Projet : Mise en place d'un FAI simplifié

Dans ce projet, nous vous proposons de mettre en place un « petit FAI » avec une partie de configuration du réseau et de ses services. Le projet se fera dans un environnement virtuel qui vous sera expliqué lors de la première séance de TP et vous permettra de travailler seul sur votre projet.

Objectifs :

- Savoir concevoir un plan d'adressage et le mettre en place
- Maîtriser le routage statique comme dynamique
- Comprendre les protocoles réseaux introduits en cours, TDs et TPs.
- Configurer des services réseaux et applicatifs simples

Description du réseau du FAI

La figure suivante (Figure 1) présente l'architecture réseau à mettre en place. Des plages d'adresses vous seront fournies individuellement, ***veillez à bien les respecter car une erreur sur ces plages vous vaudra une note nulle au projet.*** Il faut impérativement que l'architecture réseau de votre projet (plan d'adressage et configuration associée des interfaces réseaux) soit correcte et opérationnelle avant d'aller plus loin. ***Il est inutile d'essayer d'avancer sur un quelconque autre élément tant que les réseaux ne communiquent pas un à un***.

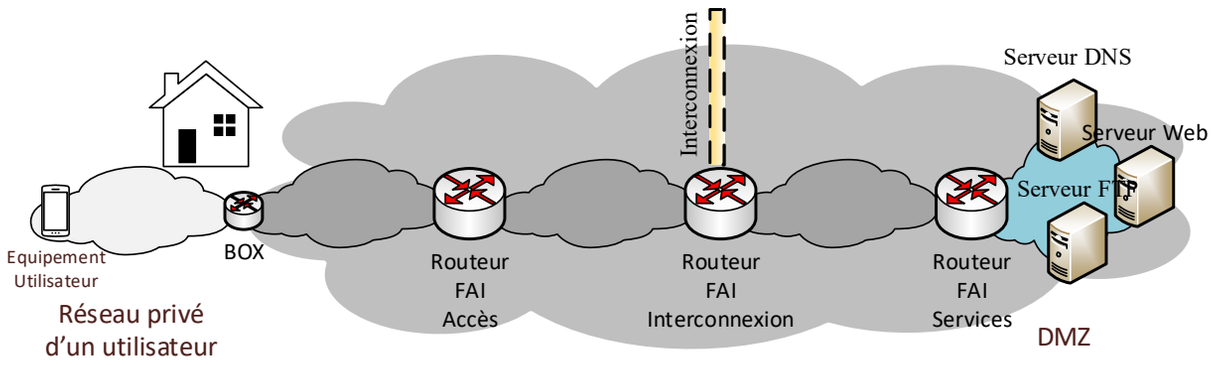


Figure 1 : Vue logique de l'architecture réseau d'un FAI

Le FAI dispose d'une plage d'adresse fournie à la première séance de projet qui doit lui permettre de mettre en place l'architecture logique présente ci-dessus. On peut noter différents éléments :

- Le cœur du réseau du FAI est constitué de trois réseaux interconnectés par des routeurs ;
- Le FAI dispose d'un client dont il configure la box pour permettre la bonne communication de ses clients (cf. TP réseau domestique). Le réseau du client est un réseau privé dont la plage d'adresse est aussi spécifiée pour chaque étudiant.
- Un réseau dit DMZ (DeMilitarized Zone) où le FAI positionne ses serveurs de service
- Un lien d'interconnexion sur le Routeur FAI d'interconnexion (à prévoir mais cette partie sera optionnelle)

Cette architecture nous donne l'architecture physique suivante (Figure 2). Lorsque vous créerez l'architecture réseau, prenez soin à créer des équipements du bon type et avec le bon nombre d'interfaces.

