COMPTE RENDU – TP DNS

BTS SIO – SISR
Année 2025/2026

1. Introduction

Dans le cadre de ce TP, il nous était demandé de mettre en place l'infrastructure réseau d'une PME fictive, comprenant :

- un serveur DNS local faisant autorité sur notre zone,
- un service DHCP fonctionnel,
- l'hébergement d'une page web locale accessible depuis le WAN,
- un filtrage DNS de domaines non autorisés,
- la configuration complète permettant la résolution interne et externe,
- le respect de la hiérarchie DNS.

L'objectif était d'obtenir un environnement opérationnel correspondant à un LAN d'entreprise.

2. Choix du nom de domaine

J'ai choisi le domaine suivant :

erreur404.ac-monge.fr

Ce nom est délégué par le serveur racine (10.10.0.1) vers mon serveur DNS local dans le LAN.

3. Configuration de l'adressage du LAN

Chaque poste correspond à un LAN de la forme :

172.30.15.0/24

Dans mon cas :

- Adresse du serveur DNS/DHCP : **172.30.15.3**
- Adresse du serveur Web : **172.30.15.3**
- Passerelle : **172.30.15.254**

4. Mise en place du serveur DHCP

Fichier : **/etc/dhcp/dhcpd.conf**

```
option domain-name "erreur404.ac-monge.fr";
option domain-name-servers 172.30.15.3;

default-lease-time 43200;
max-lease-time 86400;
authoritative;

subnet 172.30.15.0 netmask 255.255.255.0 {
  range 172.30.15.100 172.30.15.200;
}
```

Justification :

- Distribution correcte des IP du réseau.
- Fourniture automatique du DNS local comme serveur de résolution.
- Permet au LAN d'être autonome.

5. Hébergement du site Web

Un serveur Nginx a été installé dans le LAN.

Fichier : **/etc/nginx/sites-available/erreur404**

```
server {
   listen 80;

   server_name www.erreur404.ac-monge.fr;

   root /var/www/erreur404;
   index index.html;
```

access_log /var/log/nginx/erreur404_access.log;

error_log /var/log/nginx/erreur404_error.log;

}

Activation :

ln -s /etc/nginx/sites-available/erreur404 /etc/nginx/sites-enabled/

systemctl restart nginx

Justification :

- La page est accessible depuis le WAN car la résolution DNS renvoie l'IP du serveur Web du LAN.
- Le serveur virtuelle répond correctement au nom demandé.

---

6. Mise en place du serveur DNS (BIND9)

6.1. Configuration globale

Fichier : **/etc/bind/named.conf.local**

```
zone "erreur404.ac-monge.fr" {
   type master;
   file "/etc/bind/db.erreur404.ac-monge.fr";
};

zone "15.30.172.in-addr.arpa" {
   type master;
   file "/etc/bind/db.172.30.15";
};

zone "leboncoin.fr" {
   type master;
   file "/etc/bind/db.blocked";
};

zone "amazon.uk" {
   type master;
   file "/etc/bind/db.blocked";
};
```

Justification :

- Le serveur gère bien la zone directe et la zone inverse.
- La zone inverse permet d'effectuer des recherches PTR (reverse lookup).
- Les zones de blocage DNS respectent les consignes.

6.2. Zone directe : db.erreur404.ac-monge.fr

Fichier : **/etc/bind/db.erreur404.ac-monge.fr**

```
$TTL 86400
```

```
@  IN  SOA ns1.erreur404.ac-monge.fr. admin.erreur404.ac-monge.fr. (
      2025100801 ; Serial (à incrémenter à chaque modification)
      3600      ; Refresh
      1800      ; Retry
      1209600    ; Expire
      86400 )    ; Minimum TTL

; Définition du serveur DNS
   IN  NS  ns1.erreur404.ac-monge.fr.

; Serveur DNS
ns1 IN  A   172.30.15.3

; Site web
@  IN  A   172.30.15.3
www IN  A   172.30.15.3
```

Justification :

- Le serveur DNS local est bien désigné comme NS.
- Le site Web pointe vers l'IP interne.
- Fonctionne depuis tous les LAN car la racine délègue vers notre serveur.

6.3. DNS filtrage : blocage de domaines

Dans ce TP, il fallait bloquer :

- leboncoin.fr
- amazon.uk

J'ai ajouté une zone noire.

