Communications entre ordinateurs

- Principaux éléments d'un ordinateur
- Comment accéder aux données ?
- Labo basé sur des protocoles applicatifs utilisés en entreprise :
  - RDP
  - SCP
  - SMB
  - LDAP
- Prérequis
  - Sécurité des Systèmes d'Information
  - Virtualisation

Eléments d’un ordinateur (PC) – vue en couches

- **Interface Homme Machine**

  Command Line Interface Graphic User Interface Web UI

- **Système de fichiers**

  FAT, NTFS, Ext3/4, Btrfs, GoogleFS, GlusterFS, …

- **Matériel**

  CPU, …, Disque, NIC (Ethernet), USB devices, …, iSCSI

- **Protocoles de communication**

  next slide

Comment accéder aux données ?

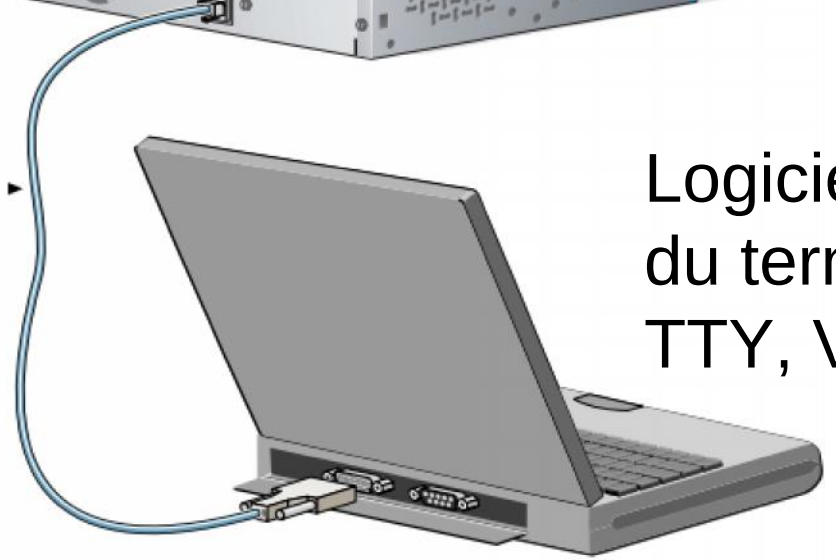
- Terminal alphanumérique
- Telnet → voir Labo Hacking – Sécurité 2ème
- Secure Shell (SSH) → semaine précédente
- Remote Desktop Connection → Labo §1 RDP
- File transfer → ftp, Secure Copy (SCP) → Labo §2 SCP
- Messagerie
- File access → cifs-smb, nfs, …, Labo §3 Samba & Labo §4 LDAP
- Data query → SQL, …
- Web UI → http

- … firewall, droits d'accès, gestion centralisée (annuaire LDAP, AD)

Terminal alphanumérique (physique / émulé)

- avec clavier – écran mais sans système de fichiers

Switch Cisco 2950

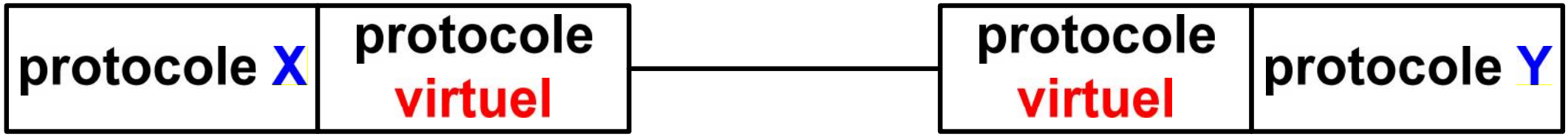


Logiciel d'émulation du terminal physique TTY, VT100, …

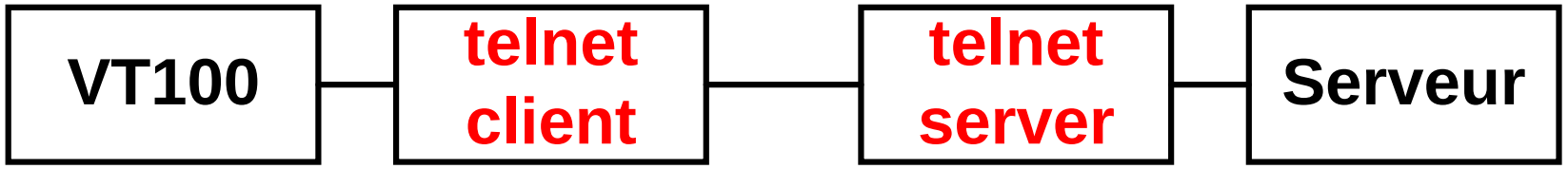
- Liaison asynchrone (1 start bit – 8 data bit – 1 stop bit) à 9600 bit/s
- Débit binaire max = 115 kbit/s
- Mode de transmission standard avant Ethernet (~1985)

Telnet

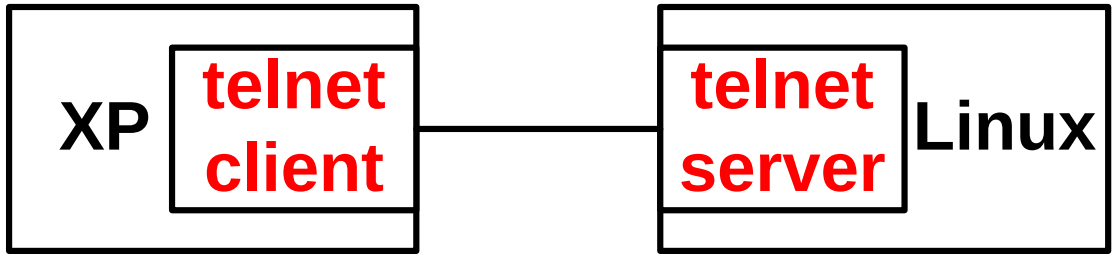
- Architecture hétérogène → Terminal supportant le protocole X – Serveur supportant le protocole Y



- Le protocole telnet (client - serveur) a été conçu pour permettre la communication entre terminal physique et serveur

