École Nationale des Sciences Appliquées de Fès

ENSA FES

Compte Rendu

Travaux Pratiques

Configuration des Services Réseau
Mail (SMTP/POP3) et DNS

Réalisé par : Yassine ELBOUKILI

Encadré par : Prof. Hakim EL FADILI

14 novembre 2025

Table des matières

1 Introduction **2**

2 Objectifs du TP **2**

3 Architecture Réseau **2**
3.1 Topologie 2

4 Configuration des Clients Mail **2**
4.1 Configuration du PC10 2
4.2 Configuration du PC11 3

5 Configuration du Serveur Mail **4**
5.1 Activation des Services 4
5.2 Configuration du Domaine et des Utilisateurs 4

6 Configuration du Serveur DNS **5**

7 Configuration du Routeur **5**
7.1 Configuration des ACL 5
7.2 Vérification de la Configuration 5

8 Tests et Résultats **5**
8.1 Test de Réception sur PC11 5
8.2 Test de Blocage de Réception sur PC10 6

9 Analyse et Observations **6**
9.1 Explication de la Politique de Sécurité 6
9.2 Importance des Compteurs de "Matchs" 7

10 Conclusion **7**

Table des figures

1 Topologie du réseau 3
2 Configuration mail du PC10 3
3 Configuration mail du PC11 4
4 Configuration du serveur mail avec les utilisateurs 4
5 Réception réussie du mail sur PC11 6
6 Blocage de la réception mail sur PC10 par l'ACL 7

1 Introduction

Ce rapport présente la mise en œuvre d'un travail pratique portant sur la configuration des services réseau essentiels, notamment les services de messagerie électronique (SMTP et POP3) ainsi que le service DNS. L'objectif principal est de configurer un environnement réseau complet permettant l'échange de courriers électroniques entre différents clients via un serveur mail centralisé, tout en assurant la résolution de noms grâce au service DNS.

2 Objectifs du TP

Les objectifs de ce travail pratique sont les suivants :
- Configuration des clients PC avec leurs comptes mail respectifs
- Mise en place d'un serveur mail avec les services SMTP et POP3
- Configuration du service DNS pour la résolution de noms
- Test de l'envoi et de la réception de courriers électroniques
- Mise en place de listes de contrôle d'accès (ACL) sur le routeur pour sécuriser les communications

3 Architecture Réseau

3.1 Topologie

L'architecture réseau déployée comprend les éléments suivants :
- **PC10 (PC-P Fa0)** : Adresse IP 192.168.0.10
- **PC11 (PC-PT)** : Adresse IP 192.168.0.11
- **Switch-PT Switch2** : Commutateur reliant PC10 et Router0
- **Switch-PT Switch3** : Commutateur reliant PC11, Server MAIL et Server DNS
- **Router0** : Routeur central avec interfaces :
  - Fa0/0 : Connexion vers le réseau des clients (192.168.0.0/24)
  - Fa0/1 : Connexion vers le réseau des serveurs (192.168.1.0/24)
- **Server-PT Server MAIL** : Serveur mail avec adresse IP 192.168.1.2
- **Server-PT Server DNS** : Serveur DNS avec adresse IP 192.168.1.3

4 Configuration des Clients Mail

4.1 Configuration du PC10

Sur le PC10, la configuration du client mail a été effectuée avec les paramètres suivants :
- **Your Name :** user1
- **Email Address :** user1@ensaf.ac.ma
- **Incoming Mail Server :** ensaf.ac.ma
- **Outgoing Mail Server :** ensaf.ac.ma
- **User Name :** user1
- **Password :** (configuré)

