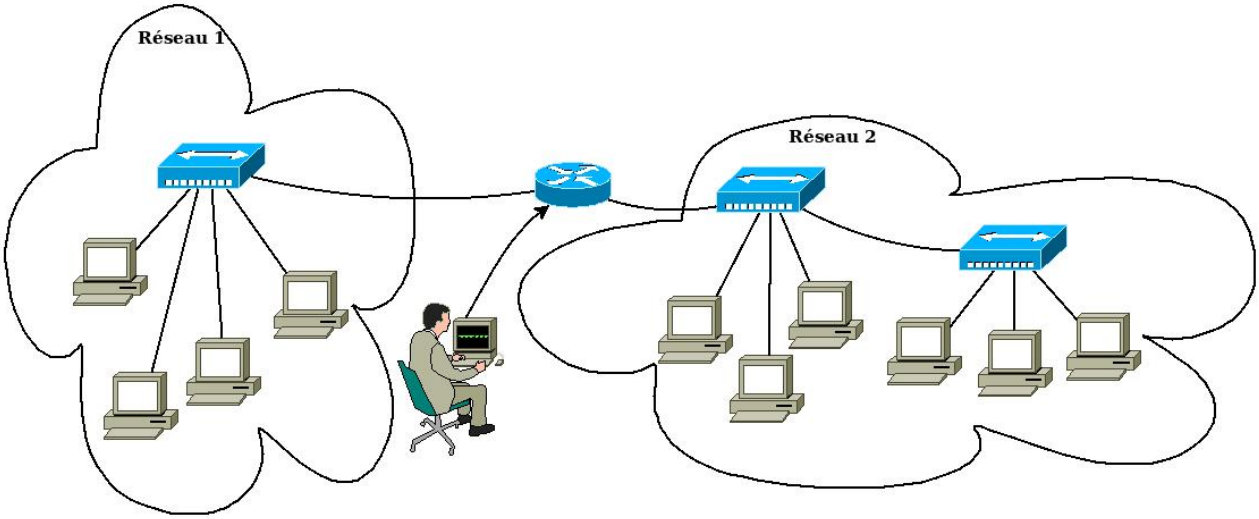
Département d'Informatique
Faculté des Sciences
Université Mohammed Premier
Oujda

TPs
Administration Réseaux



Filière : SMI
Semestre : 6

Pr. Abdelhak LAKHOUAJA
abdel.lakh@gmail.com

http://lakhouaja.oujda-nlp-team.net/teaching/bachlor-level/administration-reseaux/

Année universitaire 2019/2020

Table des matières

TP numéro 1

Gestion des utilisateurs

Exercice 1

Vous allez travailler dans une machine virtuelle.

Créez un fichier « noms.txt » contenant un ensemble de noms et de prénoms sous la forme suivante :

Oujdi ;Ali
Berkani ;Lina
⋮
Figuigui ;Aïcha

1. Créez un script qui permet de lire le fichier et de l'afficher. Le nom du fichier sera passé comme argument au script. Contrôlez l'existence du fichier avant de poursuivre le traitement du script. Utilisez un message de type :
   - « Usage : . . . », si l'argument n'a pas été donné.
   - « Fichier <. . . > inexistant », si le fichier passé en argument n'existe pas.
2. Modifier le script pour remplacer les caractères accentués par leur équivalent non accentué :
   `[éèàùçï] -> [eeauci]`
3. Pour éviter les doublons éventuels au niveau des « logins », vous prenez le premier caractère du prénom suivi de point (.) et du nom, tout en minuscule, pour former le nom de login de l'utilisateur (p.nom). Faire afficher ce login.
4. Modifiez le script précédent pour créer des comptes à partir du fichier « noms.txt », avec les caractéristiques suivantes :
   - login comme définit dans 3.
   - shell : /bin/bash
   - Le compte créé doit avoir un dossier personnel et un mot de passe. Pour simplifier, le mot de passe doit être fixé pour tous les comptes (par exemple smi6-2020).
5. Tester la connexion sur un des comptes créés.
6. (Question optionnelle) Créer un script qui permet de supprimer les comptes créés. Utiliser la commande « userdel ».