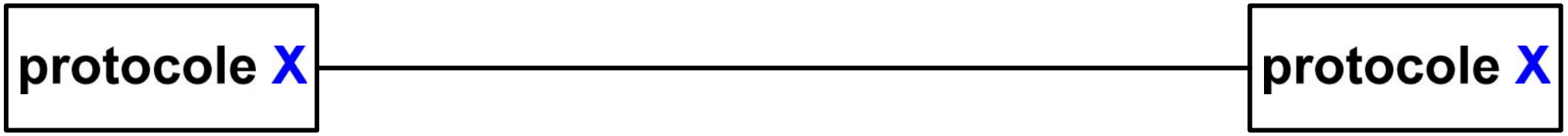


- Il permet aussi l'accès à distance (remote access) via internet

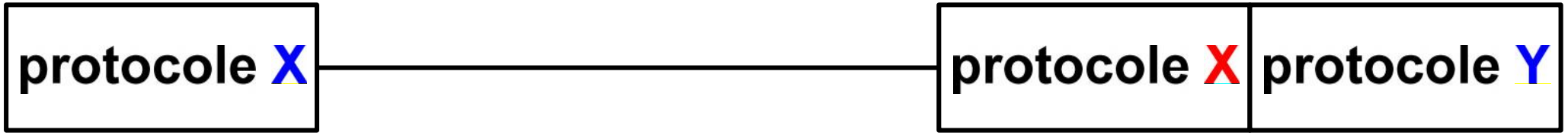


Architectures homogène & hétérogène

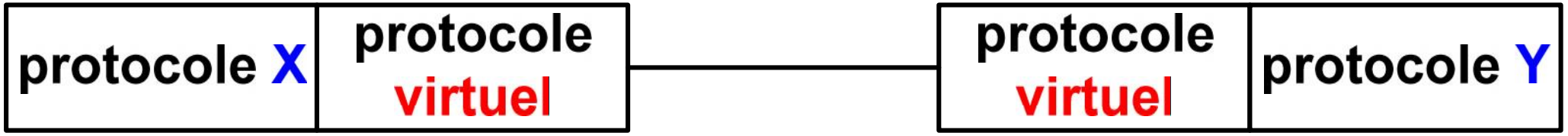
Architecture homogène



Architecture hétérogène et émulation



Architecture hétérogène et concept virtuel



Utilité des protocoles RDP, Citrix, Spice, VNC, …

- Administration à distance des serveurs Windows (Domain controller, messagerie Exchange, virtualisation Hyper-V, …)

  http://www.tdeig.ch/windows/Jardon_RTB.pdf

  http://www.tdeig.ch/windows/Korso_RTB.pdf

- Terminal server → next slides

  HP thin client
  http://www.intel.com/content/www/us/en/nuc/nuc-thin-client.html

- Développement d'un client léger low cost par Lionel Schaub

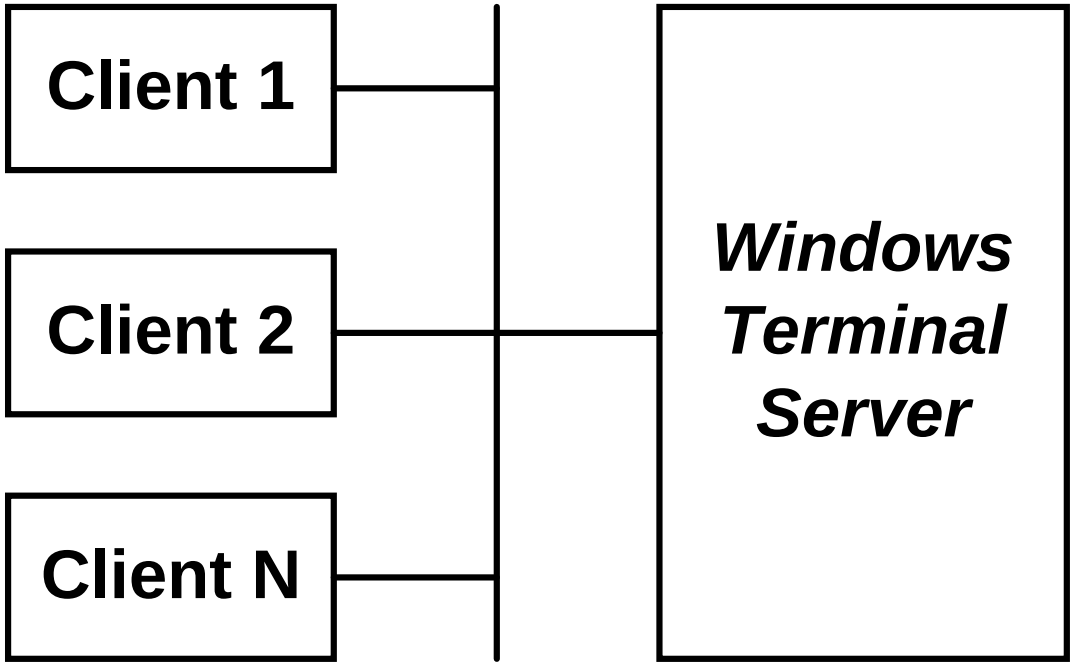
  Système minimum basé sur CPU Atom – 2 GB RAM) sans disque mais avec clé USB et la distribution Linux Core Plus

  → Annexe 1 = Labo optionnel Virtual Desktop avec Spice

Thin client (1)

- L’architecture thin client (client léger) n’est en fait qu’une évolution du modèle précédent capable d’offrir une interface graphique avec système de fenêtres

- La figure illustre 3 utilisateurs qui accèdent à un serveur MS en mode GUI (Graphical User Interface)



- Il est aussi possible d’accéder à distance (remote access) via internet à son poste de travail d’entreprise

Thin client (2)

- Minimum de fonctionnalité (clavier - écran) côté client
  → Administration simplifiée du poste client (DHCP, …)

