

## **Filtrage avec ACL**

### **Introduction**

Dans ce TP, l'objectif était de configurer des ACLs (Access Control Lists) sur des équipements réseau pour contrôler l'accès à certaines ressources et services.

### **Objectifs**

1. Créer et appliquer des ACLs sur un switch CISCO.
2. Tester les règles de filtrage et contrôler l'accès.

### **Étapes réalisées**

#### **1. Création d'une ACL sur un switch CISCO :**

- Pour créer une ACL standard, utilisez la commande suivante :

```
Switch(config)# access-list 10 deny host 192.168.1.10
```

```
Switch(config)# access-list 10 permit any
```

- Appliquez cette ACL sur une interface :

```
Switch(config)# interface fa0/1
```

```
Switch(config-if)# ip access-group 10 in
```

#### **2. Test des ACLs :**

- Testez l'application de l'ACL en tentant d'accéder à un hôte restreint et en vérifiant si l'accès est bloqué.

### **Résultats obtenus**

Les ACLs ont été correctement appliquées et ont permis de restreindre l'accès aux hôtes selon les règles définies.

### **Conclusion**

Ce TP m'a permis de comprendre comment configurer des ACLs sur des équipements réseau pour restreindre l'accès à certaines ressources en fonction des adresses IP ou des types de trafic.