Indications :

- Utilisez la commande « cut », pour manipuler les différents champs du fichier « noms.txt ».
- Utilisez la commande « tr », pour pour remplacer transformer les majuscules en minuscules : tr A-Z a-z
- Utilisez la commande « sed », pour pour remplacer les caractères accentués : sed y/éèàùçï/eeauci/
- man useradd (pour les différentes options).
- La commande « chpasswd » permet d'affecter un mot de passe à un compte : `echo "login:MotPasse" | chpasswd`

TP numéro 2

HTTP et serveur web Apache

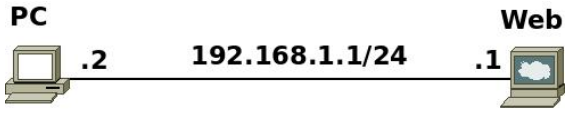
Exercice 2

Les principaux codes de retour du protocole HTTP.

Code	Signification
200	OK.
301	Le document a été déplacé définitivement.
302	Le document a été déplacé temporairement.
303	Il faut s'adresser à un autre serveur.
400	La syntaxe de la requête est mauvaise.
401	La requête requiert une autorisation.
403	La ressource demandée est interdite.
404	La ressource demandée n'existe pas.
408	Temps épuisé.
410	La ressource n'existe plus.
500	Le serveur, suite à une erreur interne, ne peut pas exécuter la requête.
501	La requête est légale mais non supportée par le serveur.
503	Service non présent.
504	Le serveur est très occupé.

Travail à faire :

Construisez et configurez le réseau présenté par la figure suivante :



Pour démarrer le serveur web apache au démarrage, ajoutez ans le fichier **web.startup**, la ligne :
/etc/init.d/apache2 start

Emplacement par défaut des pages html : **/var/www**

Pour la navigation, utilisez le navigateur en ligne de commandes **lynx**.

Utilisation de lynx

Commande	**Signification**
<Page Suiv.>, <Page Préc.>	Avancer ou reculer d'une page.
↓, ↑	Se positionner sur le lien suivant, précédent.
→ ou <Entrée>	Activer un lien (il faut être dessus).
←	Revenir sur la page précédente.
g	Saisir une URL.
m	Revenir à la page d'accueil.
ctrl+r	Rafraîchir la page courante.
h	Affiche l'aide (en anglais).
/	Effectuer une recherche d'une chaîne.
q	Quitter Lynx. A valider par y ou q.

L'option « -dump » permet d'afficher la page visité est de sortir. La commande :
lynx -dump 192.168.1.1
affichera à l'écran :

```
Looking up '192.168.1.1' first
        It works!
```

Téléchargement d'une page ou d'un fichier avec l'outil « wget »

```
pc:~# wget 192.168.1.1 /index.html
```

Protocole HTTP

Dans la machine web, créez dans le répertoire **/var/www** le fichier **test.txt** avec les droits `-rw-------`

Dans **pc**, en utilisant **telnet** (**telnet 192.168.1.1 80**), tapez les requêtes suivantes (il faut taper « Entrée » 2 fois après la requête) :

1. GET / HTTP/1.0
2. HEAD / HTTP/1.0
3. GET /test HTTP/1.0
4. GET /test.txt HTTP/1.0
5. HEAD / HTTP/3.0
6. Test / HTTP/1.0

Capture avec tcpdump

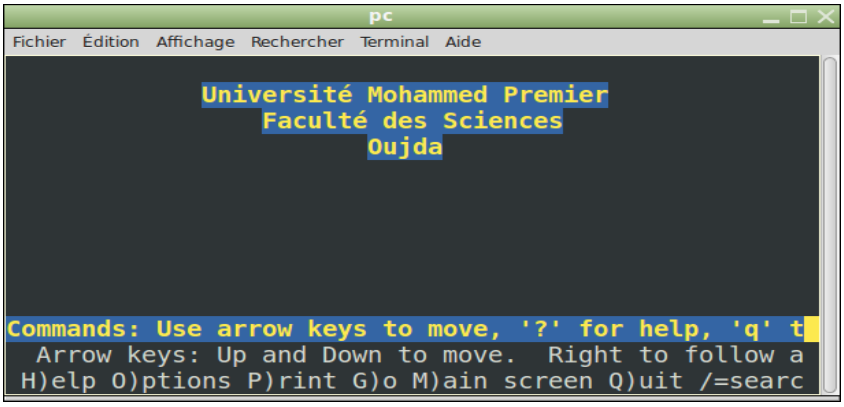
1. Dans la machine web, tapez la commande suivante :
   `tcpdump -s 1500 -w /hostlab/capturewb`
   L'option « `-s 1500` » est utilisée pour capturer l'intégralité des paquets (1500 Octets).