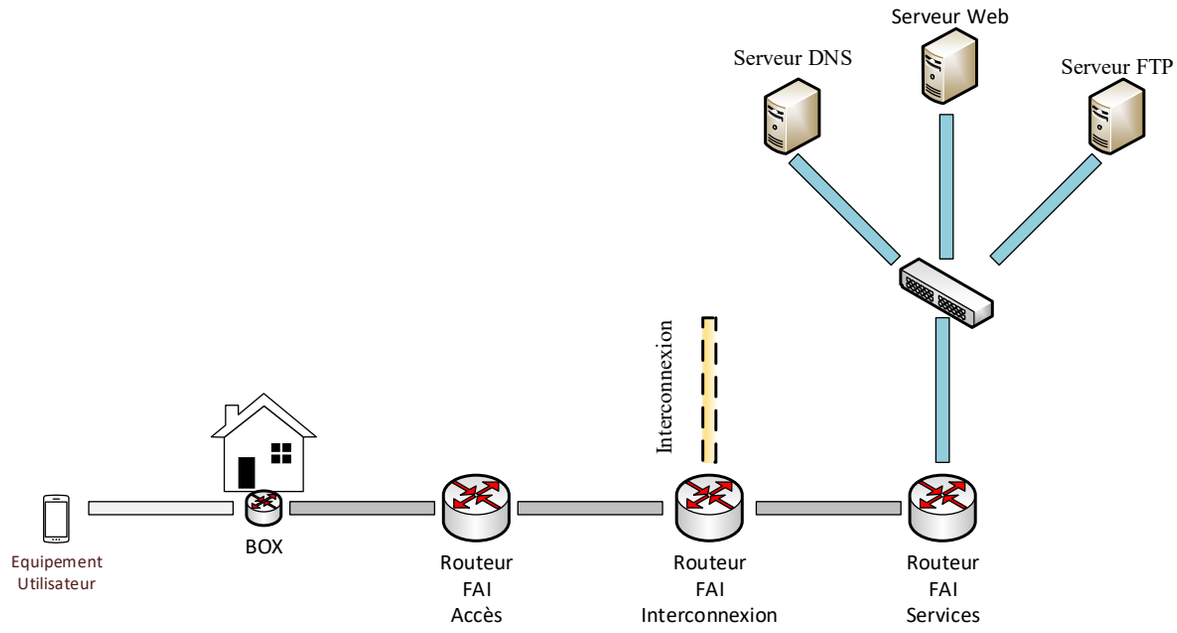


Figure 2 : Architecture du réseau du FAI

Etapes du projet

- Prise en main des outils de virtualisation et installation sur sa machine ;
- Création de l'architecture réseau ;
- Mise en place de l'adressage et test par routage statique ;
- Mise en place du routage dynamique entre les routeurs du FAI en utilisant RIP, test et visualisation ;
- Configuration de la box et du réseau privé, test et visualisation ;
- Mise en place du service web du FAI, test et visualisation ;
- Mise en place du service DNS du FAI, test et visualisation ;
- Mise en place de la sécurité de la DMZ ;
- Mise en place de la sécurité du réseau privé ;
- Mise en place du service FTP du FAI, test et visualisation ;
- Interconnexion avec un autre FAI (**Optionnel**) ;

Organisation et déroulement des séances

Le projet se déroule sur plusieurs mois et est ponctué de cinq séances planifiées :

	Séance 1	Séance 2	Séance 3	Séance 4	Séance 5
Dates	Semaine du 8 Février	Semaine du 22 Février	Semaine du 5 Avril	Semaine du 3 Mai	Semaine du 17 Mai Double créneau
Objectifs	Lancement du projet	Séance encadrée	Evaluation intermédiaire	Séance encadrée	Présentation et évaluation finale

Les séances sont planifiées dans les salles C308, C309, A005a et A005b. Toutefois, il est possible que cela doive avoir lieu à distance. **Je vous demande donc d'installer l'environnement sur votre ordinateur**. La séance 1 nous permet de présenter le projet et l'utilisation de l'environnement de virtualisation. Elle est essentielle pour votre bonne compréhension du sujet, du travail attendu et de comment le réaliser. La séance 3 est un point intermédiaire durant lequel vous nous expliquerez votre travail et elle sera évaluée. La séance 5 sera pour vous le moment de présenter votre travail et de nous en faire la démonstration ce qui nous permettra d'avoir une évaluation finale de votre travail. Des questions seront posées pour juger de votre compréhension.

