

Document élève — formalisation après le geste TP CBS350.

o. Réactivation sans document

1. [RAPPEL] Que sépare un VLAN ? _____
2. Différence access / trunk ? _____
3. Pourquoi un ping inter-VLAN échoue sans routeur ? _____

1. Du geste à la règle

Le geste vu sur CBS350 (vlan, switchport mode access/trunk, show vlan brief) devient la règle : **un VLAN = un domaine de broadcast.**

Corps du cours (contenu validé préservé)

COURS 1 — Les VLAN : Concepts fondamentaux

Séquence 07 — VLAN Segmentation réseau Séance S1 — Cours interactif + TP1 (3h) Classe : 1CIEL — La Réunion

Objectif du cours

À l'issue de cette partie, tu dois être capable de :

- Expliquer ce qu'est un VLAN et pourquoi on segmente un réseau
- Distinguer un domaine de diffusion (broadcast) avec et sans VLAN
- Identifier la différence entre un port **access** et un port **trunk**
- Connaître les commandes CLI de base pour créer un VLAN sur un switch Cisco

1. Le problème : le réseau plat

Situation de départ — TechServices Réunion

L'entreprise TechServices Réunion a un réseau avec **un seul switch** et **tous les postes sur le même réseau** (VLAN 1 par défaut). Tous les utilisateurs — administrateurs, techniciens, direction — partagent le même réseau. RÉSEAU PLAT (avant intervention)

SWITCH (VLAN 1 par défaut)	
P1: PC Admin	P5: PC Technicien 1
P2: PC Compta	P6: PC Technicien 2
P3: PC Direction	P7: Imprimante
P4: PC RH	P8: Serveur

→ TOUT le monde est dans le MÊME domaine de broadcast

Les problèmes concrets

Problème	Explication concrète
Sécurité	Un technicien peut "sniffer" le trafic de la direction (mots de passe, fichiers confidentiels)

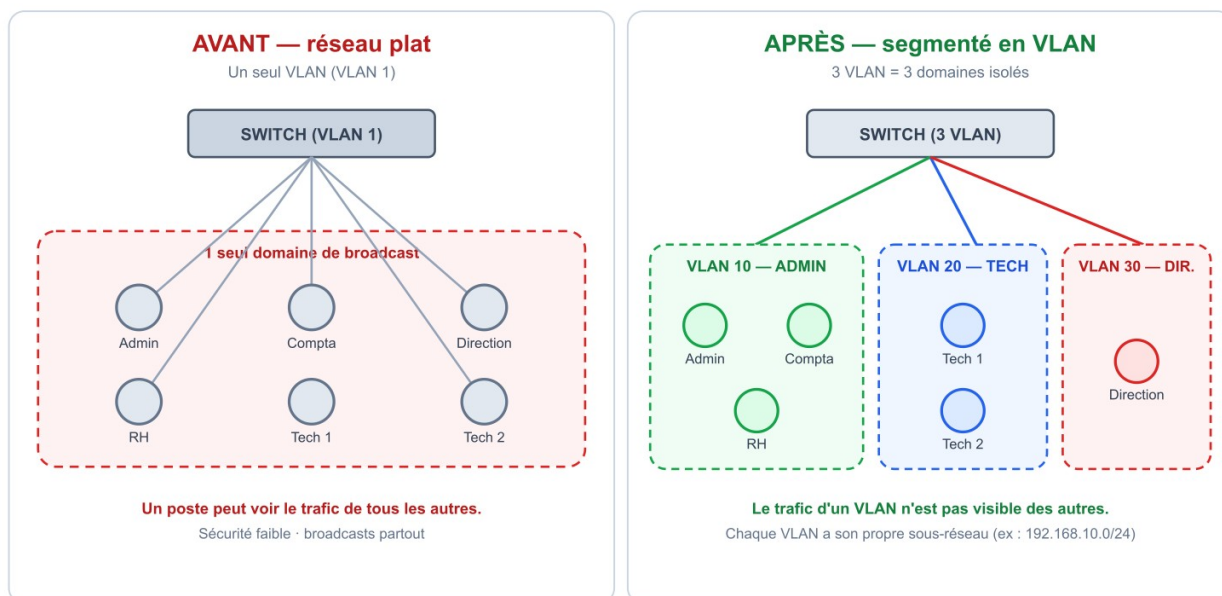
Problème	Explication concrète
Performance	Un broadcast envoyé par le PC Admin est reçu par TOUS les postes — même ceux qui n'en ont pas besoin
Organisation	Impossible de séparer les règles réseau par département (ex : interdire l'accès serveur aux invités)

Analogie : C'est comme si tous les bureaux d'une entreprise étaient dans la même pièce ouverte, sans cloisons. Tout le monde entend tout, tout le monde peut accéder à tout.