2. Dans pc, tapez la commande suivante :
   `lynx -dump 192.168.1.1`

Dans la machine réelle, visualiser le contenu du fichier « captureweb » en utilisant wireshark.

Configuration d'apache

- Sur la machine **web** :
  (a) modifiez la page d'accueil pour qu'elle affiche la page suivante :



  (b) Ajouter l'utilisateur smi.
  (c) Activez l'accès aux pages personnelles des utilisateurs :
  (d) Créez une page personnelle.
  (e) Testez l'accès a cette page.
  (f) Créez deux sites virtuels par nom : **etudiants-smi.ma** et **etudiants-sma.ma** (accessibles aussi par **www.etudiants-smi.ma** et **www.etudiants-sma.ma**).
  Remarque : sous **netkit**, il ne faut pas ajouter **.conf** aux fichiers de configuration (par exemple : **smi** et non **smi.conf**)
  (g) Créez un site virtuel par adresse IP : **info-smi.ma** (accessible aussi par **www.info-smi.ma**). Le site aura pour adresse 192.168.1.254
  (h) Interdisez l'accès au serveur principal et laissez l'accès aux sites virtuels créés.
  (i) Modifier la configuration du serveur web pour la page d'accueil soit « **accueil.html** » au lieu de « **index.html** ».
- Sur la machine **pc** :
  (a) Téléchargez la page d'accueil de la machine **web**.
  (b) Testez l'accès à la page personnelle de l'utilisateur **smi**.
  (c) Testez l'accès aux différents sites virtuels par nom et par adresse IP, créés dans la machine web.

Sécuriser le serveur web

1. Activez le mode sécurisé en tapant les commandes suivantes :
   `a2ensite default-ssl`
   `a2enmod ssl`

2. Dans la machine web, tapez la commande suivante :
   `tcpdump -s 1500 -w /hostlab/captureSSL`
3. Dans pc, accédez au serveur sécurisé via :
   `lynx https://192.168.1.1`
   (Vous devez accepter le certificat.)
4. Dans la machine réelle, visualiser le contenu du fichier « captureSSL » en utilisant wireshark. Que constatez vous ?

Ajout/suppression automatique d'un site virtuel

Dans la machine réelle, écrivez deux scripts qui seront appelés dans la machine **web** :

1. **ajoutSiteVirtuel.sh** qui permet d'ajouter un site virtuel par nom :
   - sera appelé comme suit : `./ajoutSiteVirtuel.sh nomDuSite` (par exemple, `./ajoutSiteVirtuel.sh smia`, pour ajouter le site smia.ump.ma et son alias www.smia.ump.ma) ;
   - fait les configurations nécessaires ;
   - active le site virtuel ;
   - redémarre serveur apache.
2. **supprimerSiteVirtuel.sh** qui permet de supprimer un site virtuel .

