segmentation?

A company with four departments — Sales, HR, Engineering, Research — all on daisy-chained switches with a single router:

1 Broadcast Flooding

A single ARP request from Sales reaches every device on the entire network, wasting bandwidth across all departments.

Every broadcast hits every host.

2 Single Point of Failure

If one middle switch dies, every department behind it is completely cut off from the network and Internet.

One failure isolates entire groups.

3 Zero Logical Separation

Any user can sniff traffic from any other department. No boundary between sensitive HR data and Sales.

No security between departments.

KEY TAKEAWAY A flat network has no segmentation — broadcasts reach everyone, failures cascade, and there is no isolation between departments.

What Is a VLAN? (1/2)

Definition & the Hotel Analogy

VLAN = Virtual Local Area Network

A VLAN takes one physical switch and divides it into multiple independent, logical switches — each with its own isolated broadcast domain.

The Hotel Analogy

Imagine a 10-floor hotel. Without VLANs, every guest shares the same hallways and noise. With VLANs, invisible walls create separate zones:

Floors	Zone	Access
1 – 3	Business Zone	Business guests only
4 – 6	Family Zone	Families only
7 – 10	VIP Zone	VIP guests only

Physical vs. Logical

Same physical building

Completely separate logical spaces

Guests in one zone cannot access another

A VLAN does exactly this for a network switch.

KEY TAKEAWAY A VLAN is a virtual broadcast domain — it segments one physical switch into multiple isolated logical networks, no extra hardware required.

What Is a VLAN? (2/2)

Four fundamental properties

1 Each VLAN = One Broadcast Domain

A broadcast in VLAN 10 stays in VLAN 10. Period. Other VLANs never see it.

2 Location-Independent

Users don't need to be physically next to each other. An engineer on Floor 1 and Floor 3 can share the same VLAN.

3 Inter-VLAN = Layer 3 Required

Communication between VLANs requires a router or multilayer switch. Without one, VLANs are completely isolated.

4 Default: All Ports in VLAN 1

On Cisco switches, every port starts assigned to VLAN 1. You must manually assign ports to other VLANs.

KEY TAKEAWAY Communication between VLANs only happens through a Layer 3 device (router). Without routing, VLANs are like separate physical networks.

VLANs in Cybersecurity (1/2)

Three critical security functions

1. Segmentation & Lateral Movement Prevention

- An attacker who compromises a workstation in VLAN 30 (Sales) is trapped inside that VLAN
- Cannot directly reach servers in VLAN 10 or management interfaces in VLAN 99
- Limits lateral movement — one of the most dangerous phases of a cyberattack
- MITRE ATT&CK: Lateral Movement (TA0008)

2. Access Control Enforcement

- VLANs + ACLs or firewall rules at Layer 3 control who communicates with whom
- Example: Guest Wi-Fi VLAN reaches Internet but has zero access to internal file servers

3. Regulatory Compliance

- PCI-DSS requires cardholder data environments to be segmented
- HIPAA, SOX, and NIST 800-171 all recommend or mandate network segmentation
- VLANs are a primary tool to achieve and demonstrate compliance

KEY TAKEAWAY VLANs limit lateral movement, enforce access boundaries, and satisfy compliance mandates like PCI-DSS, HIPAA, and NIST 800-171.

VLANs in Cybersecurity (2/2)

Limitations — VLANs are NOT firewalls

IMPORTANT CAVEAT

VLANs operate at **Layer 2 only** — they are not a substitute for a firewall

Security professionals must know how to **build** these controls AND how to **break** them

VLAN Hopping: Double-Tagging

Attacker crafts a frame with two 802.1Q tags. The outer tag matches the native VLAN, the inner tag targets a victim VLAN. The first switch strips the outer tag and forwards the inner-tagged frame to the victim VLAN.

VLAN Hopping: Switch Spoofing

Attacker configures their NIC to negotiate a trunk with the switch using DTP (Dynamic Trunking Protocol). If successful, the attacker's port becomes a trunk and can access all VLANs.