2. La solution : les VLAN

Pourquoi segmenter un réseau en VLAN ?

Réseau plat vs réseau segmenté — TechServices Réunion



Comparaison réseau plat (avant) et réseau segmenté en 3 VLAN (après) — cas TechServices Réunion.

Définition

Un **VLAN** (Virtual Local Area Network) est un réseau local **virtuel** qui regroupe logiquement des ports d'un ou plusieurs switches, indépendamment de leur position physique.

Chaque VLAN crée un **domaine de broadcast séparé**. Les machines dans un VLAN ne peuvent communiquer qu'avec les machines du même VLAN (sauf si un routeur les interconnecte).

Le réseau segmenté — Objectif cible

RÉSEAU SEGMENTÉ (après intervention)

SWITCH (3 VLANs configurés)		
VLAN 10 — ADMIN	VLAN 20 — TECH	
P1: PC Admin	P5: PC Technicien 1	
P2: PC Compta	P6: PC Technicien 2	
P4: PC RH	P7: Imprimante Tech	
VLAN 30 — DIRECTION		
P3: PC Direction		

Broadcast VLAN 10 ≠ Broadcast VLAN 20 ≠ Broadcast VLAN 30

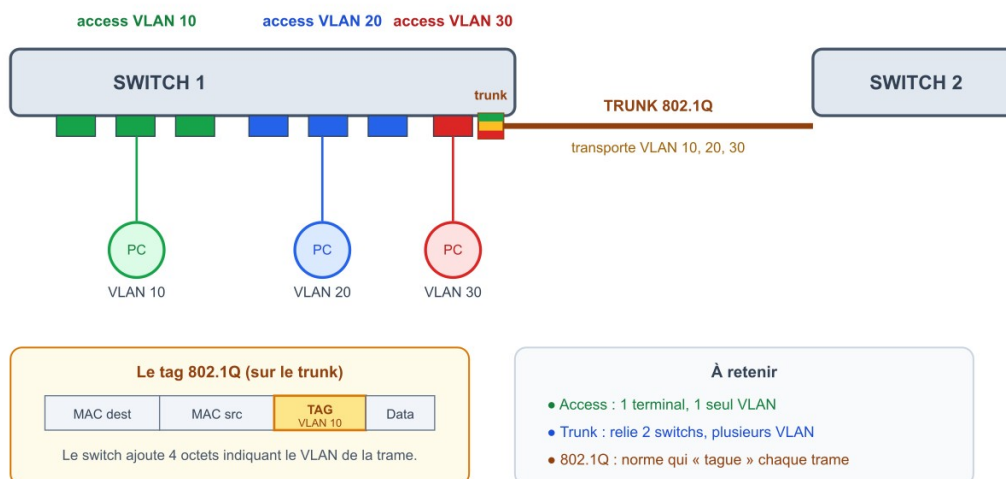
→ Isolation complète entre départements

Les avantages (à retenir)

Avantage	Ce que ça change concrètement
Sécurité	Le trafic d'un VLAN n'est pas visible depuis un autre VLAN
Performance	Les broadcasts sont limités au VLAN concerné (moins de trafic inutile)
Flexibilité	On peut déplacer un PC d'un département à un autre en changeant le VLAN du port (sans toucher au câblage)
Organisation	Regroupement logique par fonction, pas par emplacement physique

3. Port Access vs Port Trunk**Port Access vs Port Trunk**

Access = 1 terminal, 1 VLAN · Trunk = plusieurs VLAN entre deux switches



Ports access (un terminal, un VLAN) et port trunk 802.1Q (plusieurs VLAN entre deux switches).
Il existe **deux types de ports** sur un switch configuré en VLAN :

