2017-2018

# Mise en place d'une architecture réseau

Epreuve E6

Raphaël Andrieu
ESICAD

# Table des matières

Cahier des charges ..... 1
Architecture ..... 2
Configuration des interfaces ..... 2
Activation du routeur ..... 4
Activation du NAT ..... 5
Tester la communication entre les réseaux ..... 5
Installation du service APACHE et SSH sur le serveur LINUX ..... 9
Installation de Apache ..... 9
Installation de SSH ..... 10
Essayer le SSH ..... 11
Sécurisation des accès avec filtrage du trafic par iptables ..... 13
Accepter le FTP et le SSH pour l'administrateur ..... 13
Accepter l'accès a l'intranet pour les stagiaires et le service administratif ..... 13
Refuser aux stagiaires tout le reste ..... 13
Automatiser le montage des règles IPTABLES ..... 14

# Cahier des charges

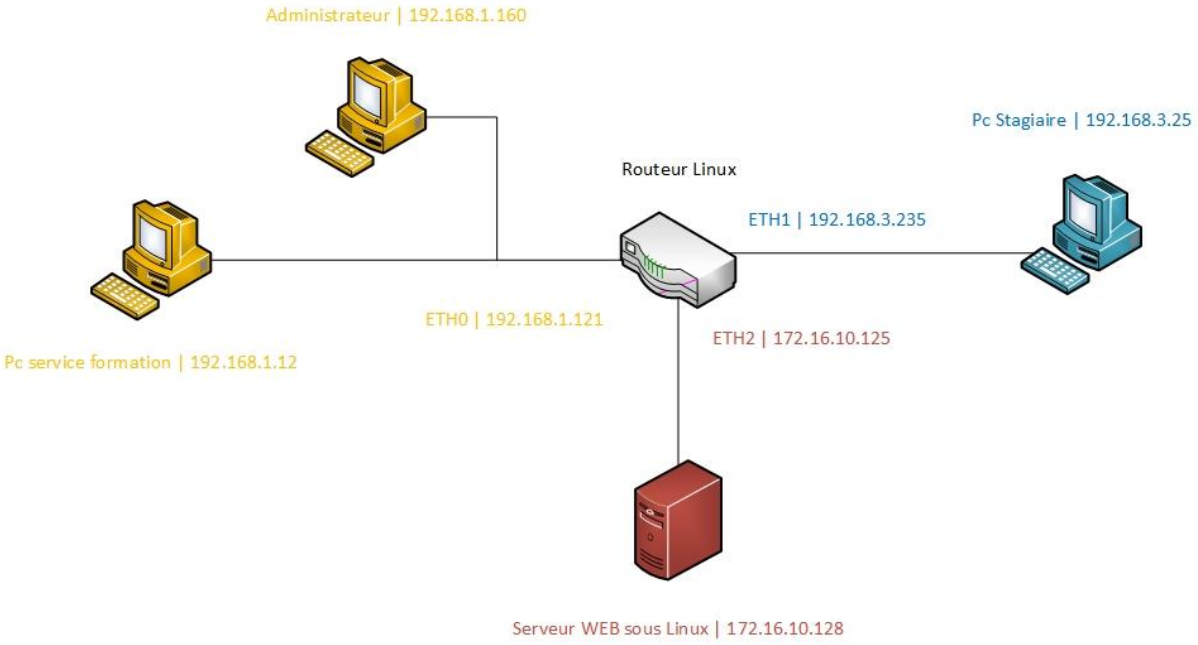
Vous êtes chargé par le groupe campus de séparer les flux du service administratif des flux venant des salles de formation. Pour simplifier l'architecture on considère que tout le service formation est dans un seul sous-réseau.

Vous devez déplacer le serveur web hébergeant l'intranet dans un autre sous-réseau dit DMZ, pour le sortir du réseau local du service administratif.

Tous les services continuent d'accéder à Intranet en utilisant le même routeur

Proposez et mettez en place une architecture répondant au CDC.

# Architecture




# Configuration des interfaces

Nous allons avoir besoin pour répondre à ce cahier des charges de 3 interfaces sur le serveur Linux. Pour cela nous allons configurer ses interfaces.