En plus de ces séances, nous mettons à votre disposition les salles en dehors des heures où elles sont utilisées, du moment que vous respectez les consignes de l'école tant au niveau respect de l'espace de travail de chacun que des équipements mis à votre disposition. Il faudra pour cela qu'une personne se porte responsable pour prendre les clés à l'accueil de l'école et s'engage à les rendre après la séance. Les salles doivent être fermées après votre passage.

Si besoin quelques séances de permanence seront organisées en soirée. Elles seront renseignées à l'EDT.

ANNEXE
Environnement de virtualisation

L'environnement qui est mis à votre disposition a été instancié dans une machine virtuelle, ce qui demande de connaître les rudiments d'utilisation des VMs.

Ici nous utiliserons Virtualbox comme outil de virtualisation, un produit opensource, mais par la suite, tout autre lecteur de VM est utilisable. Depuis cette année, l'image est directement installée sur les machines de TP (boot projetRézo) et doit être téléchargée pour être mise sur votre machine. Des tutoriels vidéos sont disponibles sous moodle.

1. Machine virtuelle
1.1 En salle de TP
Etape 1 – Démarrer la machine de TP dans le bon mode
Pour le moment, il faut utiliser la version sécurité (Ubuntu 18) pour faire tourner la VM du projet.
Le login est tls-sec et le mot de passe toorb301
Etape 2 – Récupérer l'image de la machine virtuelle
L'image est toujours disponible sur le serveur tpsn.enseeiht.fr/jufasson, accessible à partir du réseau de l'école.

- Télécharger l'image – bouton de droite -> enregistrer la cible du lien sous et attendre la fin du téléchargement.
- couper/coller l'image de Mes Téléchargements au dossier /STORAGE. S'il existe déjà une image dans STORAGE, vous pouvez l'utiliser ou l'écraser, ou encore faire un répertoire pour votre travail.

Attention : Si cette partie sera toujours possible, nous avons prévu d'installer directement l'image en mode non modifiable en utilisant KVM, ce qui pourra par la suite vous éviter cette étape.
Etape 3 – Lancement, importation de l'image et configuration sous VirtualBox
Après avoir lancé Virtualbox en mode administrateur :

- Importer l'image de la VM ;
- Configurer le dossier de partage pour pouvoir monter votre clé usb ou un dossier de travail dans la machine virtuelle ;
- Configurer la mémoire de la machine à 2048Mo
- Enfin démarrer la machine virtuelle que vous avez chargée.

Etape 4 – Vérification de l'accès au dossier partagé
1.2 Sur votre propre équipement
Etape 1 – Récupérer l'image de la machine virtuelle
L'image est toujours disponible sur le serveur tpsn.enseeiht.fr/jufasson, accessible à partir du réseau de l'école. Vous pouvez donc soit la télécharger à partir du site de l'N7 soit en vous connectant via VPN.
Stocker là sur un support physique amovible pour pouvoir travailler dessus et l'amener à l'école (clé usb, disque dur portable, PC portable).
Etape 2 – Installer VirtualBox (optionnel si déjà effectué)
Sur votre équipement télécharger la version de VirtualBox correspondant à votre OS et installer là.
Etape 3 – Lancement, importation de l'image et configuration sous VirtualBox
Cf. partie 1.1