- Chaque application (Word, …) n'est installée qu'une seule fois côté serveur

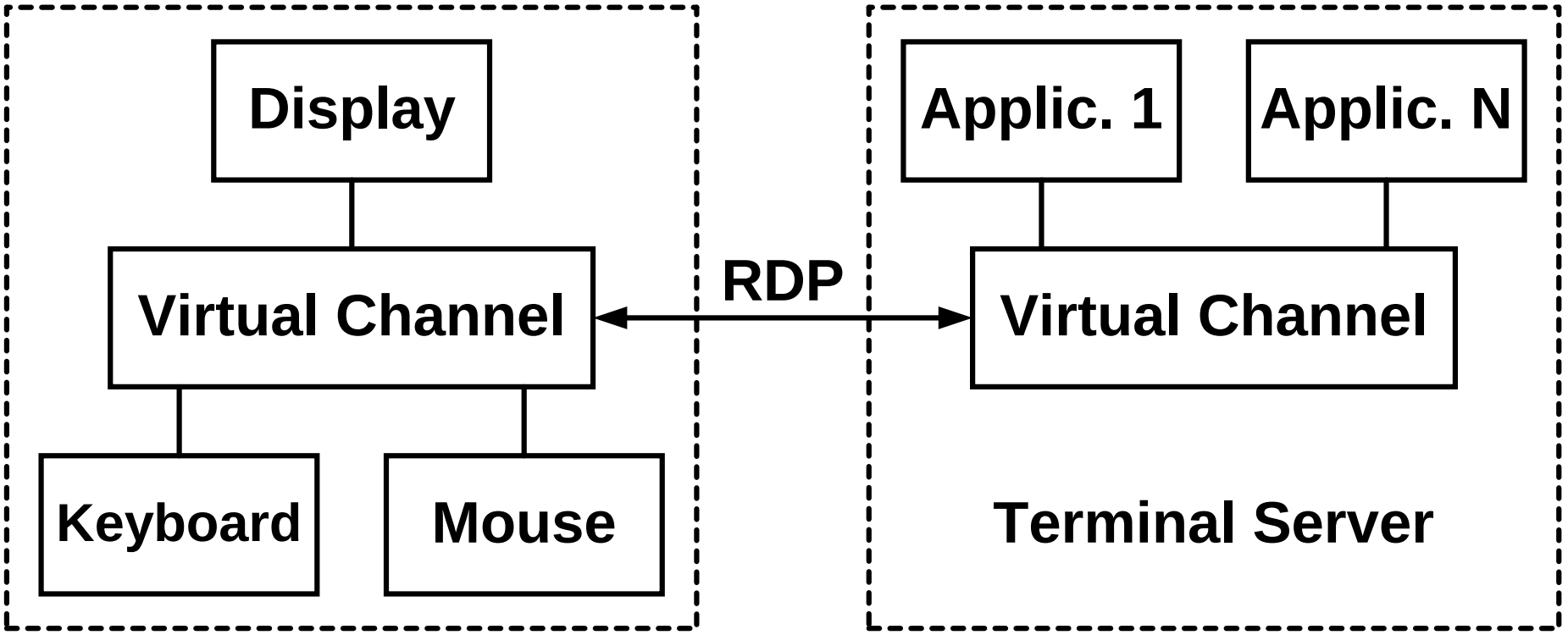
- Aucune donnée personnelle mémorisée sur le poste qui ne possède pas de mémoire de masse

- Unicité des données garantie quel que soit le poste client (poste de travail dans l'entreprise, PC à domicile, portable, PDA, …)

- Produit leader → http://www.citrix.com/

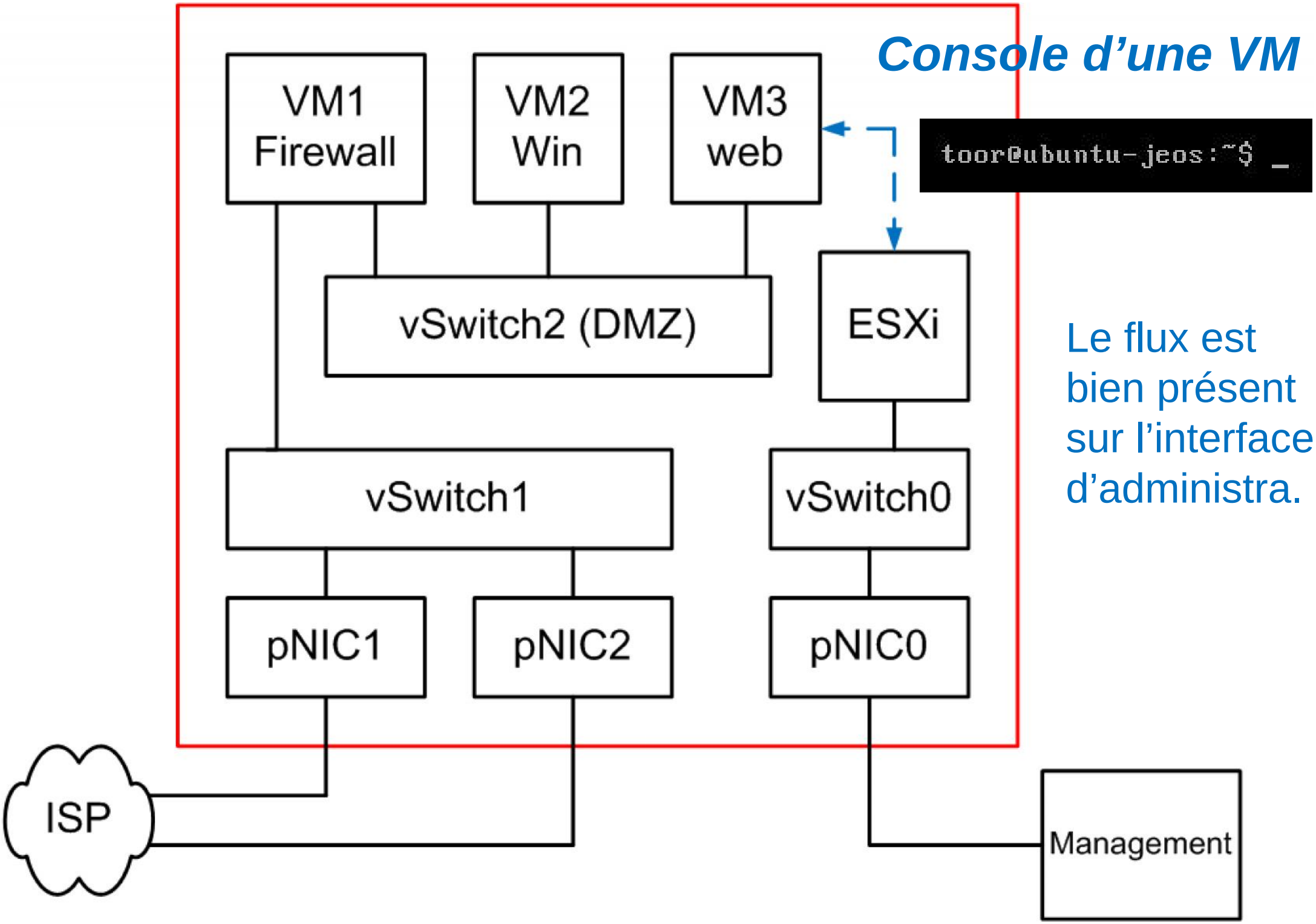
Thin client (3)