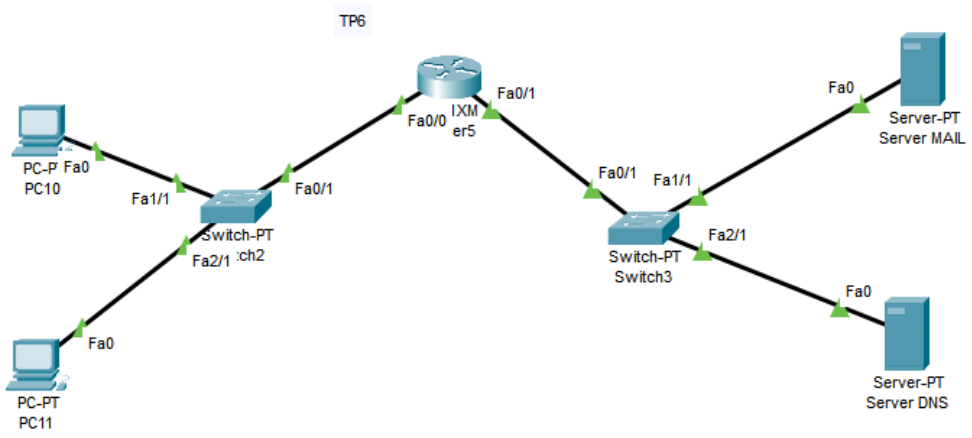

FIGURE 1 – Topologie du réseau

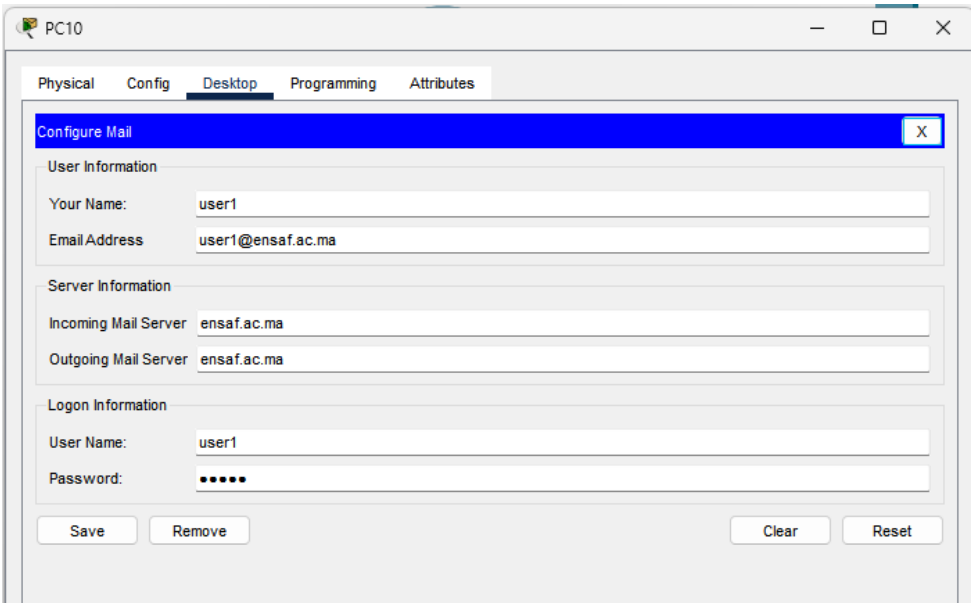

FIGURE 2 – Configuration mail du PC10

4.2 Configuration du PC11

Sur le PC11, la configuration du client mail a été réalisée avec les paramètres suivants :

- **Your Name :** user2
- **Email Address :** user2@ensaf.ac.ma
- **Incoming Mail Server :** ensaf.ac.ma
- **Outgoing Mail Server :** ensaf.ac.ma
- **User Name :** user2
- **Password :** (configuré)

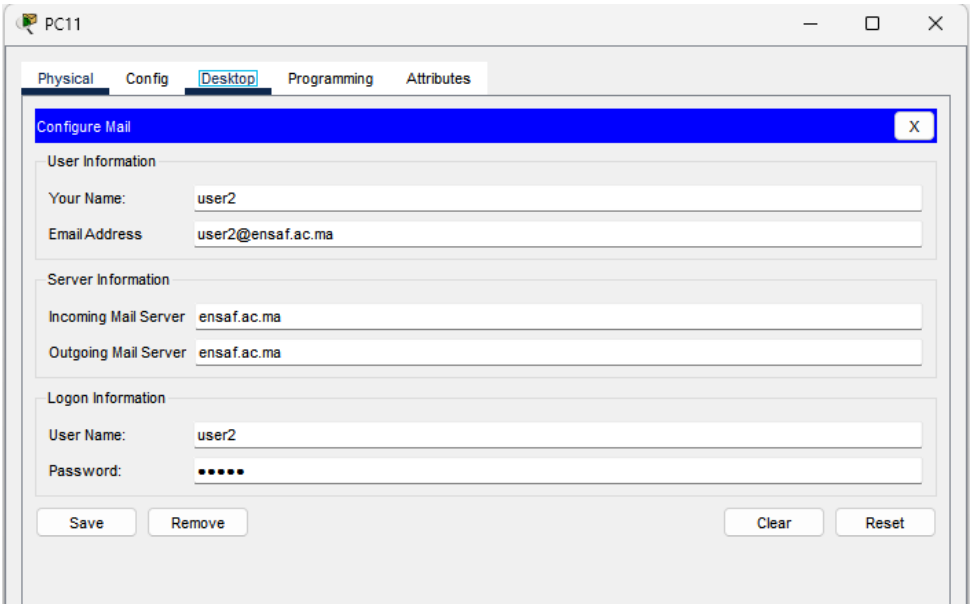

FIGURE 3 – Configuration mail du PC11

5 Configuration du Serveur Mail

5.1 Activation des Services

Sur le serveur mail (Server MAIL), les services suivants ont été activés :