TP numéro 3

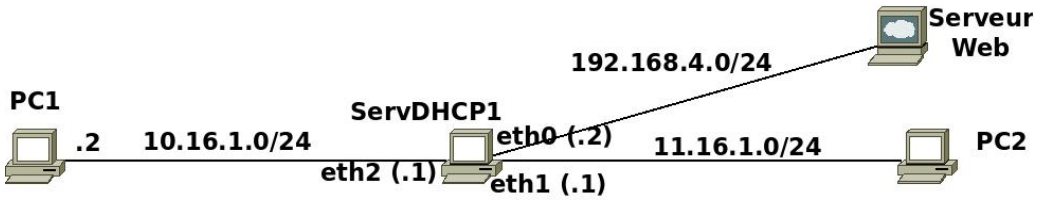
DHCP

Rappels

1. Dans **netkit**, le fichier **lab.dep** permet de définir l'ordre de démarrage des machines. Par exemple, si on a 4 machines **pc1, pc2, pc3** et **R** et on on veut que **R** démarre avant **pc2** et **pc3**, il faut mettre dans **lab.dep** la ligne suivante :
   `pc2 pc3: R`
2. La commande **ifdown eth0** permet de désactiver l'interface **eth0**.
3. La commande **ifup eth0** permet d'activer l'interface **eth0**.
4. Pour que l'adresse de l'interface **eth0** soit obtenue de façon automatique au démarrage, il faut ajouter au fichier **/etc/network/interfaces**, les lignes :
   ```
   auto eth0
   iface eth0 inet dhcp
   ```
5. Pour démarrer le service réseau, il faut taper la commande :
   `/etc/init.d/networking start`

Serveur DHCP

Construisez le réseau présenté par la figure suivante :



Remarque : dans netkit, le serveur DCHP s'appelle **dhcp3-server**. Les fichiers de configuration sont :

- **/etc/default/dhcp3-server**
- **/etc/dhcp3/dhcpd.conf**

1. PC2 et le « serveur web » obtiennent leurs adresses de façon automatique.

2. Donnez au « serveur web » l'adresse MAC : `08:00:27:73:B8:C9`.
Commande pour attribuer l'adresse MAC :
`ifconfig eth0 hw ether 08:00:27:73:B8:C9`

3. Configurez le serveur DHCP pour :

(a) qu'il soit un serveur principal ;

(b) qu'il joue aussi le rôle de routeur pour les différents réseaux ;

(c) que « eth0 » et « eth1 » affectent les adresses IP ;

(d) qu'il affecte :
- le domaine DNS : www.smi.ma
- les adresses IP des serveurs DNS : 196.10.1.1 et 196.10.1.2
- le masque de sous réseau : 255.255.255.0

(e) attribuer une adresse IP (quelconque) de type 11.16.1.N° à PC2.

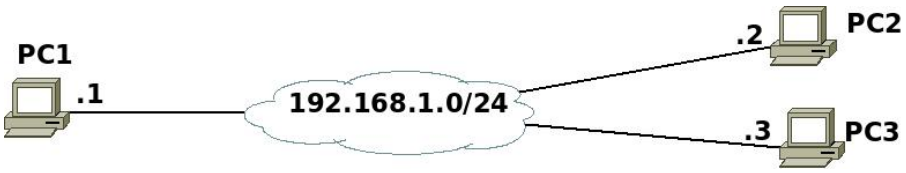
(f) attribuer l'adresse IP fixe (192.168.4.120) au serveur web.

TP numéro 4

FTP et SSH

Partie commune

1. Construisez le réseau présenté par la figure suivante :



2. Sur **pc1** :
   — créez l'utilisateur **smi** avec le mot de passe **smi**.
   — créez dans /**home/smi**, le répertoire « Test », dans ce répertoire, créez le fichier « **smi6.txt** », contenant le texte « Ceci est un test » ;
3. Sur **pc2**, créez le répertoire « **TestCopie** », dans ce répertoire, créez le fichier **smi6-copie.txt** , contenant le texte « Ceci est un autre test » ;

Partie FTP

1. Sur **pc3**, lancez la commande :
`tcpdump -s 1500 -A`
Retrouvez le mot de passe utilisé lors de la connexion par ftp.

2. Sur **pc1**, démarrez le serveur **ftp** (`/etc/init.d/proftpd start`).

3. Sur **pc2**, connectez vous par **ftp** au compte **smi** de **pc1**, puis fermez la connexion.

4. Sur **pc2** :
   — récupérez le fichier **smi6.txt** de **pc1** ;
   — copiez le répertoire **TestCopie** ainsi que son contenu sur le répertoire personnel de l'utilisateur **smi** de **pc1**.