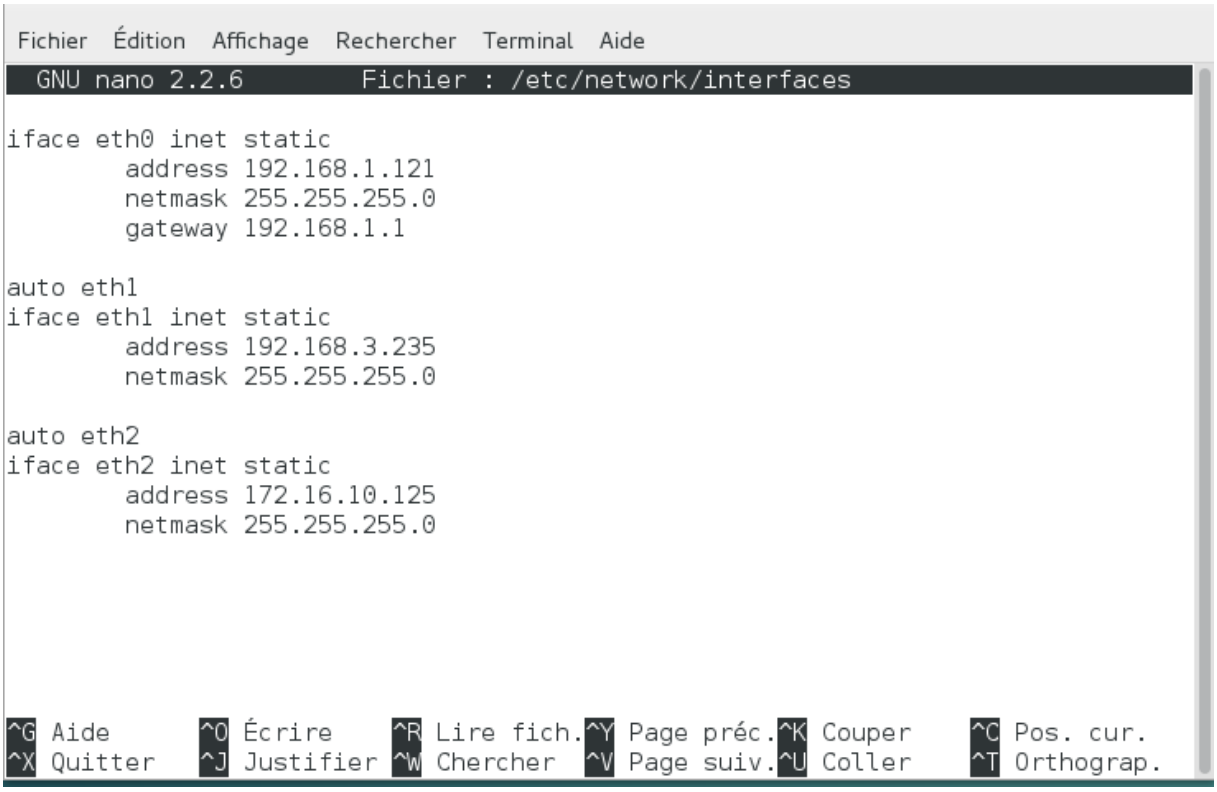
Ouvrez le terminal, puis passez en mode « root » en écrivant :

- su root

Un mot de passe vous sera demandé.

Après être passé en mode « root » nous allons ajouter les interfaces dans le fichier « interfaces » en écrivant la commande :

- nano /etc/network/interfaces




Nous configurons la première interface en eth0, avec comme adresse : 192.168.1.121, un masque de sous réseau : 255.255.255.0 et une passerelle : 192.168.1.1 (l'adresse du routeur internet)

Puis la deuxième interface en eth1, avec comme adresse : 192.168.3.235 et un masque de sous réseau : 255.255.255.0

Puis la troisième interface en eth2, avec comme adresse : 172.16.10.125 et un masque de sous réseau 255.255.255.0

Nous ne configurons pas de passerelle sur eth1 et eth2 car ces 2 interfaces n'ont pas à envoyer de trafic sur d'autres routeurs

Après avoir fini de configurer le fichier « interfaces », il faut redémarrer le service réseau avec la commande :

- /etc/init.d/networking restart

Pour vérifier que nos paramètres ont bien été pris en compte, il faut écrire la commande :

- Ifconfig

```
root@srv-deb-ar:/home# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:fb:d9:43
          inet adr:192.168.1.121  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fefb:d943/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:17068 (16.6 KiB)  TX bytes:18277 (17.8 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:b6:22:8e
          inet adr:192.168.3.235  Bcast:192.168.3.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:feb6:228e/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:17059 (16.6 KiB)  TX bytes:18236 (17.8 KiB)

eth2      Link encap:Ethernet  HWaddr 08:00:27:05:9b:09
          inet adr:172.16.10.125  Bcast:172.16.10.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe05:9b09/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1293 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
```

Vérifiez que chaque interface a bien la bonne configuration.

## Activation du routeur

Pour relier les différents sous-réseaux nous avons besoin d'un routeur. Ici nous utiliserons ce serveur Linux comme routeur.

Après avoir configuré les interfaces, nous pouvons mettre en place le mode routeur sur notre Linux, pour cela il faut modifier le fichier sysctl.conf en écrivant la commande :

- nano /etc/sysctl.conf

Dans ce fichier, il faut dé-commenter la ligne :