- Le protocole RDP (Remote Desktop Protocol) transmet les commandes (clavier, souris) ainsi que les écrans (bitmap) à afficher



- Equivalent Linux = VNC, Spice → Labo VDI (en réserve)

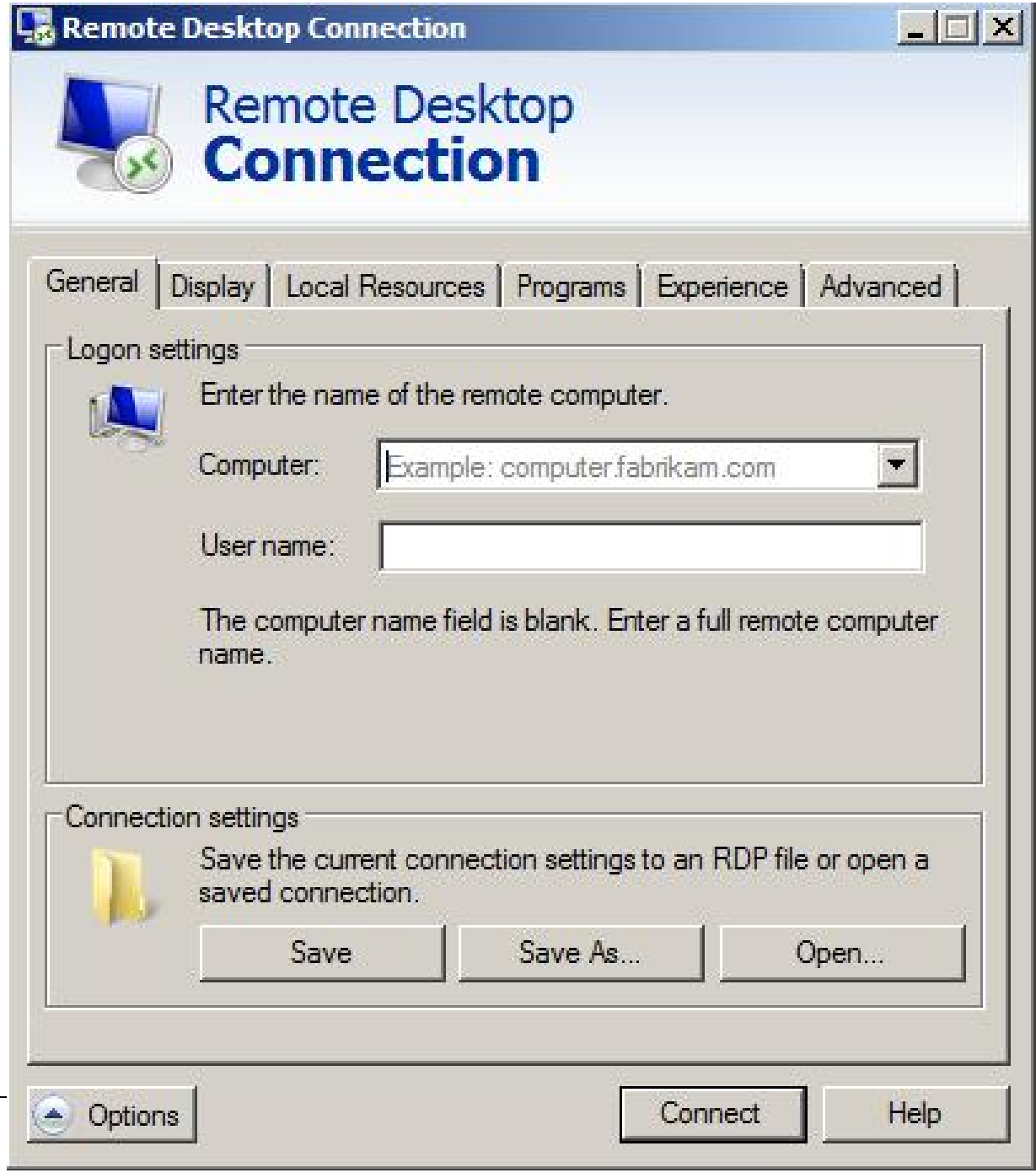
Console d'une VM



Le flux est bien présent sur l'interface d'administra.

Labo §1 : Remote Desktop Connection (20 min)

- Accéder à XP depuis Win7
- Créer un compte membre du groupe Bureau à distance
- Autoriser l'accès distant sur XP
- Le client MS (XP, …) est limité à une session distante