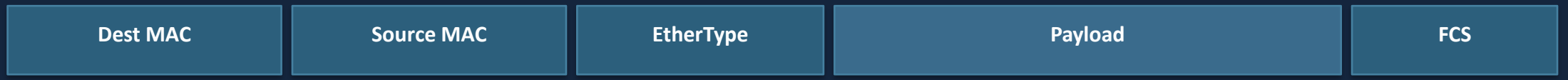
Mitigations

- Change native VLAN to an unused VLAN
- Disable DTP on all access ports (switchport nonegotiate)
- Explicitly configure access ports — never leave them in dynamic mode
- Prune unused VLANs from trunks

The Tagging Problem

Why standard Ethernet frames aren't enough

Standard Ethernet Frame — No VLAN field exists:



The Problem:

Two switches share traffic from multiple VLANs over a single cable (trunk)

When Switch B receives a frame, it has no way to know if it came from VLAN 10 or VLAN 20

The standard Ethernet frame has no VLAN identification field whatsoever

The Solution: Trunk Links + a Tagging Protocol

Protocol	Standard	Support
802.1Q	IEEE open standard	All major vendors — industry standard
ISL	Cisco proprietary (legacy)	Cisco only — being phased out

KEY TAKEAWAY Standard Ethernet frames carry no VLAN information. Trunk links use 802.1Q tagging to label each frame with its VLAN identity.

802.1Q Tag — Anatomy

A 4-byte tag inserted into the Ethernet frame

802.1Q Tagged Frame:

Inside the 802.1Q Tag (4 bytes / 32 bits):

Field	Size	Purpose
TPID (Tag Protocol ID)	16 bits	Fixed value 0x8100 — identifies frame as 802.1Q tagged
PCP (Priority Code Point)	3 bits	QoS priority level (0–7); e.g., VoIP = priority 5
DEI (Drop Eligible)	1 bit	Marks frame as eligible for dropping under congestion
VID (VLAN Identifier)	12 bits	The VLAN number — range 0–4095, usable: 1–4094

Key Numbers to Remember:

4 bytes
Total tag size

12 bits → 4,094
Usable VLANs

0x8100
EtherType identifier

How Tagging Works — Step by Step

Computer A (VLAN 10, Switch A) → Computer B (VLAN 10, Switch B)

Step	Action	Frame State
1	Computer A sends a normal Ethernet frame into Switch A's access port (VLAN 10)	Untagged
2	Switch A associates the frame with VLAN 10 based on port assignment	—
3	Switch A inserts the 802.1Q tag (VID=10) and sends it out the trunk port	Tagged
4	Switch B receives the frame on its trunk port and reads the tag: VLAN 10	Tagged
5	Switch B removes the tag and delivers the clean frame to Computer B (VLAN 10)	Untagged

Two Essential Rules:

Rule 1: End devices never see the tag

Tagging/untagging happens entirely on trunk links between switches

Rule 2: Access ports = always untagged

The switch handles VLAN identification internally based on port assignment

KEY TAKEAWAY Switches add the 802.1Q tag when sending onto a trunk and strip it when delivering to an access port. Tagging is transparent to hosts.

The Native VLAN

The exception to the tagging rule

The native VLAN is the one VLAN on a trunk whose frames are sent WITHOUT an 802.1Q tag.

Property	Detail
Default native VLAN	VLAN 1
Behavior on trunk	Native VLAN frames cross the trunk untagged
Receiving switch	Untagged frames on a trunk → assumed native VLAN
Critical requirement	Native VLAN must match on both sides of the trunk
What travels here?	CDP, STP BPDUs, VTP, and non-802.1Q-aware devices

Security: Double-Tagging Attack

- Attacker sends frame with two 802.1Q tags
- Outer tag = native VLAN (gets stripped)
- Inner tag = victim VLAN (gets forwarded)
- Result: frame reaches a VLAN it shouldn't

Best Practices:

- Change native VLAN from VLAN 1 to an unused VLAN
- Match native VLAN on both ends of every trunk
- Tag the native VLAN explicitly (Cisco: vlan dot1q tag native)

KEY TAKEAWAY The native VLAN is untagged on trunks — a VLAN hopping vector. Always change it from default, ensure it matches, and consider tagging it.