- net.ipv4.ip_forward=1

```
Fichier  Edition  Affichage  Rechercher  Terminal  Aide
 GNU nano 2.2.6          Fichier : /etc/sysctl.conf

#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Après avoir modifié ce fichier, nous pouvons recharger le fichier en écrivant la commande :

- sysctl -p /etc/sysctl.conf

## Activation du NAT

Pour utiliser notre routeur Linux comme passerelle internet pour tous les sous-réseaux, nous devons y implémenter la translation d'adresses, le NAT. Cela permettra aux adresses privées des réseaux locaux d'accéder à Internet.

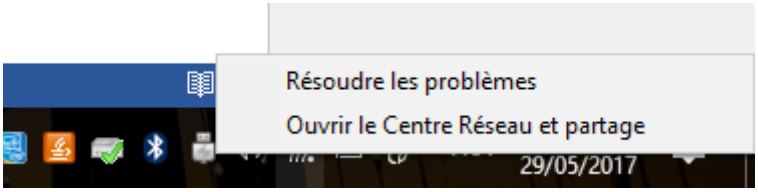
Nous allons donc préciser que eth0 est notre interface qui communiquera avec l'extérieur. Pour activer le nat sur l'interface eth0, il faut écrire la commande :

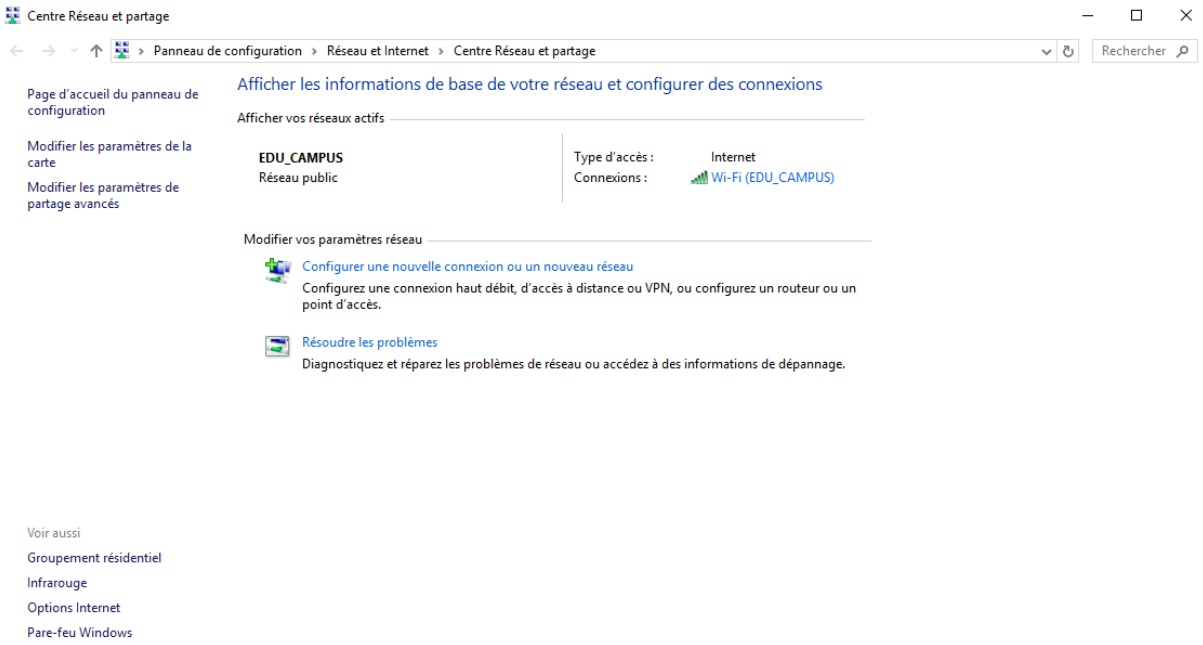
- iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

## Tester la communication entre les réseaux

Après avoir configuré les interfaces, activé le routeur et activé le NAT, nous allons « essayer de pinger » les réseaux entre eux. Pour cela nous allons mettre en place un ordinateur dans le réseau 192.168.3.0 qui sera notre réseau pour le service formation, un ordinateur dans le réseau : 192.168.1.0 et un serveur linux dans la DMZ en 172.16.10.0 qui nous servira par la suite de serveur WEB.

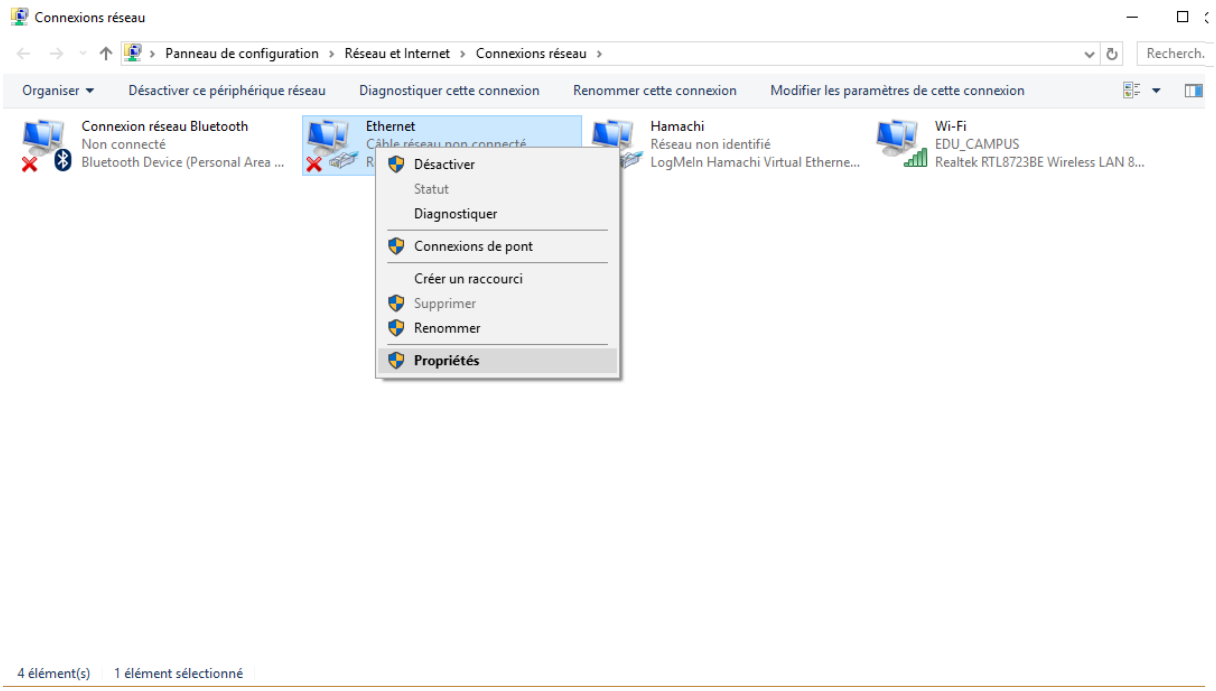
Pour configurer le poste sous Windows du réseau de formation. Il vous faut ouvrir le centre de réseau et partage en faisant un clic droit sur internet dans la barre des tâches.



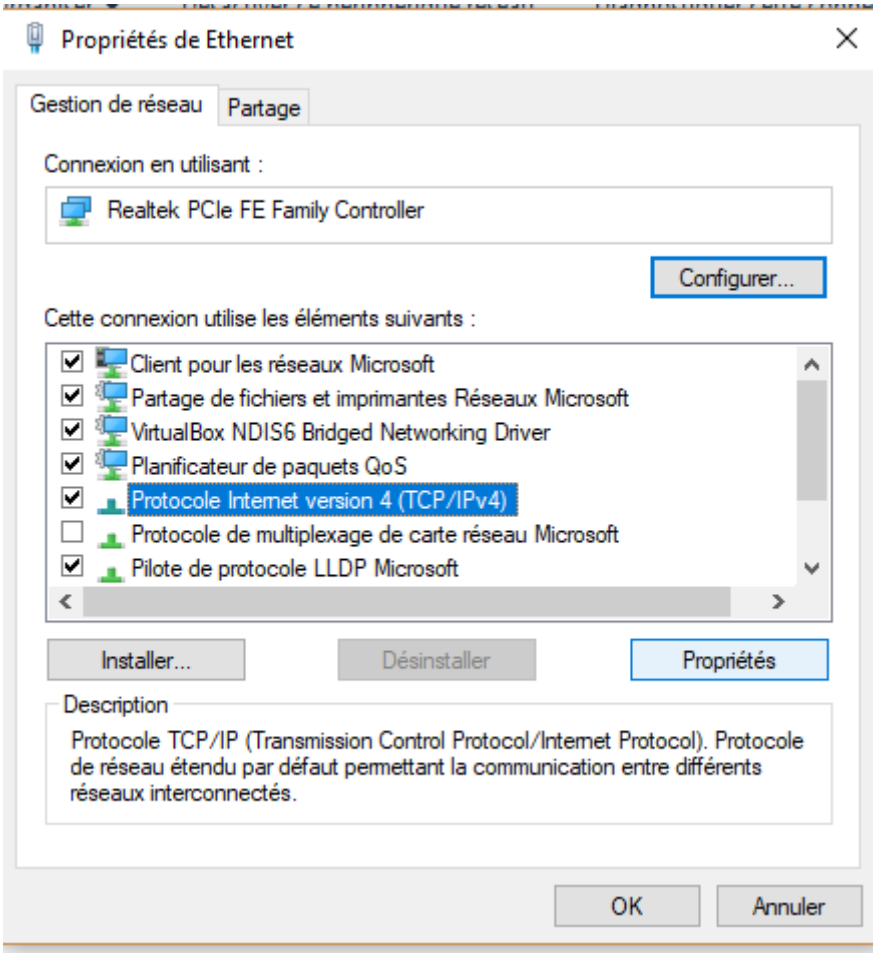