Partie SSH

1. Sur **pc3**, lancez la commande :
`tcpdump -s 1500 -A`

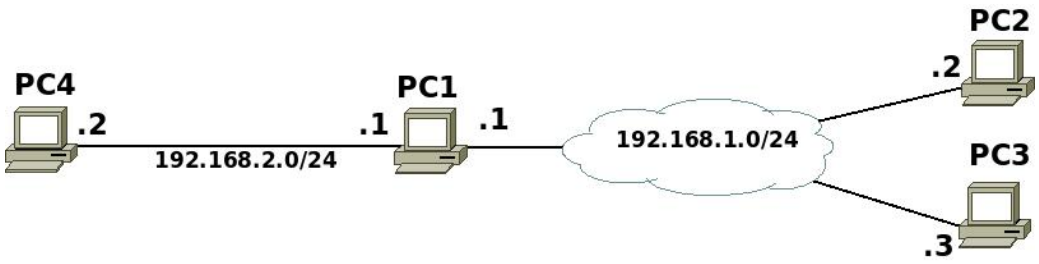
Est-ce que vous avez retrouvé le mot de passe utilisé lors de la connexion par ssh ?

2. Sur **pc1**, démarrez le serveur **SSH** (`/etc/init.d/ssh start`)
3. Sur **pc2**, connectez vous par **ssh** au compte **smi** de **pc1**, puis fermez la connexion. Commande :
   ssh smi@pc1 ou bien **ssh smi@192.168.1.1**
4. Sur **pc2** :
   — récupérez le fichier **smi6.txt** de **pc1** ;
   — copiez le répertoire **TestCopie** ainsi que son contenu sur le répertoire personnel de l'utilisateur **smi** de **pc1**.

TP numéro 5

NFS

Construisez et configurez les interfaces des **Pcs** du réseau présenté par la figure suivante :



1. Sur **pc1** :
   - créez l'utilisateur **smi** avec le mot de passe **smi** ;
   - démarrez le serveur **NFS** (`/etc/init.d/nfs-kernel-server start`) ;
   - configurez le serveur pour qu'il puisse autoriser **pc2** et **pc3** à exporter le répertoire **/home** en lecture et écriture ;
   - configurez le serveur pour qu'il puisse autoriser toutes les machines du réseau à exporter le répertoire **/tmp** en lecture seule ;
   - créez le répertoire « **/NFS_mnt** » et autoriser toutes les machines du réseau **192.168.1.0** à utiliser ce répertoire ;
   - affichez les informations sur les montages en cours (commande « **showmount** »), après chaque opération sur **pc2**.
   - testez la différence entre les options : **root_squash**, **no_root_squash** et **all_squash**.
2. Sur **pc2** :
   - démarrez le service **nfs-common** (pour que **pc2** puisse monter les répertoires distants) `/etc/init.d/nfs-common start`
   - Créez le répertoire « **Test** » et monter sur ce répertoire le répertoire **/home** de **pc1**. ;
   - après montage, essayez différents tests de lecture/écriture avec différents comptes (**root** et **smi**).
   - refaire la même chose avec le répertoire **/tmp** distant ;
   - pour chaque modification faite sur **pc1**, refaire les tests sur **pc2**.
3. Configurez **pc3** pour qu'elle puisse utiliser le répertoire **home** de **pc1** comme répertoire par défaut des utilisateurs. Le montage doit se faire de façon automatique au démarrage du système.
4. Dans **pc4**, testez le montage des différents répertoires de **pc1**.

TP numéro 6

Samba

Construisez et configurez les interfaces des **Pcs** du réseau présenté par la figure suivante :

1. Sur **pc1** :
- créez trois utilisateurs : **smi**, **sma** et **smia** ;
- démarrez le serveur **samba** (`/etc/init.d/samba start`) ;
- créez dans « **/home/smi** » un dossier portant le nom « TestSamba » et mettez dedans des fichiers. Configurez SAMBA pour que ce dossier soit partagé et utilisé par le seul utilisateur « **smi** ».
- Créez un dossier « /public » et partagez le pour un accès en lecture seule pour tous les utilisateurs et sans authentification.
- Configurer Samba pour que tous les utilisateurs puissent accéder à leurs dossiers personnels.

