

EXERCICE 2 - VLANs et Analyse de Trafic (Explications Simples)

EXERCICE 2 : Configuration et Analyse VLAN

ÉNONCÉ :

L'administrateur dispose d'un portable avec analyseur de trames. Il capture les trames ARP lors d'un ping de 192.168.1.1 vers 192.168.3.1.

C'EST QUOI UN VLAN ? (Concept Simple)

Analogie : Immeuble de Bureaux

Imaginez un **immeuble de bureaux** avec plusieurs entreprises :

- **VLAN 1** = Entreprise A (Étage 1)
- **VLAN 2** = Entreprise B (Étage 2)
- **VLAN 3** = Entreprise C (Étage 3)

Règle : Les employés d'une entreprise ne peuvent **pas** parler directement aux employés d'une autre entreprise !

VLAN = Segmentation Virtuelle

- **Physiquement :** Tous sur le même commutateur (même immeuble)
 - **Logiquement :** Séparés en groupes (différentes entreprises)
 - **Isolation :** Chaque VLAN = réseau indépendant
-

ANALYSE DE LA CONFIGURATION

Configuration VLAN Donnée :

VLAN	Ports Assignés
VLAN 1	C1e1, C1e2, C1e3, C1f1
VLAN 2	C1e4, C2f1, C2e1, C2e2, C2e3
VLAN 3	C2e4, C2f2, C3e2, C3e3, C3e1, C3f1

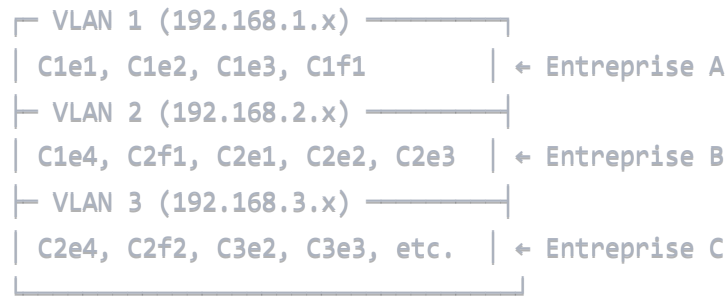
Décodage Simple :

- **C1e1** = Commutateur 1, port Ethernet 1
- **C2f1** = Commutateur 2, port FastEthernet 1


- etc.

Répartition par "Étages" :

IMMEUBLE RÉSEAU :



QUESTION 1 : Analyse ARP

 ÉNONCÉ : Ping 192.168.1.1 → 192.168.3.1

 PREMIÈRE ANALYSE : Qui Est Où ?

- 192.168.1.1 → Dans **VLAN 1** (Entreprise A)
- 192.168.3.1 → Dans **VLAN 3** (Entreprise C)

PROBLÈME DÉTECTÉ !

Entreprise A essaie de parler à **Entreprise C** directement ! **C'est INTERDIT** par les VLANs ! 

 Que se passe-t-il vraiment ?

Étape 1 : ARP Request

192.168.1.1 (VLAN 1) dit :
"Qui a l'adresse 192.168.3.1 ? Donnez-moi votre MAC !"

Action : Envoi ARP Request en BROADCAST dans VLAN 1
Portée : SEULEMENT les ports de VLAN 1 !

Étape 2 : Pas de Réponse

Machines dans VLAN 1 : "On ne connaît pas 192.168.3.1"
Résultat : AUCUNE ARP Reply !

Réponse à la Question :

Combien de trames ARP ?

- **ARP Request** : 1 trame (broadcast dans VLAN 1)

- **ARP Reply** : 0 trame (pas de réponse !)
- **TOTAL** : 1 seule trame ARP

Entités MAC :

- **ARP Request** :
 - MAC source : 192.168.1.1
 - MAC destination : FF:FF:FF:FF:FF:FF (broadcast)
 - **ARP Reply** : Aucune (pas de réponse)
-

QUESTION 2 : Paramètres VLAN

 **ÉNONCÉ** : Quels paramètres pour qu'une station participe à un VLAN ?

 **Configuration d'un Port pour VLAN :**

1. VLAN ID (Numéro d'Entreprise)

```
cisco
switchport access vlan 2
```

Explication : "Ce port appartient à l'entreprise numéro 2"

2. Mode du Port

```
cisco
switchport mode access
```

Explication : "Ce port est pour UN SEUL VLAN" (pas un lien entre commutateurs)

3. (Optionnel) Pour Liens Inter-Commutateurs :

```
cisco
switchport mode trunk
switchport trunk allowed vlan 1,2,3
```

Explication : "Ce câble transporte PLUSIEURS VLANs entre bâtiments"

 **Configuration Complète Type :**

cisco

```
interface FastEthernet 0/1
switchport mode access
switchport access vlan 2
spanning-tree portfast
```

✅ QUESTION 3 : VLAN vs Segmentation IP

😞 QUESTION : Cette technique = simple segmentation en sous-réseaux ?