Puis sur « modifier les paramètres de la carte » sur la gauche.

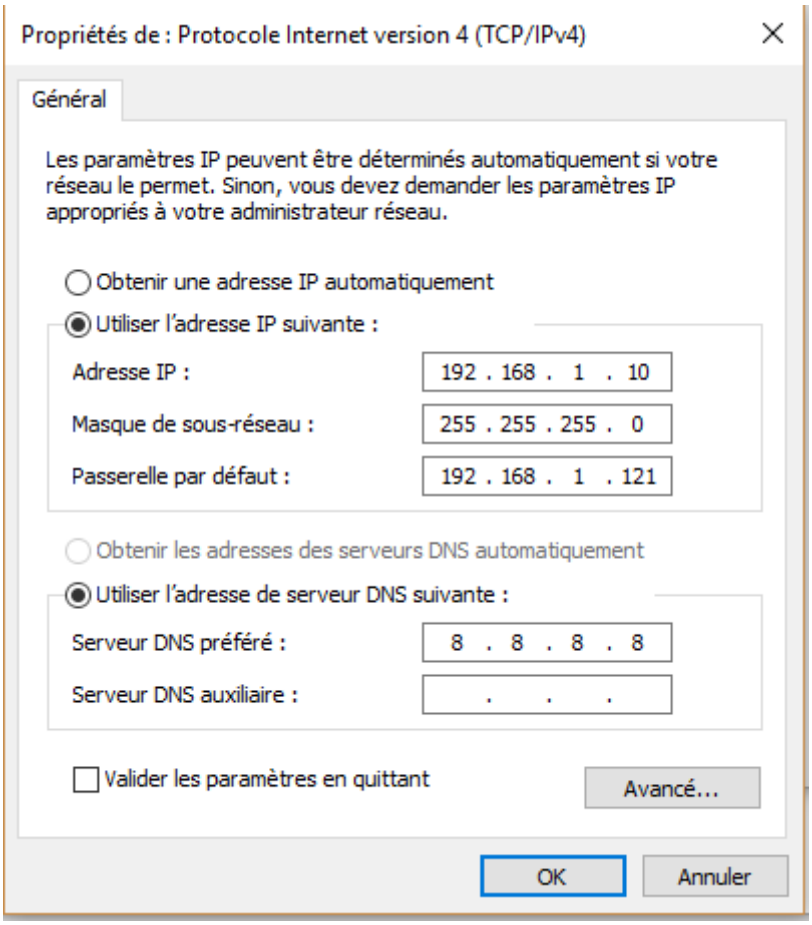
Puis faire un clic-droit > propriété sur la carte réseau.



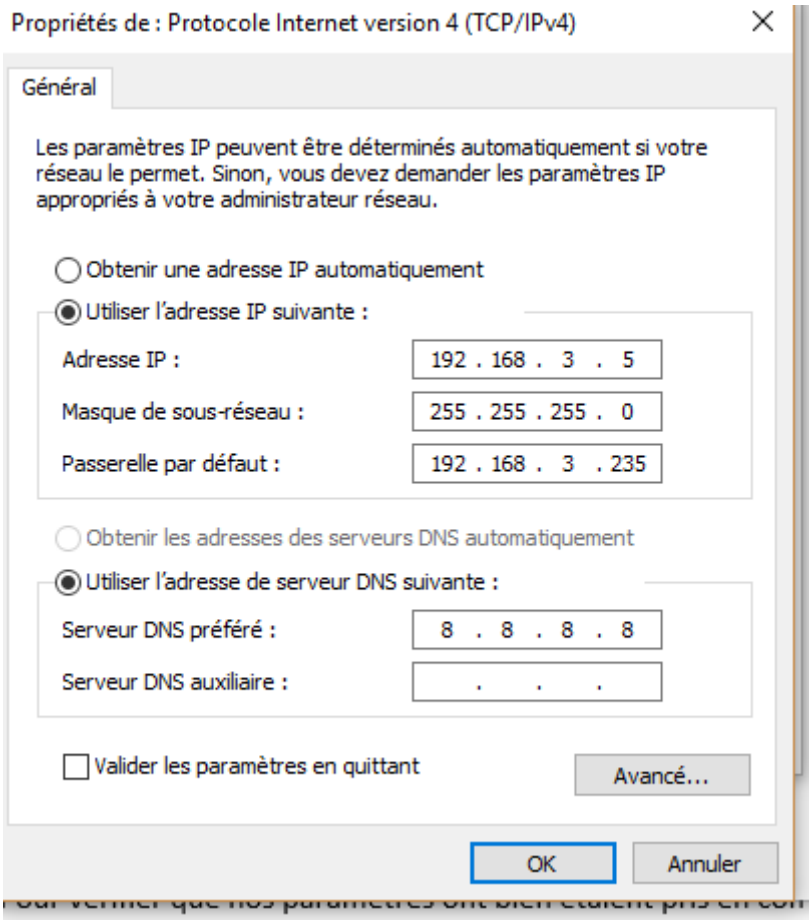

Puis sur « protocole internet version 4 (TCP/IVP4) » et sur propriétés



Puis remplissez les champs Adresse IP avec une adresse sur le réseau 192.168.1.0, un masque de sous réseau en 255.255.255.0 et mettre en passerelle, l'adresse IP de l'interface eth0.




Faire la même chose pour l'ordinateur sur le réseau de l'interface eth1, et mettre en passerelle l'adresse de l'interface eth1




Faire la même chose sur le serveur linux en configurant le fichier : /etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 172.16.10.128
netmask 255.255.255.0
gateway 172.16.10.125
```

