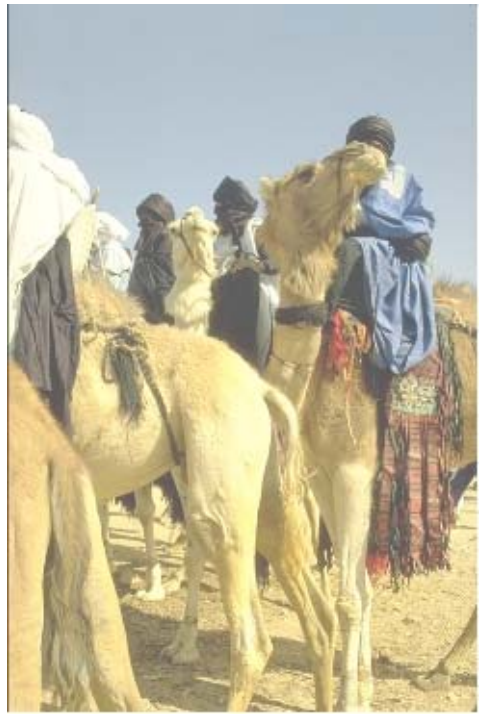
Nomadisme à l'IN2P3



Wikipédia : Le nomadisme est un mode de vie [... où] la quête de nourriture motive les déplacements des hommes.

Nomadisme à l'IN2P3

- Différents profils de nomades à l'IN2P3
- Différents besoins pour les nomades
- Fonctionnalités déployés pour les nomades

Profils de nomades IN2P3

- Mobile dans son laboratoire
  - Demande forte pour avoir l'accès au réseau partout dans le laboratoire : salles de réunion, salles de conférence. VMPS et Wi-Fi
- Mobile à l'extérieur de son laboratoire
  - Les nomades veulent rester en contact avec leur laboratoire quand ils sont à l'extérieur. SSL, SSH, VPN.
  - Ils veulent retrouver leur environnement de travail (à l'identique) quand ils sont à l'extérieur.
  - ***Les données contenues sur leur portables doivent être sauvegardées.***

Profils de nomades

- De l’ordre de 1000 PC portables dans l’Institut
- Majorité sous Windows, puis MacOS et quelques Linux

Profil des nomades accueillis à l'IN2P3

- Accueil de visiteurs et congressistes
  - Les visiteurs de nos laboratoires demandent aussi l'accès à Internet
    - A partir du réseau filaire
    - Et surtout à partir du réseau Wi-Fi

Fonctionnalités déployées à l'IN2P3 pour les nomades

1 - Mobilité sur le réseau local
- VMPS pour la mobilité sur le réseau filaire à l'intérieur du laboratoire et l'accueil des visiteurs dans un VLAN dédié.
- Wi-Fi pour plus de mobilité à l'intérieur et pour l'accueil de visiteurs.