— **SMTP Service :** ON
— **POP3 Service :** ON

5.2 Configuration du Domaine et des Utilisateurs

Le nom de domaine a été configuré en tant que `ensaf.ac.ma`, et deux comptes utilisateurs (‘user1‘ et ‘user2‘) ont été créés sur le serveur.

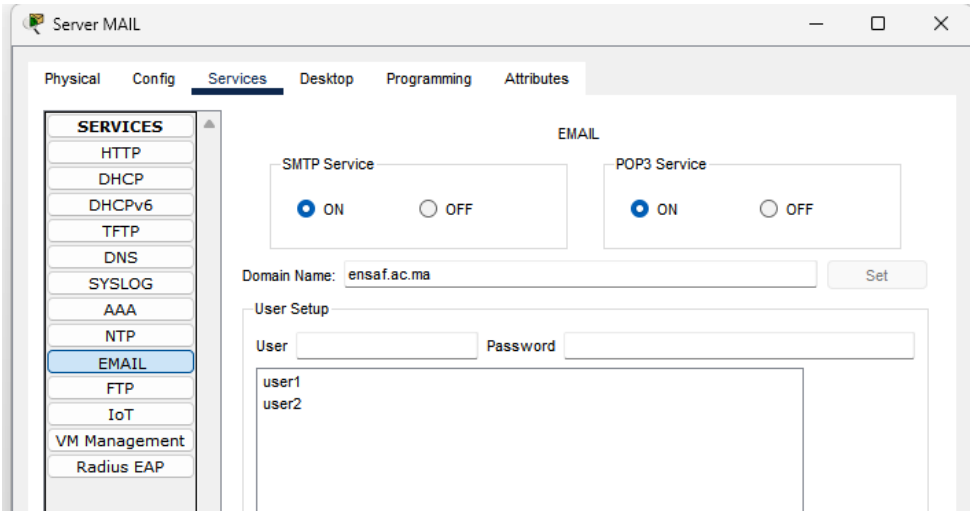

FIGURE 4 – Configuration du serveur mail avec les utilisateurs

6 Configuration du Serveur DNS

Le serveur DNS a été configuré pour résoudre le nom de domaine `ensaf.ac.ma` vers l'adresse IP du serveur mail (192.168.1.2). Cette configuration est cruciale pour que les clients puissent contacter le serveur mail en utilisant son nom.

7 Configuration du Routeur

7.1 Configuration des ACL

Une liste de contrôle d'accès (ACL) étendue et nommée `BLOCK_MAIL` a été configurée sur le routeur pour filtrer le trafic.

Listing 1 – Configuration de l'ACL étendue BLOCK$_MAIL$

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended BLOCK_MAIL
Router(config-ext-nacl)# deny tcp host 192.168.0.11 host
   192.168.1.2 eq 25
Router(config-ext-nacl)# deny tcp host 192.168.0.10 host
   192.168.1.2 eq 110
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# interface Fa0/0
Router(config-if)# ip access-group BLOCK_MAIL in
Router(config-if)# exit
```

7.2 Vérification de la Configuration

La commande `show access-list` permet de vérifier que l'ACL est correctement configurée.

Listing 2 – Vérification de l'ACL avec show access-list