Fichier : **/etc/bind/named.conf.local**

```
zone "leboncoin.fr" {
```

```
    type master;
    file "/etc/bind/db.blocked";
};

zone "amazon.uk" {
    type master;
    file "/etc/bind/db.blocked";
};
```

Fichier : **/etc/bind/db.blocked**

```
$TTL 86400
@   IN  SOA ns1.erreur404.ac-monge.fr. admin.erreur404.ac-monge.fr. (
        2025100801 ; Serial
        3600       ; Refresh
        1800       ; Retry
        1209600    ; Expire
        86400 )    ; Minimum

    IN  NS  ns1.erreur404.ac-monge.fr.
ns1 IN  A   172.30.15.3

; Bloquer tout le domaine en le renvoyant vers localhost
@   IN  A   127.0.0.1
www IN  A   127.0.0.1
*   IN  A   127.0.0.1
```

Justification :

- Les postes du LAN ne peuvent plus résoudre ces domaines.
- Le blocage est DNS, donc indépendant du navigateur.
- Conforme aux consignes.

6.4. Zone inverse (reverse DNS)

db.172.30.15

Cette partie est indispensable pour que le serveur DNS puisse traduire une adresse IP → un nom de domaine.

Fichier : **/etc/bind/db.172.30.15**

```
$TTL 86400
@  IN  SOA ns1.erreur404.ac-monge.fr. admin.erreur404.ac-monge.fr. (
      2025101001 ; Serial
      3600      ; Refresh
      1800      ; Retry
      1209600   ; Expire
      86400 )   ; Minimum

   IN  NS  ns1.erreur404.ac-monge.fr.
ns1 IN  A   172.30.15.3

3   IN  PTR erreur404.ac-monge.fr.
```

Explications :

- L'IP **172.30.15.3** correspond au serveur DNS → enregistrement PTR ajouté.
- L'IP **172.30.15.3** correspond au serveur Web → enregistrement PTR ajouté.
- Permet la commande dig -x et certaines vérifications de serveurs mail.

Justification :

- Le reverse DNS complète la zone directe.
- Permet une résolution cohérente dans les deux sens.
- Important dans une architecture correcte d'entreprise.

7. Tests et vérifications

7.1. Résolution interne :

dig erreur404.ac-monge.fr @172.30.15.3

8.2. Résolution externe (depuis un autre LAN) :

dig erreur404.ac-monge.fr @10.10.0.1

Cela fonctionne grâce à la délégation.

8.3. Blocage DNS :

dig leboncoin.fr @172.30.15.3

Retour :

0.0.0.0

8.4. Accès Web :

Depuis un autre poste :

http://erreur404.ac-monge.fr

La page s'affiche correctement.

9. Mise en place du serveur mail (Postfix + Dovecot + Roundcube)

9.1. Objectif

L'objectif de cette partie est de mettre en place un **serveur de messagerie complet** permettant :

- l'envoi et la réception de mails internes ;
- la consultation ;
- la gestion sécurisée des connexions SMTP et IMAP ;
- l'utilisation d'un domaine cohérent avec notre DNS local : **erreur404.ac-monge.fr**.

9.2. Architecture du service mail

Service	Logiciel utilisé	Fonction
SMTP	Postfix	Envoi et réception de mails

Service	Logiciel utilisé	Fonction
IMAP	Dovecot	Consultation des mails
Webmail	Roundcube (via Nginx)	Accès graphique depuis un navigateur

9.3. Configuration de Postfix

Fichier principal : /etc/postfix/main.cf

```
# ============================
#      POSTFIX CONFIG
#  erreur404.ac-monge.fr
# ============================

myhostname = mail.erreur404.ac-monge.fr
mydomain = erreur404.ac-monge.fr
myorigin = erreur404.ac-monge.fr

inet_interfaces = all
inet_protocols = ipv4

mydestination = erreur404.ac-monge.fr, mail.erreur404.ac-monge.fr, localhost

mynetworks = 127.0.0.1/32, 172.30.15.0/24, 10.10.0.0/24

home_mailbox = Maildir/

smtpd_banner = $myhostname ESMTP
biff = no

append_dot_mydomain = no
```

```
readme_directory = no

# Sécurité minimale
smtpd_helo_required = yes
disable_vrfy_command = yes

# TLS (désactivé pour le TP)
smtpd_use_tls = no
smtp_use_tls = no

# SPF déjà géré par DNS
smtpd_recipient_restrictions = permit_mynetworks, reject_unauth_destination

# Boîtes mail locales
local_recipient_maps = unix:passwd.byname $alias_maps

alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases

smtpd_sasl_auth_enable = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes

# autoriser l'auth dans le LAN
smtpd_recipient_restrictions =
   permit_mynetworks,
```

permit_sasl_authenticated,

reject_unauth_destination

sender_canonical_maps = hash:/etc/postfix/sender_canonical

Justification :

- Le service écoute sur toutes les interfaces du LAN.
- Les mails sont stockés dans Maildir/ pour la compatibilité avec Dovecot.
- mydestination inclut bien le domaine et le serveur local.