2. YANE
YANE est un outil de virtualisation développé à l'origine par Emmanuel Chaput. Un étudiant en stage de première année est venu compléter cet outil pour offrir une interface aux projets et aux TPs. L'utilisation de l'outil passe par plusieurs étapes, toutes sont accessibles à partir du dossier YANE_GUI.
2.1 Création du projet (étape optionnel si le projet existe déjà)
La première étape d'un projet est de créer le projet lui-même. Dans un premier temps on génère graphiquement une architecture à l'aide de l'outil de création (01-Create.html). On peut ici glisser pour déposer les différents éléments que l'on souhaite retrouver dans notre réseau, leur attribuer un nom réseau, un nombre d'interfaces et les relier entre elles. Une fois notre architecture terminée on peut cliquer sur le bouton en bas à droite « Télécharger l'Architecture ». Un fichier JSON est alors téléchargé.
La seconde étape consiste à générer le projet en disposant d'une architecture précédemment créée avec l'interface graphique (fichier JSON). Pour cela il suffit d'exécuter le script 02-Build avec la commande suivante : ./02-Build <PATH TO JSON>. Ce script va créer un nouveau projet dans le dossier ./Projets/<NOM DU PROJET>.

ATTENTION : Pour sauvegarder ce projet, c'est ce dossier qu'il faut enregistrer sur votre clé ou sur votre espace.

2.2 – Utilisation

Une fois crées, les projets se trouvent dans le dossier "./Projets". Un projet est un dossier contenant YANE et des scripts permettant son bon fonctionnement et ajoutant d'autres fonctionnalités comme l'utilisation de wireshark sur n'importe quel élément du réseau virtuel.

Un projet dispose de 2 scripts de gestion START et STOP pour lancer et arrêter le projet.

Un projet dispose de 2 types de machines émulées, des dockers et des namespaces. Chaque machine émulée dispose d'un script qui lui est associé (présent dans le dossier scripts du projet correspondant) et de fichiers « partagés » (présents dans le dossier files du projet correspondant).

Fichiers partagés :

Dans le dossier files du projet on retrouve des dossiers correspondants aux éléments réseaux (docker) de notre architecture (exemple : serveur web, dns, dhcp..). A chaque démarrage de projet ces fichiers remplacent les fichiers présents dans le container Docker. Ce système permet ainsi de sauvegarder les modifications des fichiers de configuration.
Chaque image Docker dispose de fichiers par défaut qui sont copiés dans leur dossier partagé lors de la création d'un Projet (Phase de Build). On peut retrouver et modifier ces fichiers par défaut dans le dossier ./ModelFiles/files/ on retrouve dans ce dossier les noms des différentes images Docker disponibles (cf partie 7). Ainsi on retrouve par défaut les fichiers suivants :

- Pour le Docker DHCP : Configuration par défaut de dhcpd
- Pour le Docker DNS : Configuration complète d'exemple (fonctionne pour l'exemple de projet fonctionnel)
- Pour le Docker FTP: Configuration complète d'exemple (fonctionne pour l'exemple de projet fonctionnel)
- Pour le Docker Routeur: Configuration par défaut de ripd
- Pour le Docker WEB: Site WEB d'exemple

Scripts :

Pour sauvegarder l'avancement de la configuration des différents éléments virtuels (par exemple configuration IP, routes, IPTABLES.. etc) un système de script a été mis en place. Dans un Projet chaque élément dispose d'un script du même nom qui lui est associé dans le dossier scripts. Pour ce qui est des Namespace ces scripts sont exécutés automatiquement au démarrage (fonctionnalité de YANE). Pour ce qui est des Dockers il suffit d'exécuter la commande suivante dans la console xterm de l'élément virtuel pour exécuter le script correspondant : ***init***

Ainsi de cette façon on peut sauvegarder notre avancement dans la configuration **en écrivant nos commandes dans les scripts** et **en modifiant les fichiers de configurations des services dans les fichiers partagés**.

Wireshark :

Dans chaque projet on trouve un script nommé "wireshark" qui permet d'exécuter wireshark sur les différents éléments virtuel du réseau. Pour l'utiliser il suffit de connaître le nom donné à l'élément que l'on veut observer dans wireshark et d'utiliser la commande suivante : ***sudo ./wireshark <NOM>***

Par exemple si on veut observer le trafic sur le serveur DHCP nommé « DHCP_1 » il suffit d'exécuter la commande suivante depuis le dossier du projet correspondant dans la VM (et non le container ou le docker): ***sudo ./wireshark DHCP_1.*** Wireshark s'ouvre alors et on peut ensuite sélectionner les interfaces de la machine DHCP_1.

