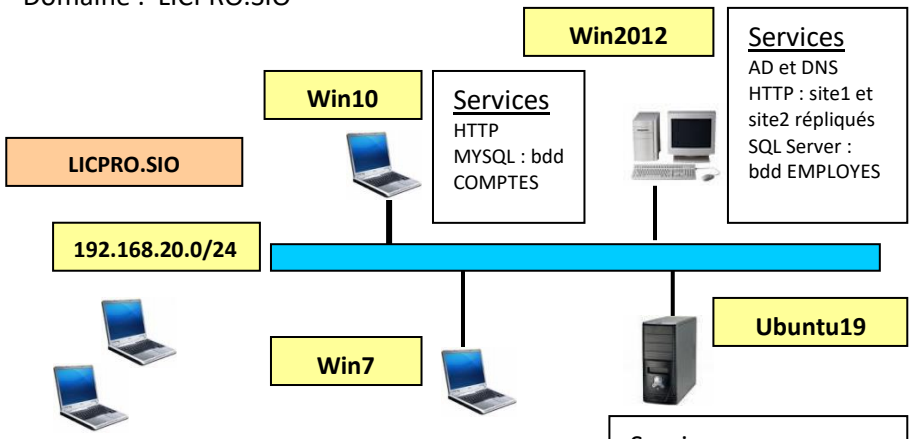
TP-0 Licence Pro SIO 2019/2020

H. TSOUNGUI

Vous travaillez dans une société de services en informatique et avez la mission de mettre en place une architecture réseau pour l'ensemble des utilisateurs (administratifs, développeurs et même stagiaires).

Fig. 1 Architecture réduite du réseau

Domaine : LICPRO.SIO



(Tous les ordinateurs ne sont pas représentés)

Pour l'adressage, on vous suggère d'utiliser le réseau local 192.168.20.0.

Travail à faire

-Mettre en place et tester le réseau TCP/IP

-Installer, configurer les différents services demandés et tester avec les clients adéquats.

-**Sécuriser les accès aux sites** site1.com et site2.com (quelques pages) que vous mettrez en place avec des **virtualhosts**.

-Mettre en place les réplications des bases de données proposées.

**Les ressources partagées (partages)

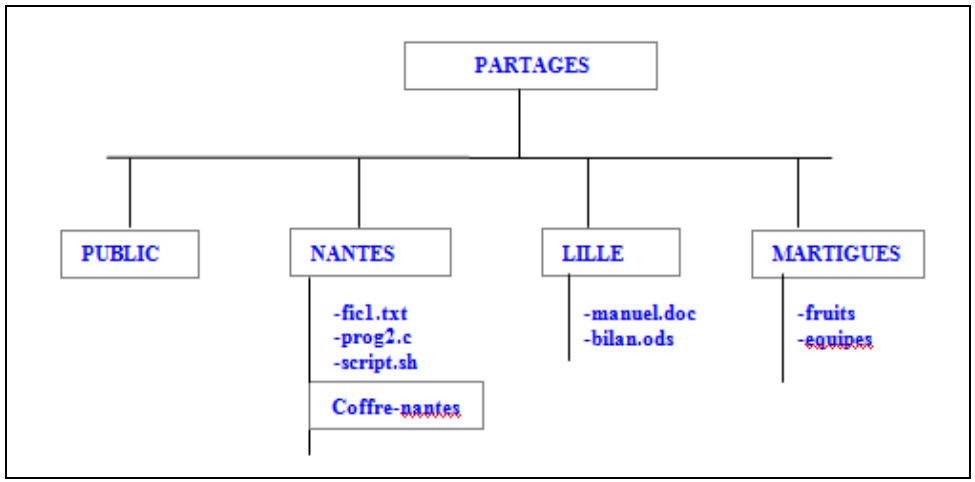


Fig. 2 Ressources

Les **groupes d'utilisateurs AD et linux et les accès aux ressources

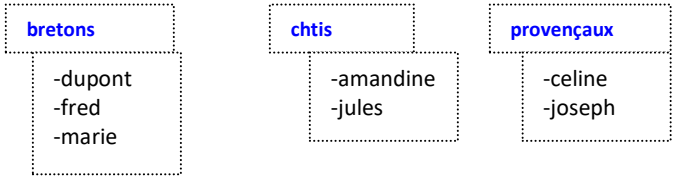


Fig. 3 Utilisateurs

* Les groupes ont par défaut, le droit d'écriture sur leurs fichiers et dossiers respectifs : les bretons peuvent tout faire dans la ressource partagée NANTES. Les chtis dans LILLE, etc. Le dossier PUBLIC doit être accessible à tous en lecture/écriture et être **browsable**.

TP-1 Licence Pro SIO 2019/2020

services DNS, mail et SMB/CIFS

- ----------

*** Cette deuxième partie est à rendre en binôme ou seul ***

- ----------

1.1 Installer et configurer un serveur **DNS primaire** (avec BIND) sur la machine linux. On y fera référence à au moins trois machines du réseau (même si elles n'existent pas en réalité).
-Les tests de résolution directe et inverse seront faits avec
* **nslookup**, **host** et **ping**.

1.2 Pour des raisons de sécurité, configurer, si ce n'est pas encore fait depuis Active Directory, le serveur windows 20XX en deuxième serveur DNS (principal et non secondaire).