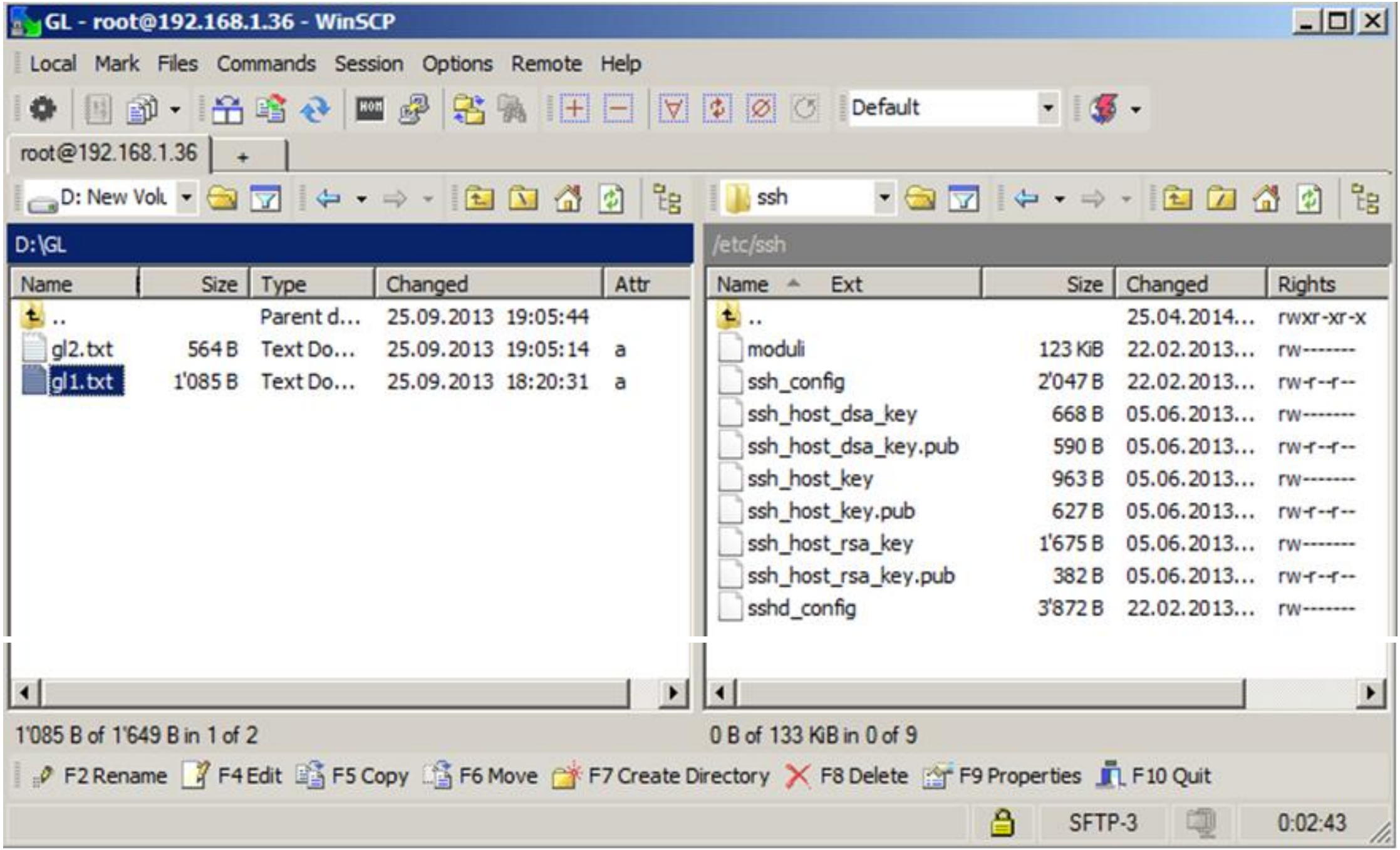


Administration du serveur 10.2.1.1

- Serveur de fichiers du labo (SMB et nfs)
- Basé sur CentOS **sans GUI → simplicité & sécurité**
- Fichiers = doc. labo, ISO, appliances ESXi, images Windows, …
- Dépôt Linux
- Serveur PXE avec listes des adr. Eth (salles A408 & A409)
- Script pour installation automatique des 20 PCs

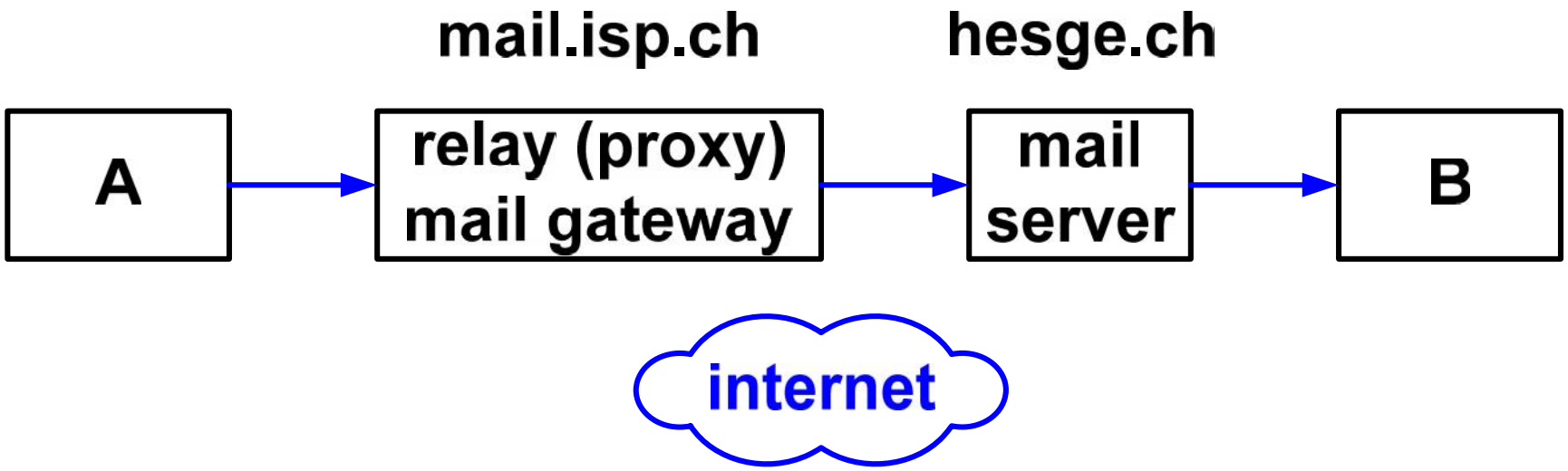
- Administration depuis Win7 avec PuTTY et WinSCP (next slide)

Labo §2 : Secure Copy Protocol (10 min)



