

## Fiche de procédure - Projet 1

Mise en place d'une infrastructure réseau sur Cisco Packet Tracer

Simulation d'une création d'infrastructure réseau pour un client dans de nouveaux locaux

### Table des matières

I. Présentation du projet.....	1
II. Environnement utilisé.....	2
1. Connexions physiques .....	2
2. Création des VLANs .....	3
3. Configuration du trunk sur les liens inter-switchs et routeur.....	3
4. Attribution des ports utilisateurs.....	4
5. Mise en place du Spanning Tree Protocol (STP) .....	4
6. Configuration du routeur pour le routage inter-VLAN .....	5
7. Configuration du serveur DHCP.....	6
8. Mise en place du NAS.....	6
9. Tests de connectivité .....	6

### I. Présentation du projet

Dans ce projet, nous allons construire une infrastructure réseau professionnelle sous **Cisco Packet Tracer**.

Les objectifs principaux sont :

- Créer 3 VLANs séparés (User, Admin et Guest),
- Mettre en place un routage inter-VLAN pour assurer la communication entre les réseaux,
- Utiliser Spanning Tree Protocol pour éviter les boucles réseau,
- Déployer des services réseau comme DHCP pour l'attribution IP automatique et NAS pour le stockage de fichiers,
- Assurer un accès filaire pour les utilisateurs internes, et un accès Wi-Fi sécurisé pour les invités.

## II. Environnement utilisé

Pour mener à bien ce projet, nous allons utiliser :

- **Cisco Packet Tracer,**
- **1 Routeur Cisco 2901 (R1),**
- **6 Switchs Cisco 2960 (SW1 à SW6),**
- **1 Serveur DHCP,**
- **1 NAS (FTP Server),**
- **Des postes clients** (PC fixes et laptops).

## III. Création de l'infrastructure

### 1. Connexions physiques

On commence par réaliser les branchements suivants :

R1 Gig9/0 → SW1 Fa0/1

SW1 Gig0/1 ↔ SW2 Gig0/2

SW2 Gig0/1 ↔ SW3 Gig0/2

SW3 Gig0/1 ↔ SW1 Gig0/2

Serveur DHCP (Gig0) → SW1 Fa0/3

NAS (Gig0) → SW1 Fa0/4

SW1 Fa0/2 → SW4 Fa0/1

SW2 Fa0/2 → SW5 Fa0/1

SW3 Fa0/1 → SW6 Fa0/1

## 2. Création des VLANs

Nous allons maintenant créer les VLANs nécessaires.

Sur **n'importe quel switch** de cœur (par exemple SW1) :

```
enable
configure terminal
vlan 10
name User
vlan 20
name Admin
vlan 30
name Guest
exit
```

Cette configuration est à réaliser sur un switch de cœur de réseau (par exemple SW1).

**Note :** Les VLANs seront propagés automatiquement aux autres switchs via les trunks.

## 3. Configuration du trunk sur les liens inter-switchs et routeur

Sur **SW1, SW2 et SW3**, configurez les ports reliés aux autres switchs et au routeur en mode **trunk** :

```
enable
configure terminal
interface range gig0/1, gig0/2, fa0/1
switchport mode trunk
exit
```

### Explication :

Le mode trunk permet de transporter plusieurs VLANs en même temps sur un seul lien réseau.

## 4. Attribution des ports utilisateurs

Maintenant, nous allons affecter les VLANs aux ports d'accès pour les utilisateurs.

- Les ports où sont branchés les PCs utilisateurs (Open Space 1 et 2) → VLAN 10 (User)
- Les ports où sont branchés les serveurs (DHCP et NAS) → VLAN 20 (Admin)
- Les ports des laptops en salle de réunion → VLAN 30 (Guest)

Exemple configuration sur SW1 :

- Pour les serveurs :

```
interface fa0/3
switchport mode access
switchport access vlan 20
exit

interface fa0/4
switchport mode access
switchport access vlan 20
exit
```

- Pour les PC utilisateurs :

```
interface fa0/5
switchport mode access
switchport access vlan 10
exit
```

## 5. Mise en place du Spanning Tree Protocol (STP)

Pour éviter les boucles réseau, nous allons activer STP et définir **SW1** comme racine.

Sur **SW1** :

```
enable
configure terminal
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 4096
exit
```

## 6. Configuration du routeur pour le routage inter-VLAN

Nous allons maintenant configurer les sous-interfaces sur le routeur pour permettre la communication entre les VLANs.

Sur **R1** :

```
enable
configure terminal

interface gig9/0.10
encapsulation dot1Q 10
ip address 10.10.10.1 255.255.255.0
ip helper-address 10.10.20.250
ip access-group 100 out
exit

interface gig9/0.20
encapsulation dot1Q 20
ip address 10.10.20.1 255.255.255.0
ip access-group 110 out
exit

interface gig9/0.30
encapsulation dot1Q 30
ip address 10.10.30.1 255.255.255.0
ip helper-address 10.10.20.250
ip access-group 120 out
exit
```

Cette configuration permet d'assurer la communication entre les VLANs tout en bloquant la communication croisée (ACLs) et en relayant les demandes DHCP.

## 7. Configuration du serveur DHCP

Le serveur DHCP est dans **VLAN 20** et a pour IP **10.10.20.250**.

Sur le **serveur DHCP**, il faut créer 3 pools pour distribuer les IP automatiquement :

- **VLAN 10 (User) :**
  - Plage IP : 10.10.10.100 - 10.10.10.200
  - Gateway : 10.10.10.1
- **VLAN 20 (Admin) :**
  - Plage IP : 10.10.20.100 - 10.10.20.200
  - Gateway : 10.10.20.1
- **VLAN 30 (Guest) :**
  - Plage IP : 10.10.30.100 - 10.10.30.200
  - Gateway : 10.10.30.1

## 8. Mise en place du NAS

Le serveur NAS est aussi dans **VLAN 20** avec l'IP **10.10.20.200**.

Sur le serveur NAS, il faut activer le service FTP

### Vérification :

Ouvrez un navigateur ou un client FTP et tapez **ftp://10.10.20.200** pour vérifier l'accès.

## 9. Tests de connectivité

À la fin du projet, effectuez les vérifications suivantes :

- Tester qu'un PC utilisateur VLAN 10 récupère une IP via DHCP.
- Tester qu'un laptop VLAN 30 récupère une IP via DHCP.
- Tester que les VLANs sont bien isolés (ping entre VLAN impossible sauf si autorisé).
- Tester que le NAS est accessible pour les machines en VLAN 20.

## IV. Conclusion

L'infrastructure réseau est maintenant totalement fonctionnelle :

- **3 VLANs** isolés,
- **Routage inter-VLAN** actif,
- **Service DHCP** opérationnel,
- **NAS** disponible pour le partage de fichiers,
- **Spanning Tree** en place pour garantir la stabilité du réseau.

Ce projet respecte les standards attendus pour une PME, et il est évolutif pour accueillir de nouveaux services ou utilisateurs.