**TP 4-2 : Access lists**

**Listes de contrôle d’accès étendues**

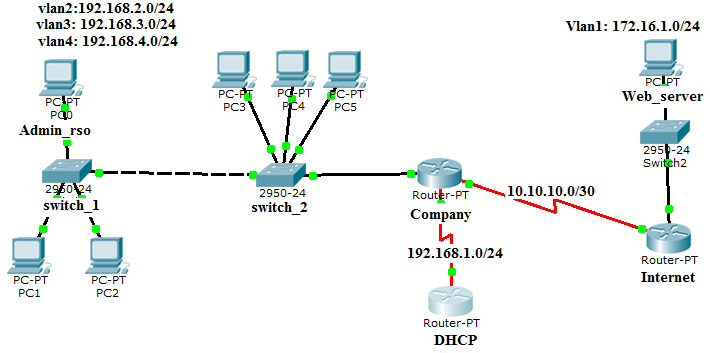
**Pré requis** : Travaux pratiques 5.5.1 : listes de contrôle d’accès de base **et**

Exercice PT 5.3.4 : configuration de listes de contrôle d’accès étendues

**Nombre de séances** : 2

**But du TP** : Manipulation des ACL : Les listes de contrôle d’accès étendues

**Soit la topologie suivante :**



VLAN2 : PC2 et PC4

VLAN3 : PC1, PC3 et PC5

VLAN4 : Administrateur réseau (Admin\_rso : 192.168.4.1 / 24 (adresse statique))

**Tâche 1 : Création des différents vlan du réseau**

Vérifiez la connectivité intra-vlan et inter-vlan.

**Tâche 2 : Configuration du** **routage RIP et d’une route par défaut sur le routeur *Company***

Vérifiez la connectivité du réseau.

**Tâche 3 : Configurez le routeur DHCP comme serveur DHCP**

Vérifiez le fonctionnement du serveur DHCP. Vous devez au préalable effacer les adresses des différents PCs (PC1-PC5).

**Tâche 4 : Configurez ip-helper address sur le routeur *Company***

Toutes les machines doivent recevoir une adresse IP valide et être capable de joindre le serveur web distant. Des *ping* suffisent à le vérifier.

**Tâche 5: Configuration d’ACLs**

Nous allons appliquer des ACL qui limiteront le trafic de la façon suivante :

* Nous n’autoriseront que le trafic DHCP entre les machines utilisateurs (vlan2 et vlan3) et le serveur DHCP.
* Nous n’autoriseront l’administration du serveur DHCP que par la machine du service informatique (Admin\_rso).
* Nous n’autoriseront que les machines utilisateur à communiquer vers Internet.

### Application des ACL

**1 – Première règle**

Les machines ***users*** (vlan2) ne doivent être capables de joindre le serveur DHCP **que** pour récupérer leurs adresses IP.

**Company(config)#ip access-list extended lan2  
Company(config-ext-nacl)#permit udp any host 192.168.1.2 range bootps bootpc**

J’applique cette règle, en entrée de l’interface fa0/0.2 au plus près de la source du flux, en entrée de l’interface (**in)** avec la commande :

**Company(config)#int fa0/0.2  
Company(config-if)#ip access-group lan2 out**

**2 – Deuxième règle**

Seule la machine d’administration est autorisée à administrer le serveur DHCP.

**Company(config)#ip access-list extended admin-dhcp  
Company(config-ext-nacl)#permit ip host 192.168.4.1 host 192.168.1.2  
Company(config-ext-nacl)#deny ip any any**

**Company(config-subif)#int se2/0  
Company(config-if)# ip access-group admin-dhcp out**

**3 – Troisième règle**

Les utilisateurs du LAN ne peuvent pas être *pingés* de l’extérieur.

**Company(config)#ip access-list ext icmp-extern  
Company(config-ext-nacl)#deny icmp any any**

**Company(config)#int s0/0/0  
Company(config-if)#ip access-group icmp-extern in**

**4- Quatrième règle**

Refuser la connexion Telnet pour les utilisateurs du réseau vlan3.

**Company(config)#Access-list 101 deny tcp 192.168.3.0 0.0.0.255 any eq 23**

**Company(config)#Access-list 101 permit ip any any**

**Company(config)#int fa0/0.3**

**Company(config-** **-subif)#ip access-group 101 in**