Messagerie

- A envoie un message destiné à B

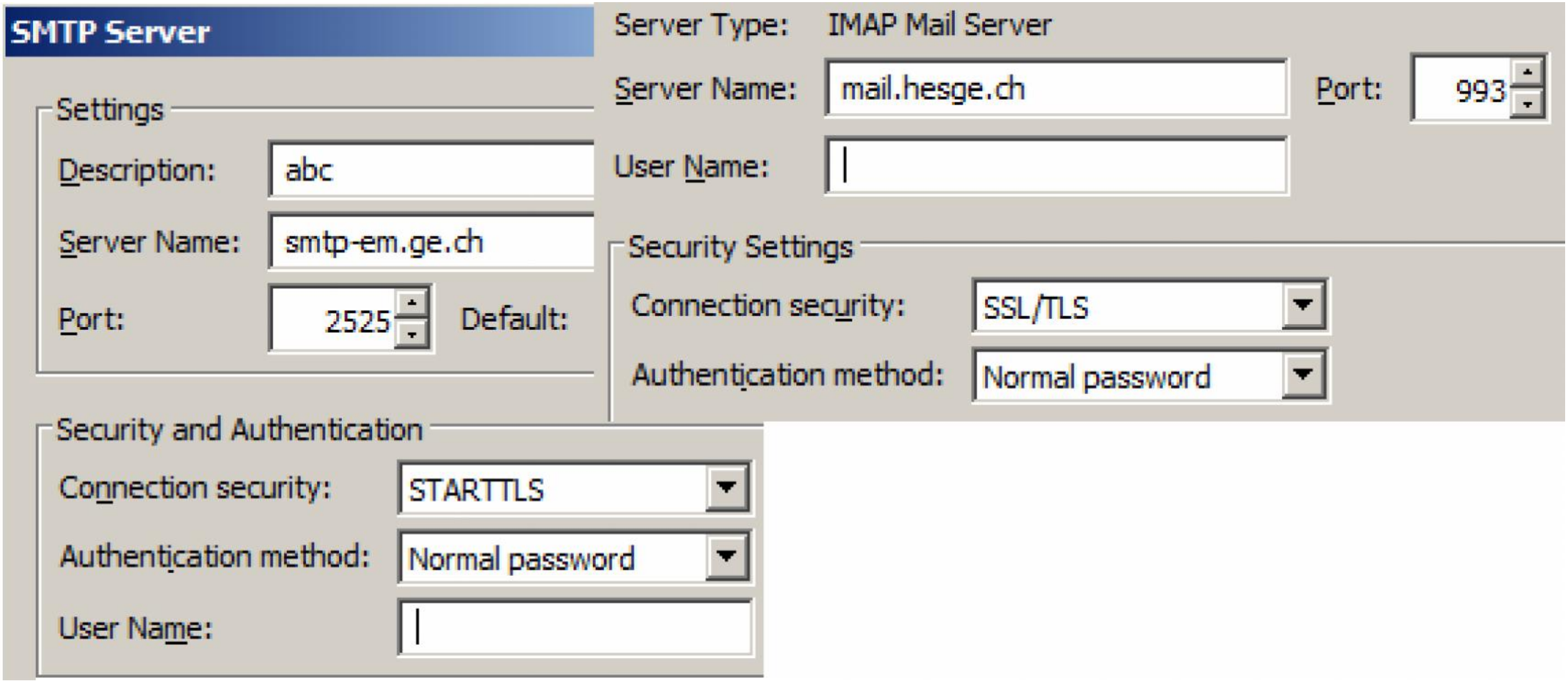


- A et B ne sont jamais connectés (TCP) → offline connexion
- A et B peuvent être éteints
- Adresse IP du serveur hesge.ch via mécanisme DNS (MX)
- Protocoles SMTP, POP et IMAP
- Utilisateurs préfèrent parfois le WebMail
- Utilisé souvent pour faire du transfert de fichiers (attachés)

Ma messagerie Thunderbird

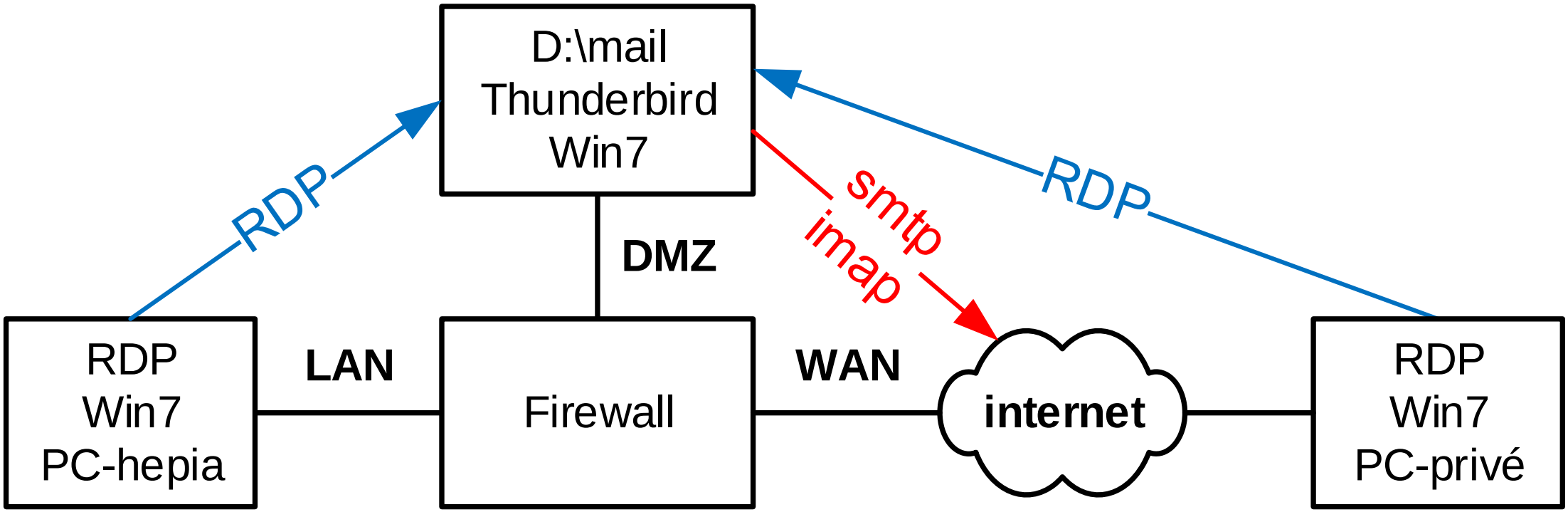
Emission (SMTP)

Réception (IMAP)



Mon système de messagerie

- Accessible depuis 2 PCs (hepia + domicile)
- 2 comptes de messagerie (prof + privé)
- 2-4 Gbyte emails stockés en local + sauvegarde
- Webmail comme solution de secours