Avec une adresse sur le réseau : 172.16.10.0 et avec comme passerelle l'adresse IP de eth2, ici : 172.16.10.125

Maintenant que les interfaces sont paramètres, vous pouvez essayer le ping entre réseau et le ping vers internet.

Depuis un poste du réseau 192.168.1.0 vers un poste du réseau 192.168.3.0


Depuis le poste du réseau 192.168.3.0 vers internet


Vous pouvez voir donc voir que tout fonctionne correctement. Si le ping vers internet ne fonctionne pas, vérifier bien que vous avez correctement activé le nat.

# Installation du service APACHE et SSH sur le serveur LINUX

## Installation de Apache

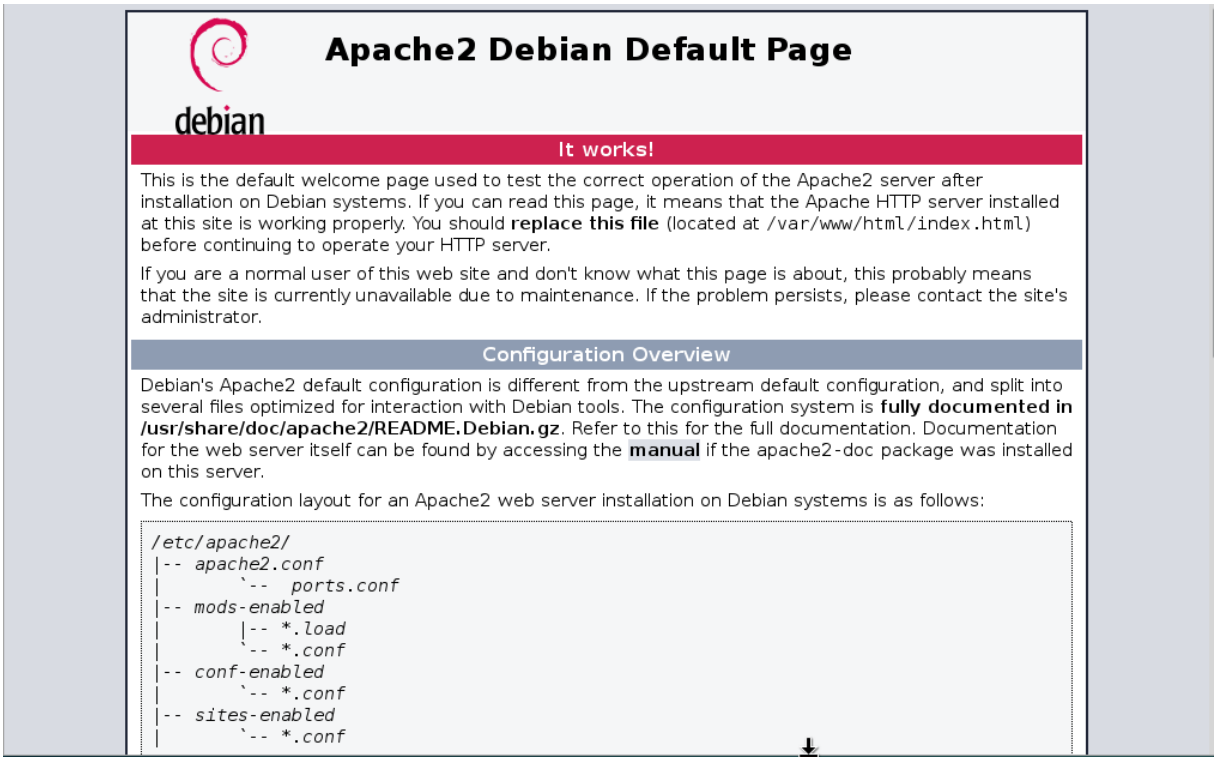
Nous allons mettre en place un serveur WEB sur le serveur linux, pour cela nous allons installer le plugin apache en écrivant la commande :

- apt-get install apache2

N'hésitez pas avant d'écrire cette commande, de mettre à jour les paquets avec la commande :

- apt-get update

Après avoir installé le module apache, vous pouvez essayer d'accéder au site intranet en rentrant l'adresse ip du serveur linux sur l'ordinateur d'un autre poste.




## Installation de SSH

Nous allons installer le module SSH en écrivant la commande :

- apt-get install ssh

Avant d'essayer le SSH, il faut créer un nouvel utilisateur avec la commande :

- adduser andry

andry est le nom de l'utilisateur que je vais créer, vous pouvez mettre le nom que vous voulez.


Un mot de passe vous est demandé.

Puis d'autres informations vous sont demandées, comme le nom ou le numéro de bureau (ces informations ne sont pas obligatoires vous pouvez laisser vide)

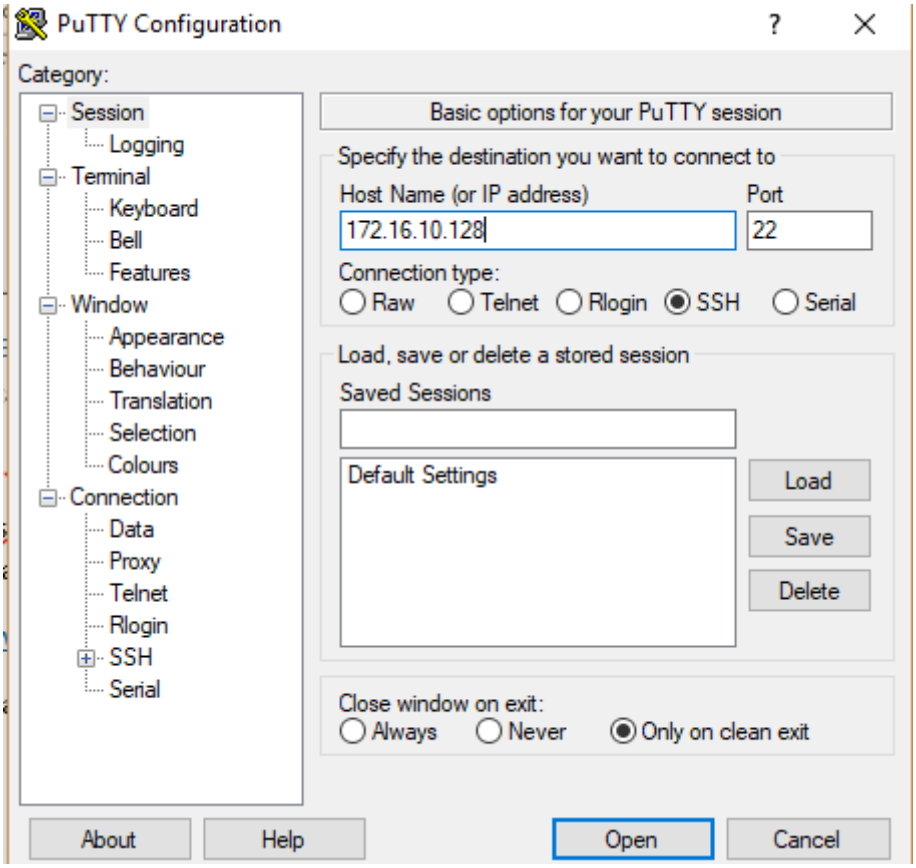
```
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur andry
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
        Nom complet []:
        N° de bureau []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Cette information est-elle correcte ? [O/n]
```