Port Access (accès)

- Connecte un **terminal** (PC, imprimante, serveur)
- Appartient à **un seul VLAN**
- Le terminal ne sait pas qu'il est dans un VLAN (c'est transparent)

PORT ACCESS

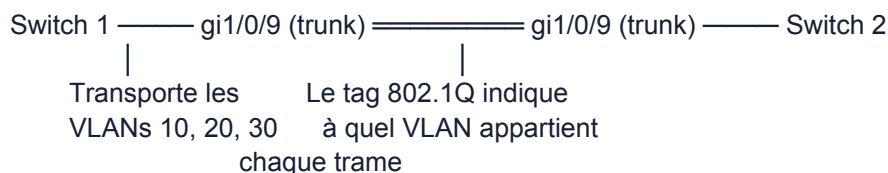
PC (ne sait rien des VLANs)

câble Ethernet normal

Switch — Port gi1/0/1 — mode ACCESS — VLAN 10

Port Trunk (liaison inter-switch)

- Connecte **deux switches** entre eux (ou un switch à un routeur)
- Transporte le trafic de **plusieurs VLANs** simultanément
- Utilise le protocole **IEEE 802.1Q** pour « taguer » chaque trame avec son numéro de VLAN



Le tagging 802.1Q (simplifié)

Quand une frame traverse un port trunk, le switch ajoute un **tag de 4 octets** dans l'en-tête Ethernet qui contient le numéro du VLAN :

TRAME ETHERNET NORMALE (port access) :



TRAME ETHERNET TAGUÉE 802.1Q (port trunk) :



▲
4 octets ajoutés par le switch
contient le VLAN ID

Tableau récapitulatif

Caractéristique	Port Access	Port Trunk
Connecte	Un terminal (PC, imprimante)	Un autre switch ou un routeur
VLANs	1 seul	Plusieurs (tagués 802.1Q)
Tagging	Non (transparent pour le terminal)	Oui (802.1Q)
Commande CLI	switchport mode access	switchport mode trunk

4. Les commandes CLI essentielles (Cisco IOS)

Créer un VLAN

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name ADMIN
Switch(config-vlan)# exit
```

Affecter un port en mode Access

```
Switch(config)# interface gi1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

Configurer un port Trunk

```
Switch(config)# interface gi1/0/9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30
Switch(config-if)# exit
```

Vérifier la configuration

Switch# show vlan brief → Liste des VLANs et ports
 Switch# show interfaces trunk → Ports trunk configurés
 Switch# show running-config → Configuration complète

5. Plan d'adressage TechServices Réunion

VLAN	ID	Nom	Réseau	Passerelle	Postes
VLAN 10	10	ADMIN	192.168.10.0/24	192.168.10.254	PC Admin, Compta, RH
VLAN 20	20	TECH	192.168.20.0/24	192.168.20.254	PC Techniciens, Imprimante
VLAN 30	30	DIRECTION	192.168.30.0/24	192.168.30.254	PC Direction

Règle : chaque VLAN a son propre sous-réseau IP. Les VLANs ne peuvent pas communiquer entre eux sans routeur (on verra ça en séquence B08).

Dans notre exemple TechServices, nous dimensionnerons chaque VLAN selon les besoins réels : VLAN 10 (ADMIN) reçoit 8 postes, VLAN 20 (TECH) 13 postes, VLAN 30 (DIRECTION) 5 postes. Tu feras cet exercice de dimensionnement en TP3.

6. Vocabulaire clé

Terme	Définition simple
VLAN	Réseau virtuel qui isole un groupe de ports sur un switch
Broadcast domain	Zone où un broadcast est diffusé — un VLAN = un broadcast domain
Port Access	Port connecté à un terminal, appartient à 1 seul VLAN
Port Trunk	Port qui transporte plusieurs VLANs entre switches (tag 802.1Q)
802.1Q	Norme IEEE qui permet de taguer les trames avec un numéro de VLAN
VLAN natif	VLAN non tagué sur un trunk (par défaut VLAN 1, à changer pour la sécurité)
show vlan brief	Commande CLI pour voir les VLANs et leurs ports

Cours 1 — Séquence 07 VLAN — BAC PRO CIEL 1CIEL