File Access

- Imaginons un fichier unique stocké sur le serveur et plusieurs clients autorisés à le lire et ou le modifier
- Un mécanisme de verrou (lock) va permettre de résoudre les conflits en écriture et d'améliorer l'interactivité grâce à des caches
- Des protocoles comme CIFS, SMB ou NFS supportent ces mécanismes
- L'application doit être capable de gérer ces verrous de façon transparente pour l'utilisateur
- L'éditeur Word de MS ne supporte pas cette fonctionnalité
- http://msdn.microsoft.com/en-us/library/windows/desktop/aa365433(v=vs.85).aspx
- http://pic.dhe.ibm.com/infocenter/zos/v1r12/index.jsp?topic=%2Fcom.ibm.zos.r12.idan400%2Flockv4.htm
- http://beej.us/guide/bgipc/output/html/multipage/flocking.html Démo

SMB – CIFS

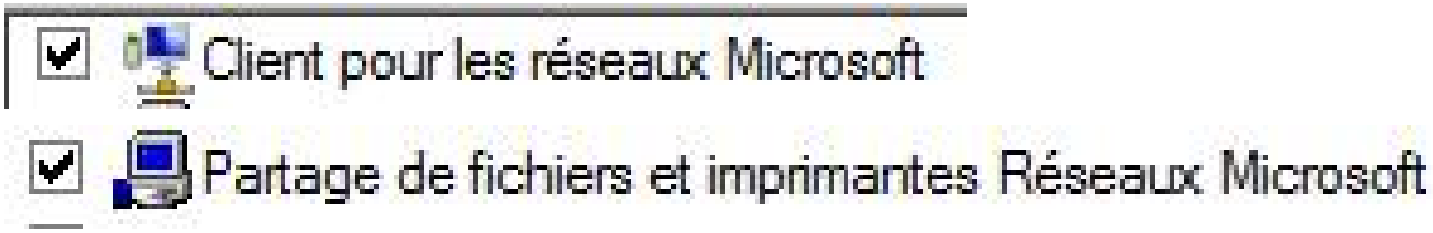
- Le protocole SMB (Server Message Block) a beaucoup évolué depuis sa création par IBM en 1985
- En 1997, MS publie une rfc CIFS (Common Internet File System)
- SMB permet le partage des ressources (fichiers & imprimantes) dans un environnement réseau Windows appelé **Workgroup**

  → Control Panel – System
- Le client doit s'authentifier pour chaque session qu'il désire établir avec Server_1, Server_2, …
- Il doit donc posséder un **compte local sur chaque serveur** qu'il désire utiliser
- Variante = Domaine non abordé dans ce cours
- SMB comprend une multitude de dialectes introduits avec XP, Win7, …, Server 2003, Server xxx

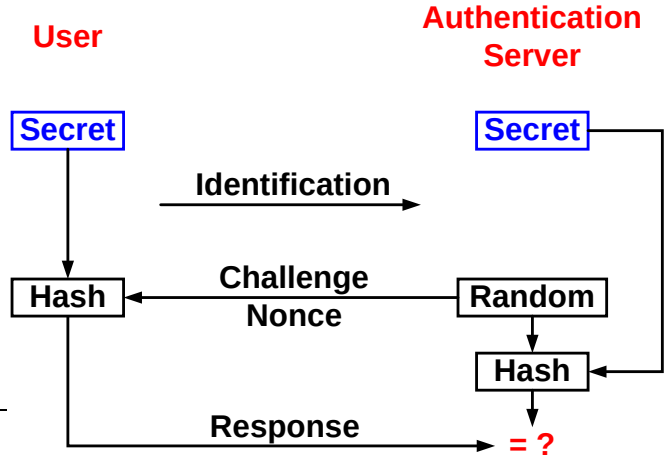
SMB (suite)

- **//10.2.1.1** active le protocole http du côté client
- Un navigateur ne supporte pas que ce protocole → ftp: ldap: …

- **\\10.2.1.1** active le protocole SMB
- Client
- Server



- Applications = partage de fichiers (file sharing)
- Attributs pour le client = lecture – écriture – exécution (NTFS)
- Authentification du type challenge-response



Labo §3 : Configuration du serveur Samba (10 min)

- Logiciel libre GNU http://www.samba.org/ déjà installé

- Etudier les commandes

```
setenforce 0                          Désactiver SELinux
adduser jean
passwd jean
mkdir /home/doc
chmod -R 777 /home/doc
smbpasswd –a jean
copier /etc/samba/smb.conf            avec WinSCP
service smb start
service nmb start
```

LDAP

- Lightweight Directory Access Protocol
- Annuaire (téléphonique, DNS, …)
- Structure hiérarchique (attributs) → schéma (modèle de nomage)

