Fiche technique — Projet Réseau Universitaire

Simulation **Cisco Packet Tracer** : conception, segmentation, services et sécurité

Auteur : Hail Amine | **Formation :** Master / Automatique Robotique

1. Contexte et objectifs

Projet de niveau Master visant à **concevoir, simuler et analyser** un réseau universitaire structuré et sécurisé sous Cisco Packet Tracer. L'architecture s'inspire d'un scénario réaliste d'interconnexion à l'échelle nationale et se concentre ici sur une faculté pilote composée de **cinq départements**.

Objectifs techniques :

— Plan d'adressage IP optimisé via **VLSM** (réseau privé **172.16.0.0/16**)

— Topologie hiérarchisée et **interconnexion** via un routeur central

— Mise en place de services essentiels : **DHCP**

— Sécurisation de base : **ACL** (standards/étendues) pour limiter l'inter-département

— Analyse des performances et perspectives d'évolution

2. Architecture réseau

Topologie : étoile autour d'un **routeur central**. Chaque département est relié via une interface Ethernet dédiée (segmentation des domaines de broadcast).

Composants :

— 1 routeur central (Cisco 2800 ou équivalent)

— 5 commutateurs d'accès (1 par département)

— Postes clients par département (PCs)

Évolutivité : conception prévue pour évoluer vers une architecture multi-facultés.

3. Plan logique (VLAN / Sous-réseaux)

Chaque département dispose de son propre **sous-réseau** afin d'assurer la segmentation des broadcasts.

Départements :

— D1 : Nom Département 1

— D2 : Nom Département 2

— D3 : Nom Département 3

— D4 : Nom Département 4

— D5 : Nom Département 5

4. Plan d'adressage IP (VLSM)

Réseau de base : 172.16.0.0/16 (privé classe B).
Méthode : VLSM pour adapter la taille des sous-réseaux aux besoins et optimiser l'allocation.

Dépt. Plage utilisable	Besoin (hôtes)	Réseau/Prefix	Masque	Passerelle	Broadcast
D1 **172.16.x.2 – 172.16.x.u**	xx	172.16.x.0/yy	255.255.x.x	172.16.x.1	172.16.x.b
D2 **172.16.x.2 – 172.16.x.u**	xx	172.16.x.0/yy	255.255.x.x	172.16.x.1	172.16.x.b
D3 **172.16.x.2 – 172.16.x.u**	xx	172.16.x.0/yy	255.255.x.x	172.16.x.1	172.16.x.b
D4 **172.16.x.2 – 172.16.x.u**	xx	172.16.x.0/yy	255.255.x.x	172.16.x.1	172.16.x.b
D5 **172.16.x.2 – 172.16.x.u**	xx	172.16.x.0/yy	255.255.x.x	172.16.x.1	172.16.x.b

Table 1 – Table d'adressage IP (VLSM) — à compléter

5. Services réseau (DHCP)

Service : DHCP pour l'attribution automatique des paramètres IP aux postes clients.
Bonnes pratiques :

— Exclusion des adresses réservées (passerelles, serveurs, équipements)
— 1 pool DHCP par sous-réseau / département
— Distribution : adresse IP, masque, passerelle par défaut, DNS (si simulé)

Exemple (Cisco IOS) — DHCP (à adapter)

Exemple :

```
ip dhcp excluded-address 172.16.X.1 172.16.X.20
ip dhcp pool DEP_D1
 network 172.16.X.0 255.255.255.0
 default-router 172.16.X.1
 dns-server 8.8.8.8
```

6. Sécurité (ACL)

Des **ACL standards et/ou étendues** sont utilisées pour limiter les communications inter-départements non autorisées et renforcer la sécurité.

Politique type (exemple) :

— Autoriser l'accès au routeur/gateway depuis chaque département

— Bloquer le trafic entre départements (sauf exceptions définies)

— Autoriser la sortie vers services communs (si présents : DNS/DHCP/serveur)

Exemple (Cisco IOS) — ACL (à adapter)

```
ip access-list extended ACL_D1_OUT
 deny ip 172.16.D1.0 0.0.0.255 172.16.D2.0 0.0.0.255
 deny ip 172.16.D1.0 0.0.0.255 172.16.D3.0 0.0.0.255
 permit ip 172.16.D1.0 0.0.0.255 any
!
interface g0/0
 ip access-group ACL_D1_OUT in
```

7. Outils et environnement

— **Outil :** Cisco Packet Tracer

— **Équipements :** routeur Cisco série 2800 (ou équivalent), commutateurs Ethernet, PCs

— **Livrables :** fichier `.pkt`, table d'adressage, configurations routeur/PC, rapport technique

8. Tests et validation (checklist)

— Ping intra-département (même sous-réseau) : **OK / KO**

— Routage inter-département (si autorisé) : **OK / KO**

— Attribution DHCP (IP/masque/gateway/DNS) : **OK / KO**

— Filtrage ACL (trafic bloqué/autorisé selon politique) : **OK / KO**

— Analyse : latence, goulots d'étranglement, limites de l'architecture : **résumé**

9. Perspectives d'évolution

— Passage à une architecture multi-facultés (routage multi-sites)

— Ajout de VLANs + trunking (802.1Q) si besoin de segmentation plus fine

— Services supplémentaires : DNS interne, serveur web, supervision (SNMP), syslog

— Renforcement sécurité : VLAN management, port-security, NAT/PAT, VPN, firewall