🚫 RÉPONSE : NON ! Voici pourquoi :

🏠 VLAN (Niveau 2 - Physique) :

- Isolation **PHYSIQUE** des trames Ethernet
- Même avec même IP, pas de communication entre VLANs
- Séparation au niveau commutateur
- Exemple : Même si 192.168.1.5 et 192.168.1.6 sont dans des VLANs différents → **AUCUNE communication !**

🌐 Segmentation IP (Niveau 3 - Logique) :

- Isolation **LOGIQUE** des paquets IP
- Communication **possible** via routeur
- Séparation au niveau réseau
- Exemple : 192.168.1.5 et 192.168.2.5 → **Communication via routeur**

📊 Comparaison :

Critère	VLAN	Segmentation IP
Niveau	2 (Liaison)	3 (Réseau)
Isolation	Physique	Logique
Bypass	Impossible sans routeur	Possible avec routage
Granularité	Par port	Par adresse
Performance	Plus rapide	Plus flexible

✅ QUESTION 4 : Échec du Ping - Diagnostic

🎯 ÉNONCÉ : Ping 192.168.1.1 → 192.168.3.1 = "délai d'attente dépassé"

🔍 ANALYSE DE LA PANNE :

Étape 1 : Tentative ARP

```
192.168.1.1 : "Qui a 192.168.3.1 ?"  
VLAN 1 : Broadcast seulement dans VLAN 1  
192.168.3.1 : N'entend PAS la question (dans VLAN 3)
```

Étape 2 : Timeout ARP

```
192.168.1.1 : "Personne ne répond..."  
Résultat : Table ARP incomplète  
État : Impossible de créer la trame Ethernet
```

Étape 3 : Échec Ping

```
Ping : Impossible de commencer  
Raison : Pas d'adresse MAC destination  
Message : "Délai d'attente dépassé"
```

CAUSE RACINE :

Isolation VLAN - Les deux machines sont dans des "entreprises" différentes !

SOLUTIONS POSSIBLES :

Solution 1 : Routeur Inter-VLAN

```
Ajouter un routeur/switch L3 :  
VLAN 1 ↔ ROUTEUR ↔ VLAN 3  
  
Configuration :  
interface vlan 1  
  ip address 192.168.1.254 255.255.255.0  
interface vlan 3  
  ip address 192.168.3.254 255.255.255.0  
ip routing
```

Solution 2 : Déplacer dans le Même VLAN

```
Changer la configuration :  
192.168.3.1 → affecter au VLAN 1  
  
switchport access vlan 1
```

Solution 3 : Switch L3

Activer le routage sur le switch :

```
ip routing
```

```
interface vlan 1
```

```
ip address 192.168.1.1 255.255.255.0
```

```
interface vlan 3
```

```
ip address 192.168.3.1 255.255.255.0
```

CONCEPTS CLÉS À RETENIR

VLANs en Simple :

- **VLAN** = Créer plusieurs réseaux sur un seul commutateur
- **Isolation totale** entre VLANs (comme des entreprises séparées)
- **Communication inter-VLAN** = obligatoirement via routeur
- **Configuration** = Assigner chaque port à un VLAN

Erreurs Fréquentes :

- Croire que **même sous-réseau IP** = communication directe → **FAUX avec VLANs !**
- Confondre **VLAN** et **sous-réseau IP** → Ce sont **2 niveaux différents !**
- Oublier qu'il faut un **routeur** pour communiquer entre VLANs

Utilité des VLANs :

- **Sécurité** : Isolation des départements
- **Performance** : Réduire les domaines de broadcast
- **Flexibilité** : Changer l'affectation sans rewiring
- **Administration** : Groupes logiques vs physiques

Debug VLAN - Questions Types :

1. **Dans quel VLAN** est chaque machine ?
2. **Y a-t-il un routeur** entre les VLANs ?
3. **La configuration des ports** est-elle correcte ?
4. **Les VLANs** sont-ils bien propagés (trunk) ?

Ces concepts VLAN sont-ils plus clairs maintenant ? Prêt pour l'EXERCICE 3 (SNMP) ? 