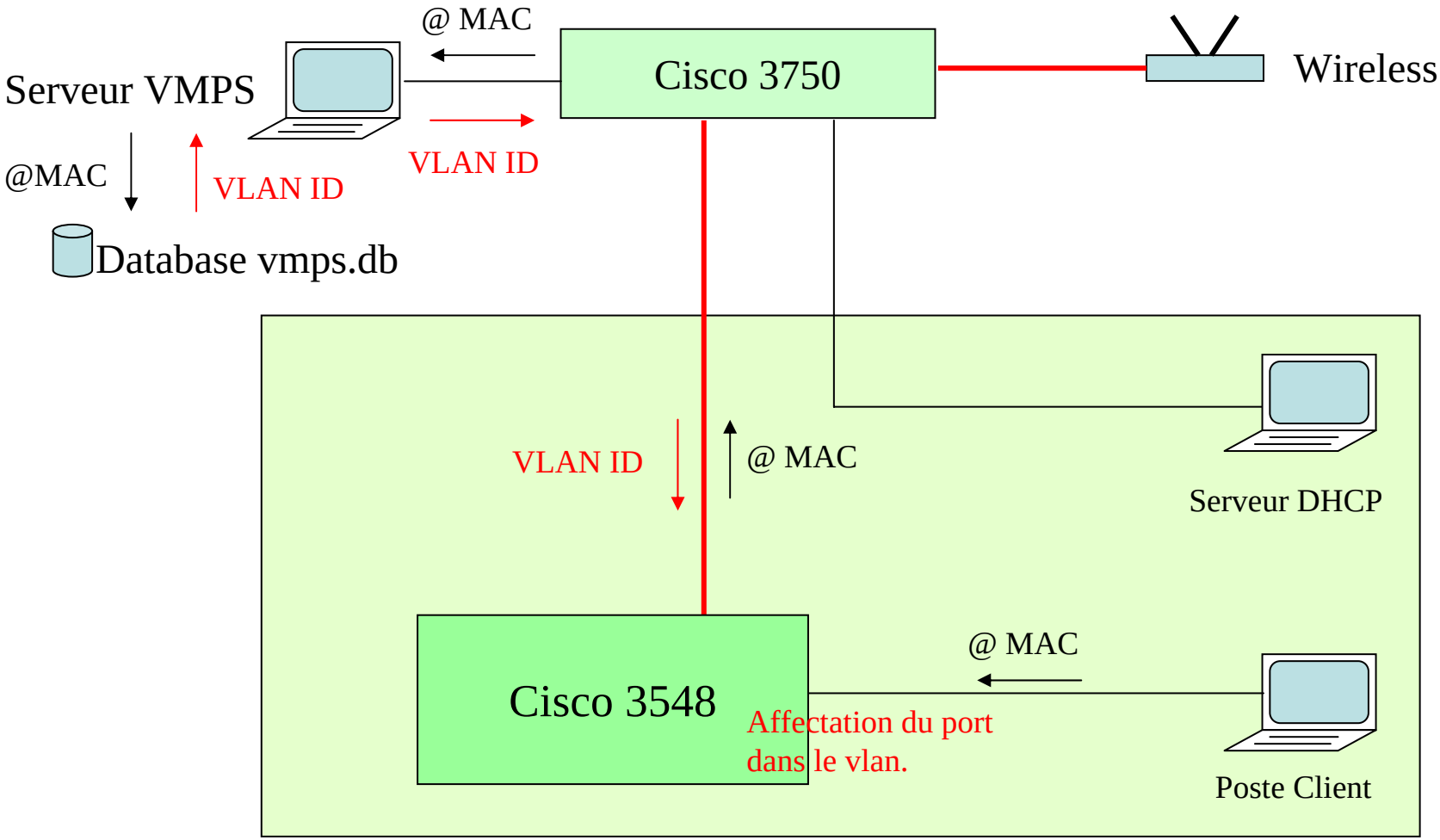
2 - Accès externes
- SSL pour des accès sécurisés aux services standards
- VPN pour les accès distants aux ressources internes.

3 - Fonctionnalités liées au système d'exploitation Windows
- La Forêt Active Directory IN2P3 permet la mobilité à l'intérieur de l'IN2P3
- Windows XP offre une synchronisation efficace des données sur les serveurs

1 - Mobilité sur le réseau local VMPS 1/4

- VMPS : Vlan Membership Policy Server
- Affectation dynamique d’un VLAN en fonction de l’adresse MAC
- Solution propriétaire CISCO

1 - Mobilité sur le réseau local VMPS 2/4



1 - Mobilité sur le réseau local VMPS 3/4

- Nécessite un serveur VMPS : Catalyst 5000/6000

ou

- Produit libre : http://vmps.sourceforge.net
- Base de données : fichier texte vmps.db
- Fonctionnalité utile le *fallback*