```
Router# show access-list
Extended IP access list BLOCK_MAIL
    10 deny tcp host 192.168.0.11 host 192.168.1.2 eq smtp
    20 deny tcp host 192.168.0.10 host 192.168.1.2 eq pop3
    30 permit ip any any (44 match(es))
```

8 Tests et Résultats

8.1 Test de Réception sur PC11

Un mail envoyé depuis PC10 (‘user1‘) vers PC11 (‘user2‘) a été reçu avec succès. Le log montre que la résolution DNS a fonctionné, suivie d'une connexion POP3 réussie. Ce test démontre que PC11 peut recevoir des mails car l'ACL n'interdit pas le trafic sur le port 110 pour cet hôte.

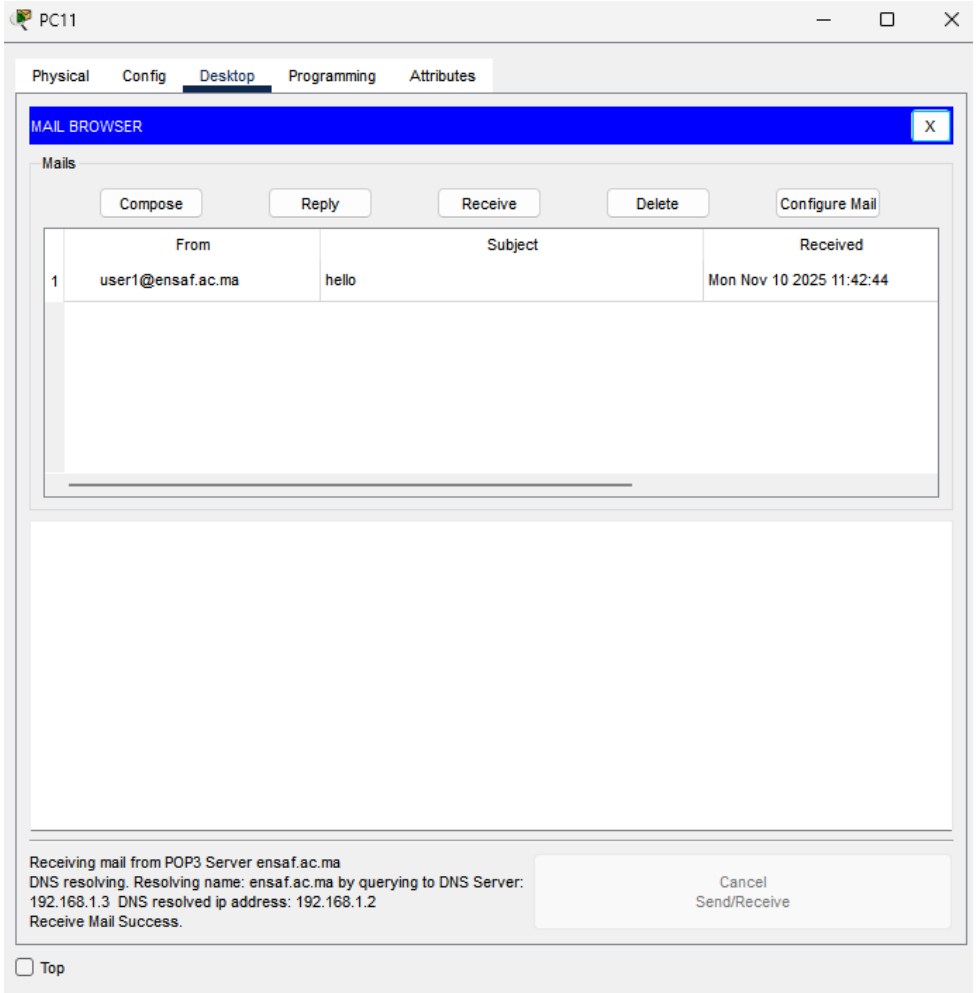

FIGURE 5 – Réception réussie du mail sur PC11

8.2 Test de Blocage de Réception sur PC10

Une tentative de réception de mail sur PC10 a été bloquée. Le log indique que bien que la résolution DNS ait réussi, la connexion au serveur POP3 a échoué avec un "Connection timeout". Ceci confirme l'efficacité de la règle de l'ACL qui bloque le trafic TCP sur le port 110 (POP3) pour l'hôte '192.168.0.10'.

9 Analyse et Observations

9.1 Explication de la Politique de Sécurité

L'ACL `BLOCK_MAIL` implémente une politique de sécurité asymétrique :

— **Règle 1 :** Le trafic de PC11 ('192.168.0.11') vers le serveur mail sur le port 25 (SMTP) est refusé. **Conséquence :** 'user2' ne peut pas envoyer d'e-mails.

— **Règle 2 :** Le trafic de PC10 ('192.168.0.10') vers le serveur mail sur le port 110 (POP3) est refusé. **Conséquence :** 'user1' ne peut pas recevoir d'e-mails.