1.3 Sur le serveur linux :
-installer un **service de messagerie** avec POSTFIX et DOVECOT-POP3d ou POSTFIX et COURIER-IMAP4
-créer les BAL (boîtes aux lettres) pour les utilisateurs des groupes CHTIS et BRETONS
-réaliser l'échange de messages entre utilisateurs et groupes :
* jules → fred
* amandine → bretons
* dupont → amandine
* joseph → chtis

**** Fournir les captures de ces échanges ****

1.4 Toujours sur le serveur linux, mettre en œuvre les **partages SMB/CIFS** nommés
* PUBLIC, accessible à tous en lecture et écriture
* LILLE accessible aux membres du groupe CHTIS sans restriction
* MARTIGUES, accessible au groupe **provençaux** en lecture mais, seul joseph et root peuvent y écrire

NB : tous ces partages doivent être visibles dans le voisinage réseau de toutes les machines du réseau (domaine LICPRO.SIO).

****

**** Il sera tenu compte de la présentation de vos CR dans la notation **

Tous les comptes rendus sont à adresser à
Henri.tsoungui@uphf.fr
ET
htsoungui@sfr.fr
ainsi qu'à vous-mêmes en copie CC.

TP-2 Licence Pro SIO 2019/2020

Routage IP, Filtrage avec iptables et supervision des services

Domaine : LICPRO.SIO

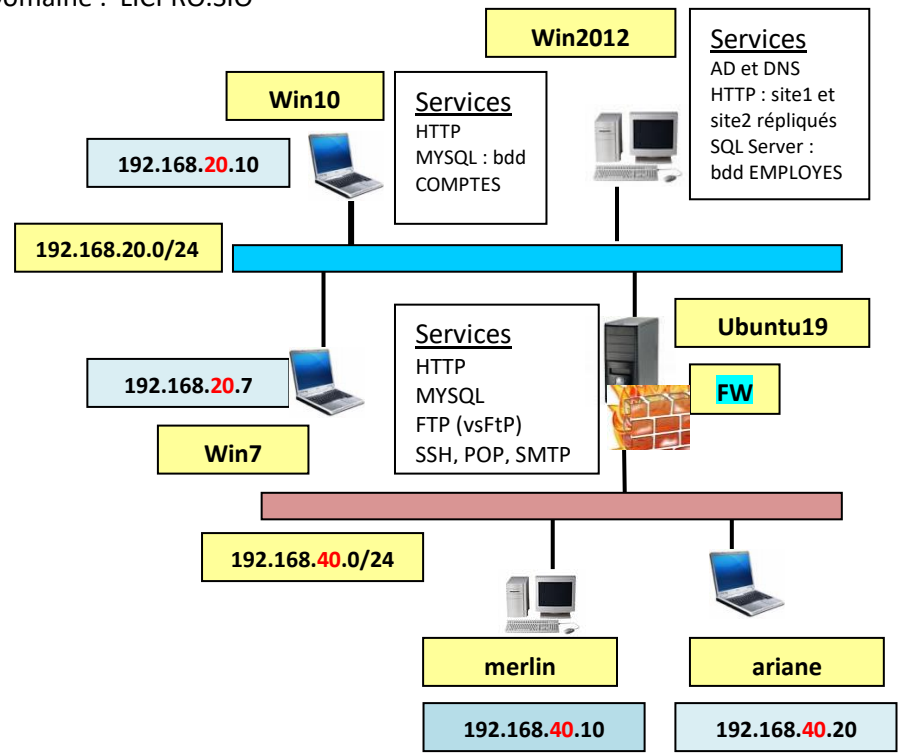


Fig. 2 : nouvelle architecture du réseau

++

RAPPEL

Tous les comptes rendus sont à adresser à
Henri.tsoungui@uphf.fr ET htsoungui@sfr.fr
ainsi qu'à vous-mêmes en copie CC.

Travail à faire

Dans cette dernière partie, la machine ubuntu19 précédente est connectée à un deuxième réseau d'adresse 192.168.40.0.

1)-Routage :mettre en œuvre le routage (RIP) pour permettre (ou interdire) la communication entre les deux réseaux. Ex : accéder au site2 de win2012 à partir de merlin. Pour tester cette fonctionnalité, vous ferez non seulement des tests ICMP mais aussi des accès à des services se trouvant de part et d'autre de la machine ubuntu19.

2)-Filtrage TCP

Ex : Bloquer tous les paquets TCP/UDP de 192.168.20.10 à destination de 192.168.40.20.

2.1)-Installer les services réseau proposés WEB/Apache, MySQL, MAIL/Postfix et FTP quelconque sur ubuntu19 (ou un autre linux).

2.2)-Mettre en œuvre le **filtrage** TCP/UDP en utilisant

-l'outil GUFW, interface de configuration de **Netfilter** (intégré au noyau) mais de préférence l'utilitaire ***iptables*** en ligne de commande ou fichier de configuration à exécuter

-Tester le respect des règles dans plusieurs cas.

Exemples de règles de filtrage à paramétrer et tester avec **iptables**.

Destination	Source	Protocole	Port	ACTION
192.168.20.10	192.168.40.19	TCP	80	ACCEPTER
192.168.20.10	192.168.40.10	ICMP	-	REFUSER
192.168.40.10	192.168.20.10	TCP	3306	ACCEPTER
192.168.40.20	192.168.20.10	TCP	3306	REFUSER
*	*	*	*	REFUSER

3)-Mettre en service un **système de surveillance/monitoring** des services par ubuntu19 à l'aide de l'un des outils suivant **icinga2** ou **zabbix**.

-Il faudra ***monitorer au moins 4 services***, une charge de CPU et un espace disque ou de partition de l'architecture.