## Essayer le SSH

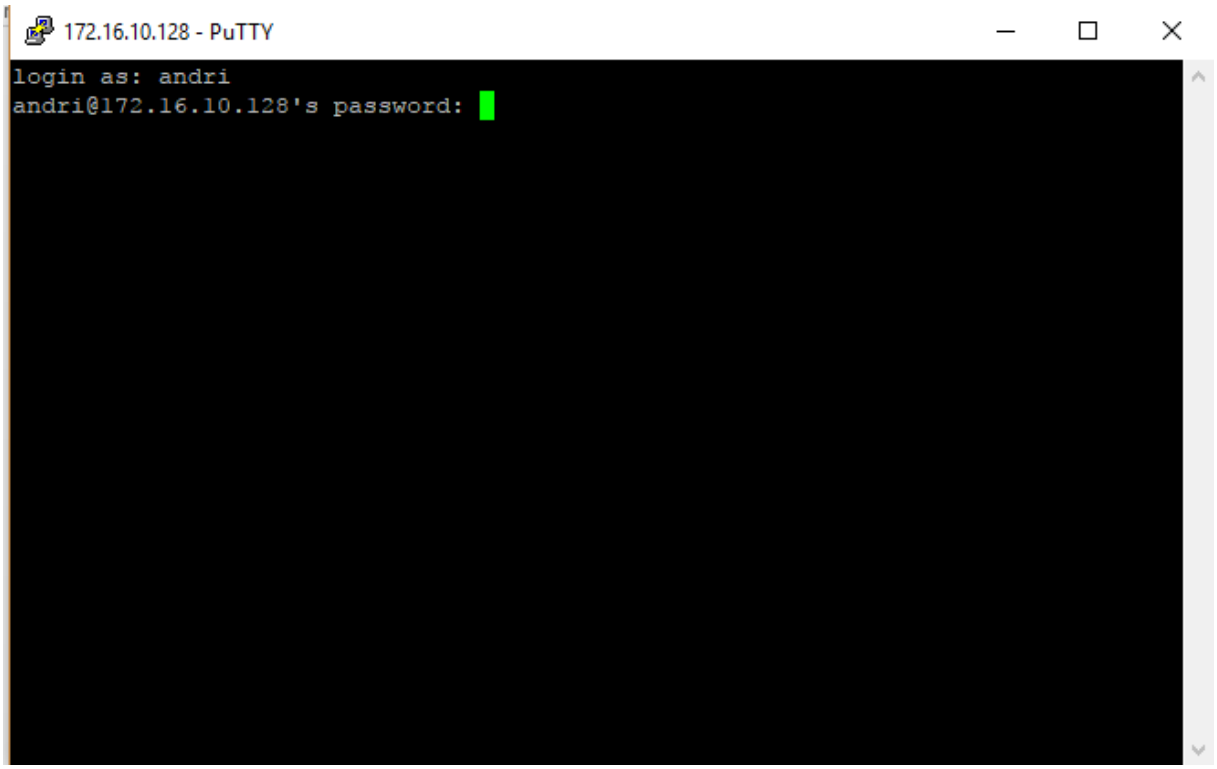
Installez PUTTY sur un des ordinateurs, par exemple un ordinateur du réseau 192.168.3.0 en allant sur l'url :