Port Types at a Glance

Access port vs. Trunk port

ACCESS PORT

Belongs to

One single VLAN

Connected to

End devices (PCs, printers, phones)

Tagging

None — frames always untagged

VLAN assignment

Configured per-port

Switch behavior

Associates all incoming frames with the configured VLAN

TRUNK PORT

Belongs to

Carries multiple VLANs

Connected to

Other switches or routers

Tagging

802.1Q on all VLANs (except native)

VLAN assignment

Allowed VLAN list configurable

Switch behavior

Reads 802.1Q tag to determine VLAN; untagged → native

KEY TAKEAWAY Access ports = single VLAN, untagged, for end devices. Trunk ports = multiple VLANs, 802.1Q tagged, for switch-to-switch links.

InterVLAN Routing

Bridging the gap between isolated VLANs

VLANs are isolated by design — a device in VLAN 10 cannot reach VLAN 20 at Layer 2. A Layer 3 device must route between them.

1 Router on a Stick

Single router with sub-interfaces, one per VLAN, connected via 802.1Q trunk to the switch.

Best for: Small networks, labs

2 SVI (Switch Virtual Interface)

Multilayer (L3) switch creates virtual interfaces per VLAN and routes internally — fast, no extra hardware.

Best for: Enterprise networks

3 Routed Port

Switch port configured as a Layer 3 interface (no VLAN) for point-to-point routing.

Best for: Distribution / core uplinks

Security: Every inter-VLAN routing point is a policy enforcement point — apply ACLs or firewall rules to control which VLANs communicate.

KEY TAKEAWAY VLANs isolate at Layer 2; Layer 3 routing is required for inter-VLAN communication. Each routing point is an opportunity for security policy enforcement.

Troubleshooting VLANs & Trunks

Common issues and verification

VLAN Problems

Symptom	Likely Cause
Same-VLAN hosts can't communicate	Ports in different VLANs
No connectivity after VLAN change	VLAN doesn't exist on switch
Traffic blocked unexpectedly	VACL (VLAN Access List) applied

Trunk Problems

Symptom	Likely Cause
Trunk not forming	Encapsulation mismatch
Some VLANs not passing	Not in allowed list
Intermittent connectivity	Native VLAN mismatch
Wrong port mode	DTP negotiation conflict

Essential Verification Commands (Cisco IOS)

Command	What It Shows
show vlan brief	VLAN list and port assignments
show interfaces trunk	Trunk status, encapsulation, native VLAN, allowed VLANs
show interfaces switchport	Detailed port mode and VLAN information

KEY TAKEAWAY Most issues: wrong VLAN assignment, VLAN not created, encapsulation mismatch, native VLAN mismatch, or VLAN missing from trunk allowed list.

Summary — The Big Picture

VLANs segment a physical switch into isolated virtual broadcast domains, enabling security, performance, and compliance.

1

VLAN = Virtual Broadcast Domain

One physical switch → multiple isolated logical networks

2

802.1Q = The Tagging Protocol

A 4-byte tag with 12-bit VLAN ID inserted on trunk links

3

VLANs = A Cybersecurity Control

Limits lateral movement, enforces access, meets PCI-DSS

What Connects Forward:

This Lesson	Leads To
VLAN isolation	InterVLAN routing (Router on a Stick, SVIs)
802.1Q tagging	VLAN hopping attacks & mitigation
Native VLAN	Double-tagging attack lab
Access vs. trunk ports	Port security & 802.1X authentication
Network segmentation	Zero Trust Architecture

Challenge Question

?

If VLANs isolate networks at Layer 2, what device or mechanism do we need to allow a host in VLAN 10 to communicate with a host in VLAN 20 — and what new security risks does that introduce?

Hint: The answer connects networking fundamentals to firewall policy, ACL design, and the principle of least privilege.

Think about this before next class!