9.4. Configuration de Dovecot

Fichier /etc/dovecot/dovecot.conf

!include_try /usr/share/dovecot/protocols.d/.protocol*

!include conf.d/.conf*

!include_try local.conf

Fichier /etc/dovecot/conf.d/10-mail.conf

mail_location = maildir:~/Maildir

namespace inbox {

inbox = yes

}

mail_privileged_group = mail

Fichier /etc/dovecot/conf.d/10-auth.conf

auth_mechanisms = plain login

!include auth-system.conf.ext

Fichier /etc/dovecot/conf.d/10-master.conf

service imap-login {

inet_listener imap {

#port = 143

```
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }
}

service pop3-login {
  inet_listener pop3 {
    #port = 110
  }
  inet_listener pop3s {
    #port = 995
    #ssl = yes
  }
}

service submission-login {
  inet_listener submission {
    #port = 587
  }
  inet_listener submissions {
    #port = 465
  }
}

service lmtp {
  unix_listener lmtp {
```

```
  #mode = 0666
 }

 # Create inet listener only if you can't use the above UNIX socket
 #inet_listener lmtp {
  # Avoid making LMTP visible for the entire internet
  #address =
  #port =
 #}
}

service imap {
}

service pop3 {
 # Max. number of POP3 processes (connections)
 #process_limit = 1024
}

service submission {
 # Max. number of SMTP Submission processes (connections)
 #process_limit = 1024
}

service auth {
unix_listener /var/spool/postfix/private/auth {
 mode = 0660
 user = postfix
```

```
  group = postfix
}
  # Postfix smtp-auth
  #unix_listener /var/spool/postfix/private/auth {
  #  mode = 0666
  #}

  # Auth process is run as this user.
  #user = $default_internal_user
}

service auth-worker {
  #user = root
}

service dict {
  # If dict proxy is used, mail processes should have access to its socket.
  # For example: mode=0660, group=vmail and global mail_access_groups=vmail
  unix_listener dict {
    #mode = 0600
    #user =
    #group =
  }
}
```

Justification :

- Le protocole IMAP est activé pour permettre la lecture depuis Roundcube.
- L'authentification locale est utilisée (utilisateurs du système).
- Le serveur écoute sur le LAN.

9.5. Création des boîtes mails

Les comptes système servent de boîtes mail :

sudo adduser apero

Chacun à son répertoire Maildir :

sudo mkdir /home/apero/Maildir

sudo maildirmake.dovecot /home/apero/Maildir

sudo chown -R apero:apero /home/apero/Maildir

9.6. Test du service SMTP

Depuis le serveur :