- http://www.putty.org/

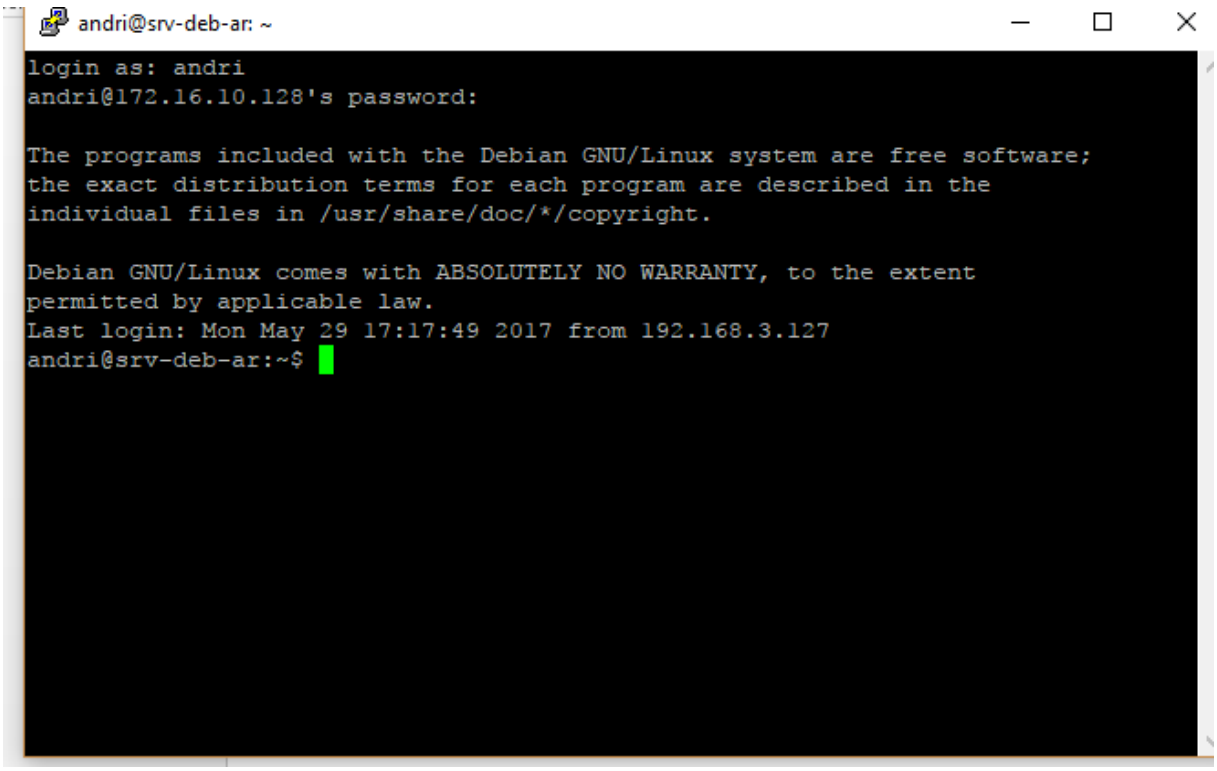
Après avoir installé PUTTY, lancez-le et écrivez dans « host name » l'adresse IP du serveur linux




Puis cliquez sur Open, il vous est demandé un nom d'utilisateur (créé auparavant et un mot de passe)




Vous voilà connecté au routeur.



# Sécurisation des accès avec filtrage du trafic par iptables

Restriction demandée :

- Les stagiaires n'ont accès qu'au serveur web (HTTP : 80)
- Le service administratif aura aussi accès à l'intranet
- Les accès en FTP et SSH sont réservés au seul administrateur dont l'adresse est : 192.168.1.160

## Accepter le FTP et le SSH pour l'administrateur

Nous allons tout d'abord mettre en place les règles permettant à l'administrateur d'accéder au FTP et SSH en écrivant les commandes :

1. Iptables –A FORWARD –s 192.168.1.160 –p tcp –dport 21 –j ACCEPT
2. Iptables –A FORWARD –s 192.168.1.160 –p tcp –dport 22 –j ACCEPT

La première commande permet d'autoriser l'adresse 192.168.1.160 d'accéder au port 21 qui est le port du FTP.

La deuxième commande permet d'autoriser l'adresse 192.168.1.160 d'accéder au port 22 qui est le port du SSH.

Vous pouvez vérifier les règles rentrées en écrivant la commande :

- Iptables –L

```
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.160        anywhere             tcp dpt:ssh
ACCEPT     tcp  --  192.168.1.160        anywhere             tcp dpt:ftp

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@srv-deb-ar:/home#
```

## Accepter l'accès a l'intranet pour les stagiaires et le service administratif

Pour permettre aux stagiaires et au service administratif d'accéder au serveur web, il faut accepter le port 80 sur leurs réseaux, pour cela il faut écrire la commande :

1. Iptables –A FORWARD –s 192.168.3.0/24 –p tcp –dport 80 –j ACCEPT
2. Iptables –A FORWARD –s 192.168.1.0/24 –p tcp –dport 80 –j ACCEPT

La première commande permet au réseau 192.168.3.0 d'accéder au port 80 qui est le port http

La deuxième commande permet au réseau 192.168.1.0 d'accéder au port 80 qui est le port http

## Refuser aux stagiaires tout le reste

Les stagiaires ne peuvent accéder qu'à l'intranet, donc il faut refuser l'accès au FTP. Pour cela nous allons écrire la commande :

1. Iptables –A FORWARD –s 192.168.3.0 –p tcp –dport 21 –j DROP
2. Iptables –A FORWARD –s 192.168.3.0 –p tcp –dport 22 –j DROP

## Automatiser le montage des règles IPTABLES

Pour aller plus loin dans les règles IPTABLES, nous pouvons automatiser ses règles pour éviter de devoir les écrire à chaque fois que le routeur est redémarré. Pour cela nous allons écrire la commande :

- iptables-save > /etc/iptables_rules.save

Iptables_rules.save = correspond à un nom que nous avons donné , ce nom n'est pas obligatoire, nous pouvons aussi appeler ce fichier : rulesiptables.save

Après avoir entré cette commande, nous allons ajouter dans le fichier /etc/network/interfaces la ligne de commande :

- post-up iptables-restore < /etc/iptables_rules.save

Cette commande permet à chaque fois de charger les règles du fichier « iptables_rules.save »