

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 2 — Isolation VLAN, 802.1Q et Dépannage méthodique

Séquence 07 — VLAN Segmentation réseau Séance S3 — Cours + TP Diagnostic (2h) Classe : 1CIEL — La Réunion

Objectif du cours

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

- Expliquer pourquoi les VLANs isolent les communications (ARP confiné)
- Comprendre le fonctionnement détaillé du tagging 802.1Q
- Appliquer une méthode de dépannage VLAN systématique
- Identifier et corriger les erreurs de configuration courantes

1. Pourquoi les VLANs isolent vraiment

Le mécanisme : ARP confiné au VLAN

Quand PC-A1 (VLAN 10) veut communiquer avec une autre machine, il envoie d'abord une **requête ARP** (broadcast) pour trouver l'adresse MAC de la destination.

Sans VLAN (réseau plat) :

PC-A1 envoie ARP broadcast → TOUS les ports du switch reçoivent la requête
→ Tous les PCs répondent s'ils reconnaissent l'IP
→ Le broadcast "inonde" tout le réseau

Avec VLAN :

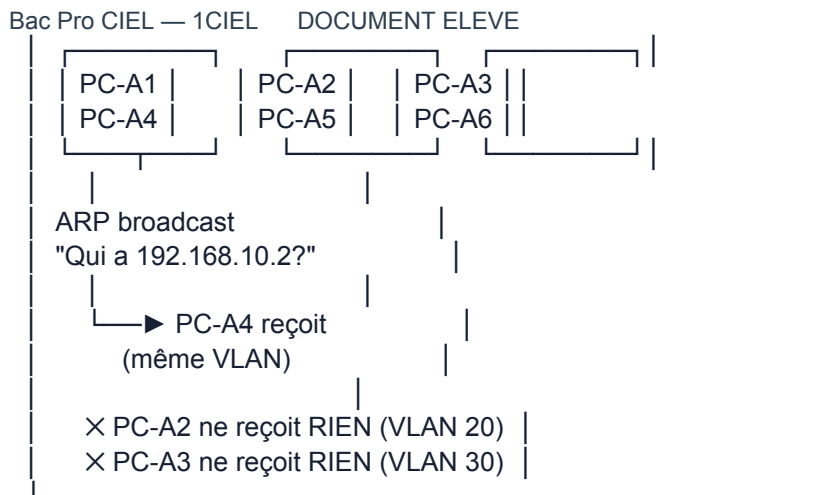
PC-A1 (VLAN 10) envoie ARP broadcast
→ SEULS les ports du VLAN 10 reçoivent la requête
→ Les ports VLAN 20 et VLAN 30 ne voient RIEN
→ Le broadcast est "confiné" dans le VLAN 10

Conséquence directe : même si PC-A1 connaît l'IP de PC-B2 (VLAN 20), la requête ARP ne sortira jamais du VLAN 10. Pas d'ARP = pas de résolution MAC = pas de communication.

Schéma : Le broadcast confiné

SWITCH avec 3 VLANs





2. Le tagging 802.1Q en détail

Comment le switch sait quel trafic appartient à quel VLAN sur un trunk ?

Sur un **port access**, c'est simple : le port appartient à un seul VLAN, donc tout le trafic de ce port = ce VLAN.
Sur un **port trunk**, plusieurs VLANs passent par le même câble. Le switch utilise le protocole **IEEE 802.1Q** pour ajouter un **tag** (étiquette) de 4 octets dans la trame Ethernet :

Structure du tag 802.1Q (4 octets = 32 bits)

TPID	TCI		
(16 bits)	PRI(3)	CFI(1)	VID(12)
0x8100	QoS	format	VLAN ID

TPID = 0x8100 → indique "je suis une trame taguée 802.1Q"
VID = VLAN ID (0 à 4095) → le numéro du VLAN (ex : 10, 20, 30)

Ce qui se passe concrètement

PC-A1 (VLAN 10) envoie une trame à PC-B1 (VLAN 10, autre switch)

1. La trame arrive sur le port access gi1/0/1 (VLAN 10)

→ Trame NORMALE (pas de tag)

2. Le switch doit envoyer la trame sur le trunk gi1/0/9

→ Il AJOUTE le tag 802.1Q avec VID = 10

3. La trame traverse le trunk jusqu'à SW2

→ La trame contient le tag VID = 10

4. SW2 reçoit la trame sur son port trunk

→ Il LIT le tag : VID = 10

→ Il RETIRE le tag

→ Il envoie la trame sur les ports du VLAN 10 uniquement

Le VLAN natif (attention piège)

Sur un trunk, il existe un **VLAN natif** : c'est le seul VLAN dont le trafic n'est **PAS tagué**. Par défaut, c'est le VLAN 1.

Bonne pratique sécurité : changer le VLAN natif (ex : VLAN 99) pour éviter les attaques de type "VLAN hopping".

3. Méthode de dépannage VLAN — Checklist systématique

Quand un ping ne fonctionne pas entre deux machines censées être dans le même VLAN, suis cette checklist dans l'ordre :

Checklist de diagnostic VLAN

Étape	Vérification	Commande	Ce qu'on cherche
1	L'IP est-elle correcte ?	Vérifier sur le PC	Bonne IP, bon masque, même sous-réseau
2	Le VLAN existe-t-il ?	show vlan brief	Le VLAN est listé avec le bon nom
3	Le port est-il dans le bon VLAN ?	show vlan brief	Le port apparaît sous le bon VLAN
4	Le port est-il en mode access ?	show interfaces gi1/0/X switchport	Mode = access
5	Le lien est-il UP ?	show interfaces status	Status = connected
6	Le trunk est-il configuré ?	show interfaces trunk	Le port trunk apparaît
7	Le VLAN est-il autorisé sur le trunk ?	show interfaces trunk	Le VLAN est dans "allowed"
8	Le VLAN existe-t-il sur les 2 switchs ?	show vlan brief sur chaque switch	Même VLAN ID des 2 côtés

Les 5 erreurs les plus fréquentes

#	Erreur	Symptôme	Correction
1	Port pas en mode access	Le port reste en VLAN 1 malgré switchport access vlan 10	Ajouter switchport mode access
2	Trunk pas configuré des 2 côtés	Ping inter-switch échoue pour tous les VLANs	Configurer le trunk sur les 2 switchs
3	VLAN pas créé sur le 2e switch	Ping inter-switch échoue pour un VLAN spécifique	Créer le VLAN sur le 2e switch
4	VLAN pas dans allowed vlan du trunk	Le trafic de ce VLAN ne traverse pas le trunk	switchport trunk allowed vlan add XX
5	Mauvaise IP ou masque sur le PC	Ping échoue même en intra-VLAN local	Vérifier la config IP du PC

4. Vocabulaire complémentaire

Terme	Définition
ARP confiné	Le broadcast ARP ne sort pas du VLAN → isolation naturelle
Tag 802.1Q	4 octets ajoutés à la trame sur un trunk, contenant le VLAN ID
VID	VLAN Identifier — le numéro du VLAN dans le tag (12 bits → 0 à 4095)
VLAN natif	VLAN non tagué sur le trunk (par défaut VLAN 1)
VLAN hopping	Attaque exploitant le VLAN natif pour accéder à un autre VLAN
DTP	Dynamic Trunking Protocol — négocie automatiquement le mode trunk (à désactiver en prod)

Cours 2 — Séquence 07 VLAN — BAC PRO CIEL 1CIEL