  ou = ITI3 uid = jean
- Annuaire =/= Base de données

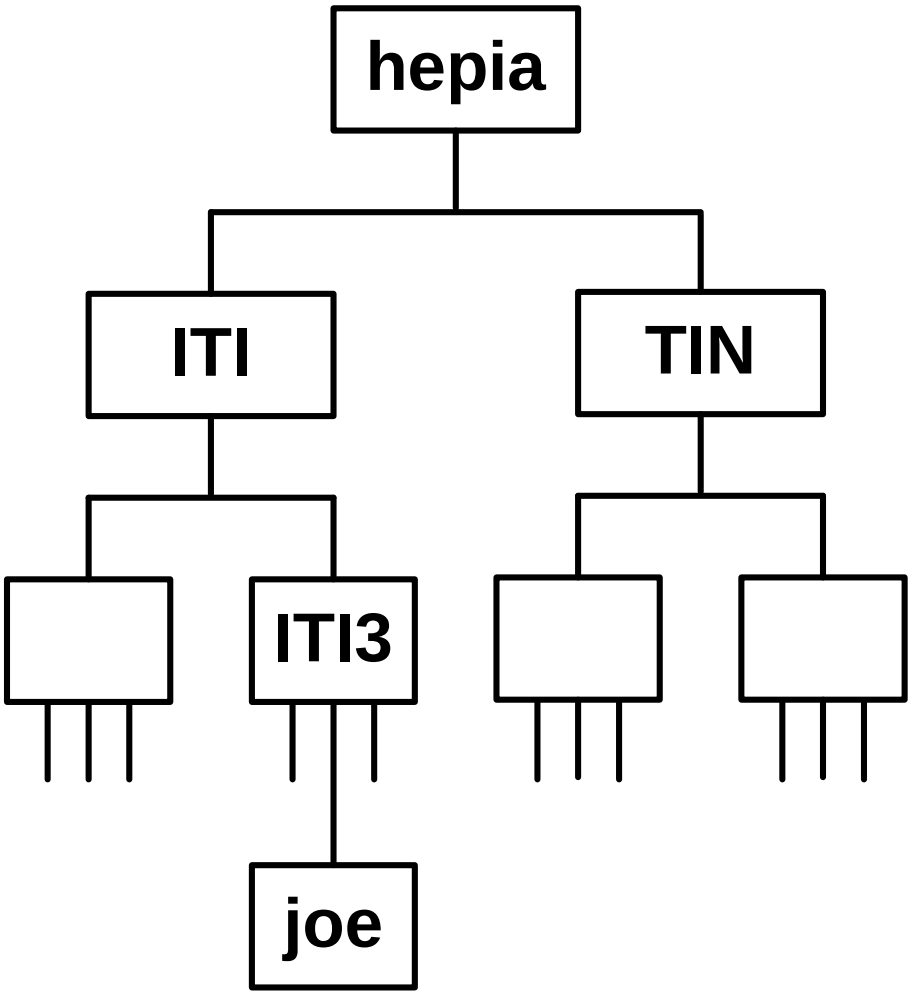
  Facilement extensible

  Rapport lecture / écriture élevé

  Performances élevées
- Protocole : search, compare, add, delete, …
- http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Modèle de nommage LDAP

	attribut
domain	dc
organization unit	ou
organization unit	ou
user identifier	uid



Labo §4 : Annuaire LDAP (10 min)

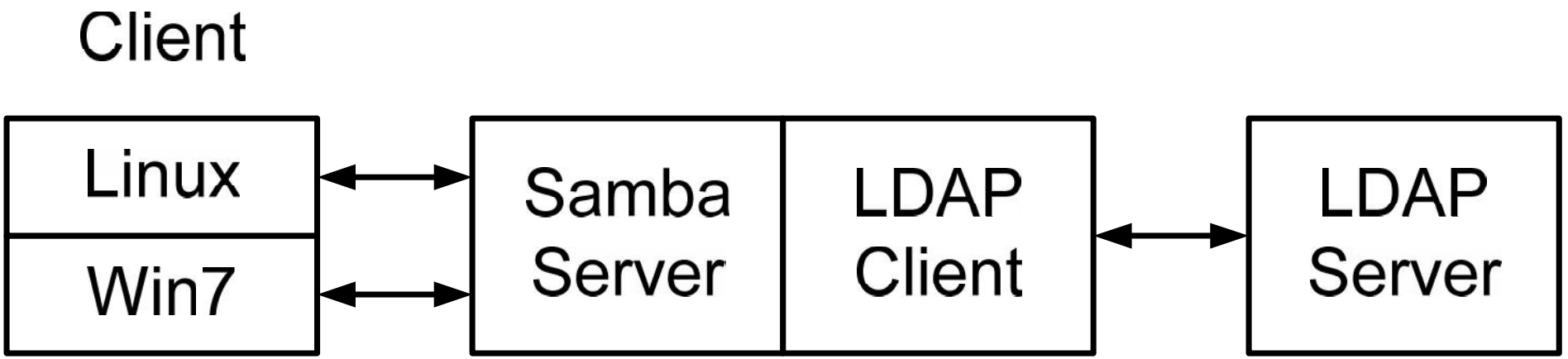
- Utiliser l'outil webmin → http://www.webmin.com/

- Tester avec le navigateur IE

  ldap://192.168.56.117/dc=tdeig,dc=labo??sub?(sn=johndoe)

Labo §5 : Samba-LDAP (20 min)

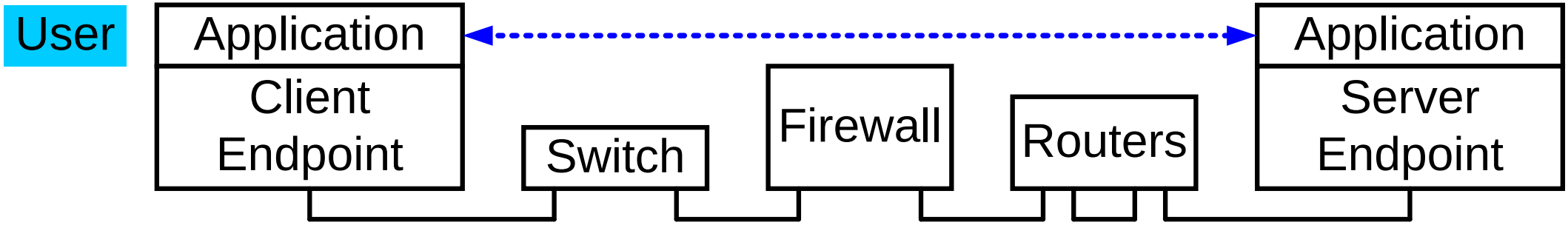
- Le serveur LDAP valide les demandes d'authentification destinées au serveur Samba



- Etapes :
  - Créer un dossier partagé
  - Utiliser l'outil SWAT (Samba Web Admin Tool)
  - Créer un compte dans l'annuaire
  - Tester depuis clients Linux & Win7

Performance réseau

- Modèle en couche



- Paramètres à estimer et à mesurer → cahier des charges

  Utilisateur :

    Débit utile (Mbyte/s) lors d'un transfert de fichier

    Temps de réponse (ms) d'un site web

  Réseau :

    Temps de latence d'un commutateur Ethernet, d'un firewall

    Débit binaire (Gbit/s)

  Endpoint :

    Charge CPU, RAM, …, ressources matérielles

Définitions

- Débit binaire (Gbit/s)

  Nombre de bit émis par seconde sur un câble Ethernet
- Round Trip Time (RTT en ms)

  Temps de réponse de la couche réseau mesurée avec ping
- Temps de latence (ms)

  Retard (inertie) produit par un commutateur Ethernet
- Response Time (ms)

  Temps de réponse d'une requête http mesuré avec Wireshark
- Throughput (Mbyte/s)

  Volume de données utile (fichier) transférer par seconde