ATTENTION : Il s'agit du nom de votre élément et non du nom affiché en haut du terminal de l'élément. Par exemple : DHCP_1 et pas 1449_DHCP_1.

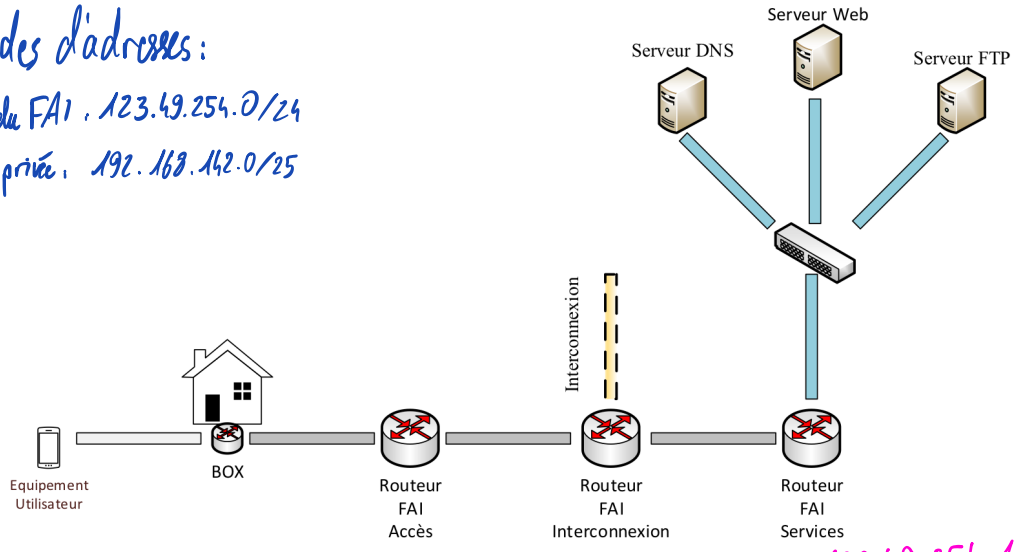
2.3 – Sauvegarde et chargement

Pour sauvegarder, il vous faut écrire les commandes à lancer dans les scripts de chacun des éléments, modifier les fichiers de configuration des éléments docker et ensuite il vous suffit de copier votre répertoire de projet sur votre clé ou votre compte.
Pour charger, il vous suffit de recopier votre répertoire de projet dans le ./Projets/. de votre VM, et ensuite de charger les scripts.