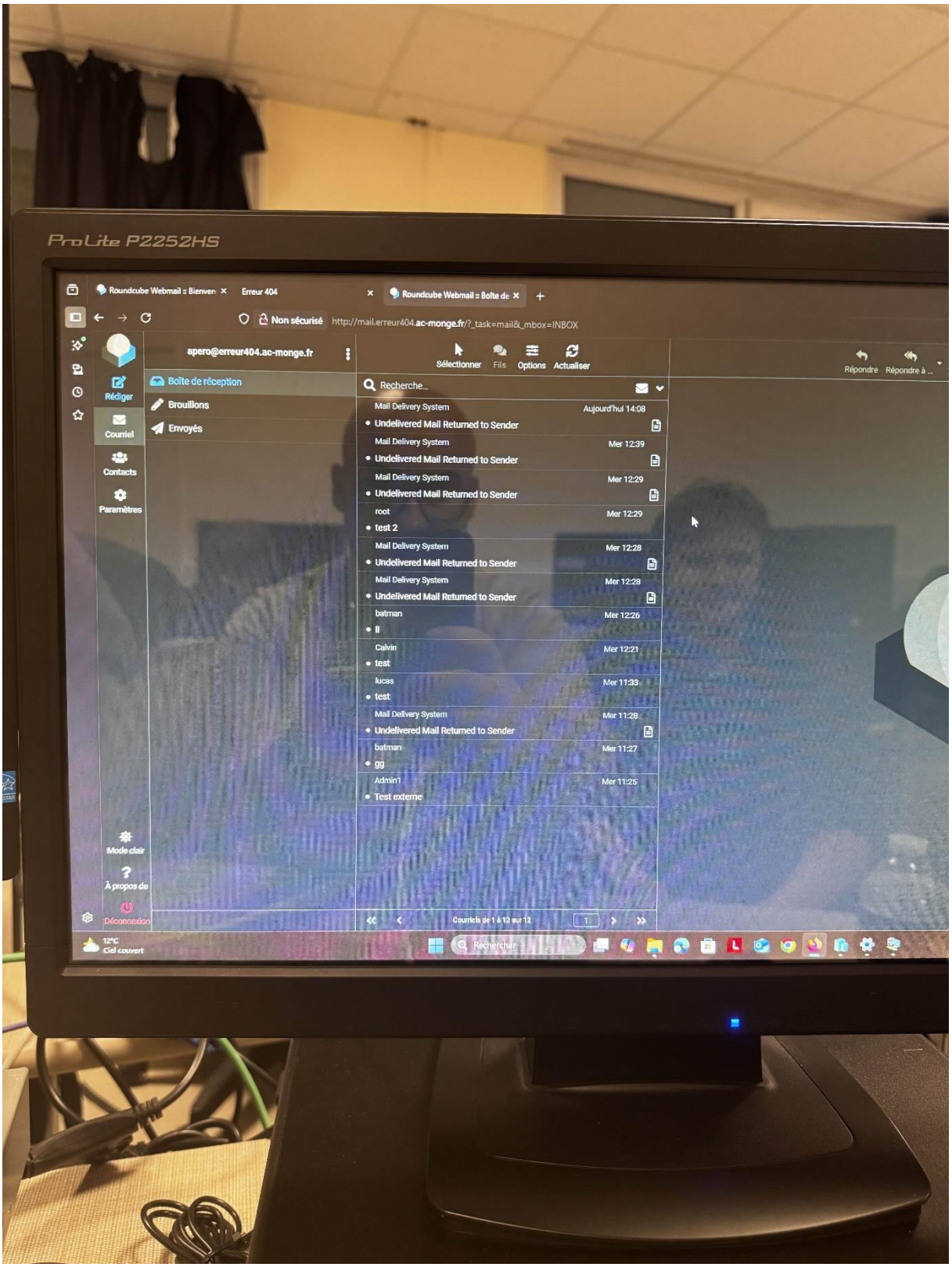
sendmail apero@erreur404.ac-monge.fr

Subject: Test

Salut, ceci est un test.

.

Puis vérifier la réception :



9.7. Configuration de Roundcube (Webmail)

Roundcube permet de consulter les mails via navigateur.

Fichier /etc/roundcube/config.inc.php

```
<?php

$config = [];

// Do not set db_dsnw here, use dpkg-reconfigure roundcube-core to configure database!
include("/etc/roundcube/debian-db-roundcube.php");

// IMAP
$config['imap_host'] = '127.0.0.1:143';

// SMTP
$config['smtp_host'] = '127.0.0.1:25';
$config['smtp_port'] = 25;

$config['smtp_user'] = '%u';
$config['smtp_pass'] = '%p';

$config['smtp_auth_type'] = 'PLAIN';

$config['smtp_conn_options'] = [
  'ssl' => [
    'verify_peer' => false,
    'verify_peer_name' => false,
  ],
];
```

$config['support_url'] = '';

$config['product_name'] = 'Roundcube Webmail';

$config['des_key'] = 'F6/1U6Zg5okvOFKw50gF3Kpg';

$config['plugins'] = [];

$config['skin'] = 'elastic';

$config['enable_spellcheck'] = false;

$config['smtp_debug'] = true;

$config['mail_domain'] = 'erreur404.ac-monge.fr';

$config['smtp_force_from'] = '%u@erreur404.ac-monge.fr';

$config['use_username_domain'] = true;

Conclusion

Ce TP m'a permis de mettre en place une infrastructure réseau complète et cohérente, similaire à celle d'une PME. J'ai configuré un serveur DNS faisant autorité, un service DHCP fonctionnel, un serveur Web accessible depuis le WAN, ainsi qu'un système de filtrage DNS. L'ensemble de la hiérarchie DNS a été respecté, avec une zone directe, une zone inverse et des zones de blocage opérationnelles.

La mise en place du serveur de messagerie (Postfix, Dovecot et Roundcube) m'a également permis de comprendre le fonctionnement d'un service mail interne, depuis la configuration SMTP/IMAP jusqu'à la consultation des messages via un webmail.

Les différents tests réalisés ont confirmé le bon fonctionnement de l'infrastructure (vu par vous): résolution interne et externe, délégation DNS, blocage de domaines, accès à la page Web, réception et envoi de mails. Ce TP m'a donc permis de maîtriser les bases essentielles de l'administration réseau et des services associés, en appliquant une architecture claire, fonctionnelle et sécurisée.