2. Sur **pc2** :
- Testez la connexion au dossier partagé « TestSamba ». Essayez la connexion avec les comptes **sma** et **smia**. Connectez vous avec avec **smi**.

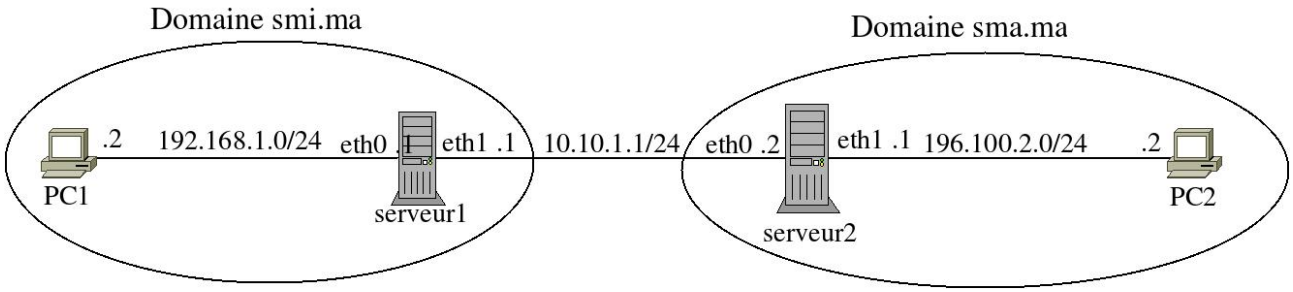
  a - Récupérez les fichiers contenus dans le dossier partagé.

  b - Créez dans ce dossier, un dossier « **Test1** ».
- Pour chaque utilisateur, testez la connexion à son dossier personnel.

TP numéro 7

DNS

Configurez le réseau suivant :

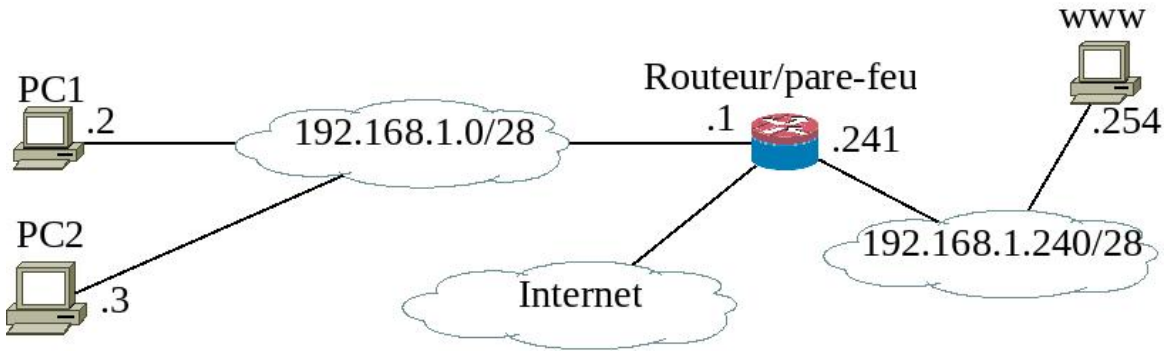


1. Configurer le **serveur1** pour qu'il joue le rôle de serveur DNS principal pour le réseau **smi.ma** et le **serveur2** pour qu'il joue le rôle de serveur DNS principal pour le réseau **sma.ma**.
2. Les différentes machines doivent communiquer entre elles (**routage statique**).
3. Testez les configurations à partir de PC1 et PC2.

TP numéro 8

Sécurité

Construisez et configurez les interfaces des **Pcs** du réseau présenté par la figure suivante :



1. Bloquez toutes les entrée/sorties et les forwards au **Routeur/pare-feu**.
2. Bloquez toutes les entrée/sorties au serveur web.
3. Autorisez les accès au serveur web.
4. Autorisez les PCs à accéder au web.
5. A partir de PC1, donnez les informations suivantes concernant le serveur web :
   — les services disponibles et leurs numéros de ports ;
   — l'adresse MAC.
   Indication : utilisez la commande **nmap**
   `nmap 192.168.1.254`