— **Règle 3 :** Tout autre trafic ('permit ip any any') est autorisé. Cela permet à 'user1' d'envoyer des mails, à 'user2' d'en recevoir, et aux requêtes DNS de fonctionner.

Le positionnement de l'ACL en entrée ('in') sur l'interface 'Fa0/0' est optimal car il

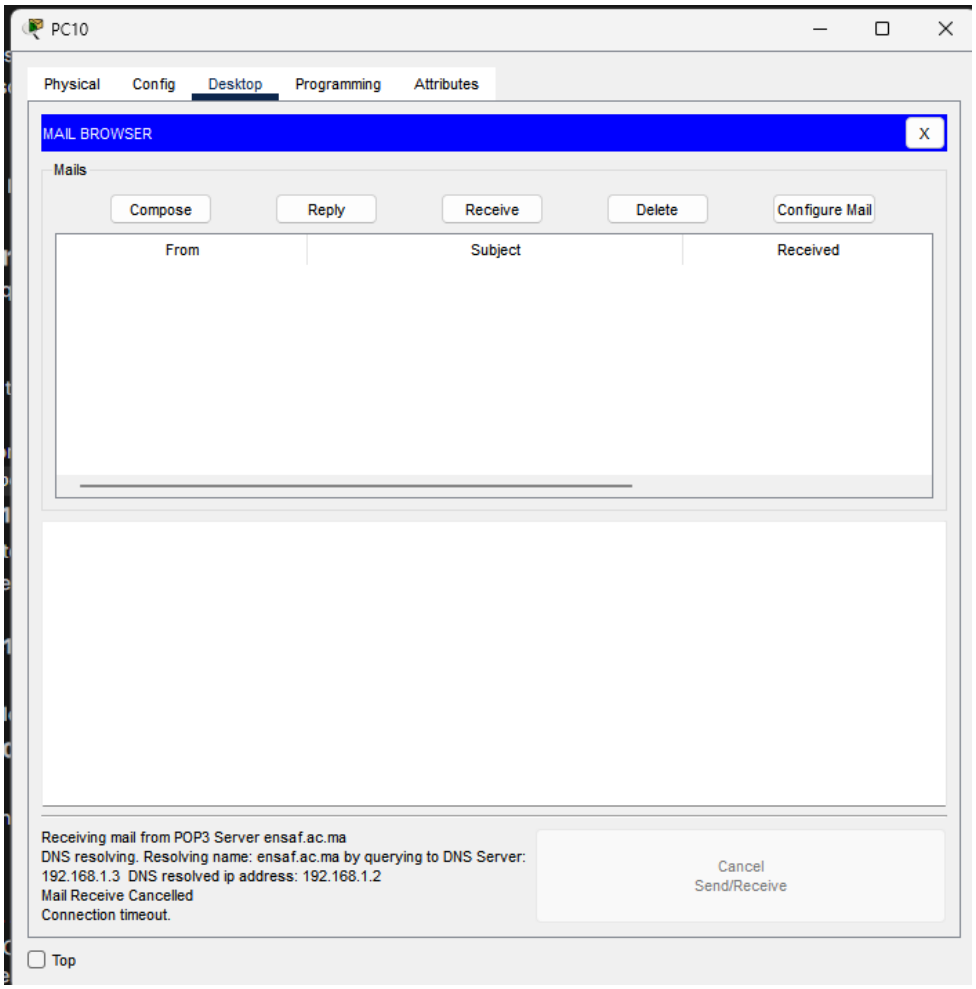

FIGURE 6 – Blocage de la réception mail sur PC10 par l'ACL

filtre le trafic au plus près de la source, empêchant les paquets indésirables de traverser le routeur.

9.2 Importance des Compteurs de "Matchs"

La sortie de la commande `show access-lists` affiche le nombre de paquets qui ont correspondu à chaque règle. Ces compteurs sont essentiels pour :

- **Vérifier l'efficacité :** Confirmer que les règles de blocage sont bien traversées par du trafic.
- **Auditer le trafic :** Quantifier le nombre de tentatives de connexions autorisées et refusées.
- **Dépanner :** Un compteur qui n'augmente pas peut indiquer un problème de placement de l'ACL ou une erreur dans la règle.

10 Conclusion

Ce travail pratique a permis de mettre en œuvre avec succès une infrastructure complète de messagerie électronique, sécurisée par une politique de filtrage granulaire. Les tests ont validé le bon fonctionnement des services DNS et Mail, ainsi que l'efficacité de la liste de

contrôle d'accès pour appliquer des permissions différenciées aux utilisateurs.

Les compétences acquises incluent la configuration de services réseau, la mise en place d'une politique de sécurité précise avec des ACL étendues, et l'analyse des résultats pour vérifier la conformité de l'implémentation par rapport aux objectifs fixés.