# Day 03 — Access VLAN Segmentation (Enterprise Operations Cheat Sheet)

## Purpose

Enforce strict Layer-2 isolation between USERS and ADMINS using access VLANs on a Cisco access switch. This document is an operational reference for build, verification, failure injection, and recovery. No routing and no default gateway are used.

## Baseline

- Cisco access switch (e.g., Catalyst 2960)
- End devices connected to access ports only
- No Layer-3 device present
- Objective is pure Layer-2 segmentation

## VLAN Definitions

VLAN 10 — USERS
VLAN 20 — ADMINS

## Build — Configuration

```
enable
configure terminal

vlan 10
name USERS
exit

vlan 20
name ADMINS
exit

interface FastEthernet0/1
description PC1-USERS
switchport mode access
switchport access vlan 10
no shutdown
exit

interface FastEthernet0/2
description PC2-ADMINS
switchport mode access
switchport access vlan 20
no shutdown
exit

interface range FastEthernet0/3-24
```

```
shutdown
exit

end
write memory
```

## Verification

```
show vlan brief
show interfaces status
show mac address-table
```

## End-Device IP Configuration (No Gateway)

PC1 (USERS / VLAN 10): 10.1.1.10 /24
PC2 (ADMINS / VLAN 20): 10.1.1.11 /24
Default Gateway: NONE

## Isolation Proof

```
PC1 → ping 10.1.1.11 → FAIL
PC2 → ping 10.1.1.10 → FAIL
```

## Failure Injection

```
configure terminal
interface FastEthernet0/1
switchport access vlan 20
end
```

## Recovery

```
show interfaces status

configure terminal
interface FastEthernet0/1
switchport access vlan 10
end
```

## Enterprise Memory Locks

- VLAN enforcement occurs at the ingress access port
- IP addressing does not override VLAN isolation
- Access ports belong to exactly one VLAN
- Unused ports must be administratively shut down
- Verification is mandatory before and after changes