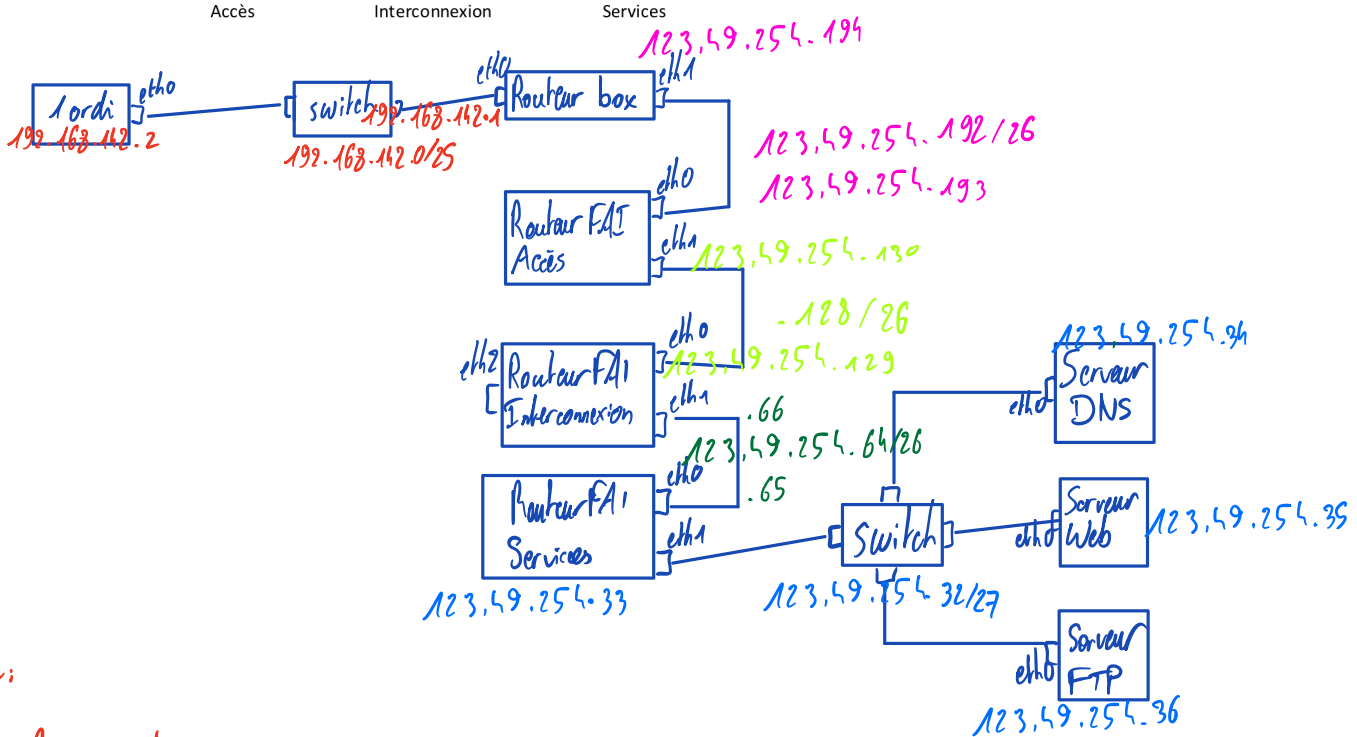
Bandes d'adresses :

Plage du FAI : 123.49.254.0/24

Plage privée : 192.168.142.0/25



sur YANE :



Routage dynamique :

⚠ ne pas oublier les init !

Pour routage dyn. modif ripd.conf (à côté démons)

l. q. :
```
router rip
network 123. .. /26    adresse réseau1
network 123. .. /26    adresse réseau2
```

+ il faut yes les démons zebra et ripd

Config. box

dans etc/dhcp/dhcp-conf : ajout des lignes après authoritative. On n'inclut pas la box dans la range.

etc/default/isc-... : mettre le eth0.

mettre ligne LAN dans Box

↳ deuxième feuille des commandes avec eth qui va vers public

(on envoie l'info comme quoi l'équip. utilisateur est ici).

Config service web

service apache2 start dans script web

pour test : depuis équip. utilisateur : wget http://123.49.254.35 (adresse serv. web)

Config DNS :

ajout dans box/etc/dhcp/dhcp.config de l'option domain-name-servers

service bind9 start dans script DNS

DNS/etc/bind/zones : modif. de monsupersite.db

Les addresses DNS, www, FTP n'étaient pas bonnes.

pour test : depuis équip. utilisateur : wget http://www.monsupersite.com

Securité DMZ :

port web : 80 port DNS : 53

iptables -policy ... Pour DNS : politique icmp WEB : politique tcp port 80

Config. FTP :

service proftpd start

mais en fait on reprend lignes du projet modèle,

et on enlève celle ligne car c'est fait à la fin

dans proftpd.conf, j'ai enlevé commentaire des ports passifs 49152 à 65534, que j'ai remis dans les fire walls.

total : 16 382 ports permis

pour test : wget ftp://ftpusr:ftpusr@123.49.254.36

telnet ftp.monsupersite.com 21

USER ftpusr

PASS ftpusr

SYST

passive mode : PASV