1 - Mobilité sur le réseau local VMPS 4/4

- Fichier vmps.db

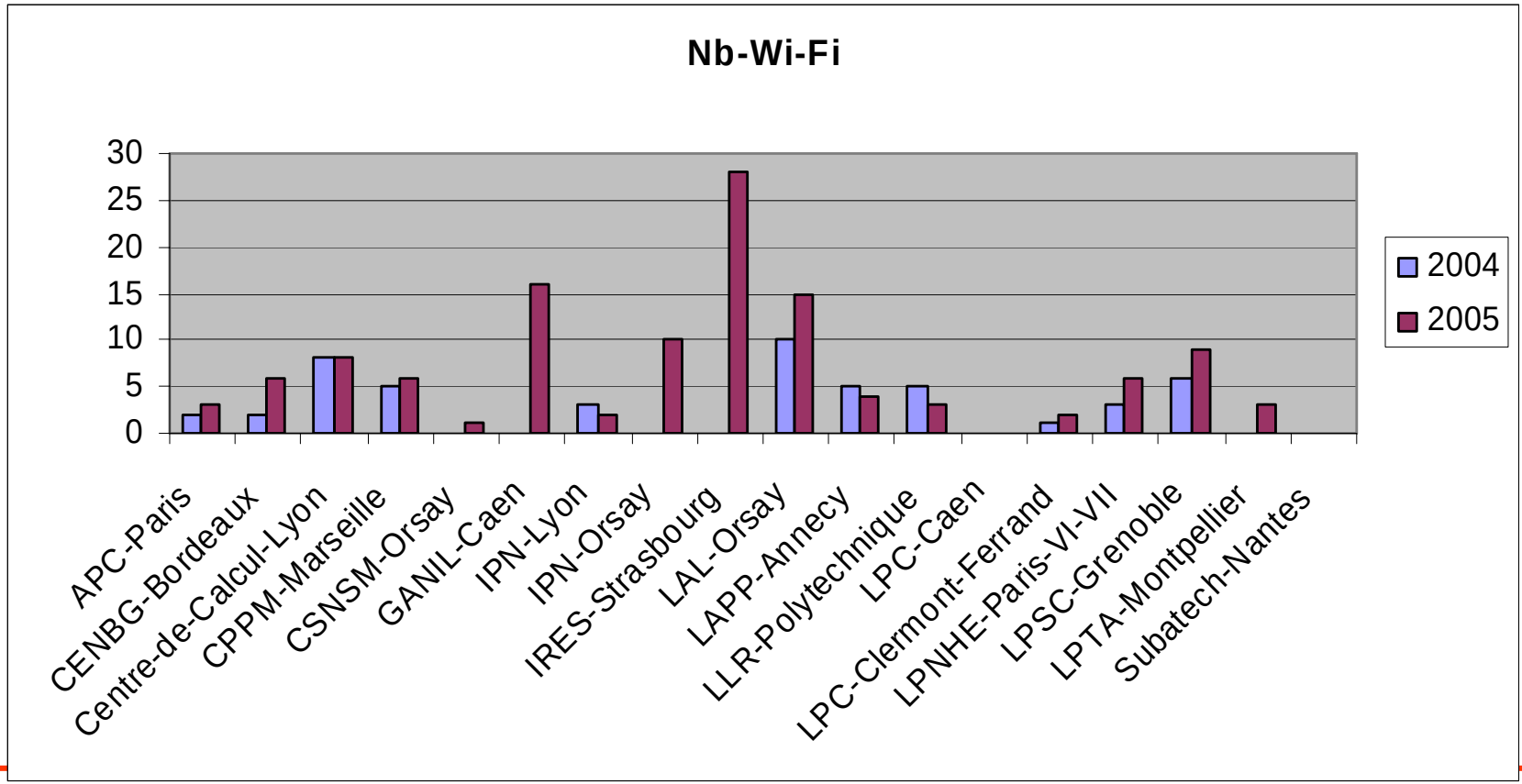
```
vmps domain DOMAIN-LPSC
vmps mode open
vmps fallback VLAN-VISITEURS
vmps-mac-addrs
!!
!  isngrid1 134.158.40.65
address 0000.1cb5.a83a vlan-name VLAN-LPSC
!
!  isnutl1 134.158.47.72
address 0020.4a34.2fa5 vlan-name VLAN-UTL
!
!  isnpc0161 134.158.40.161
address 0010.dc08.abfc vlan-name VLAN-LPSC
!
!  isnpx0167 BB 2eme carte ethernet 192.168.1.167 dans VLAN1
address 00e0.4c39.2be3 vlan-name default
```

1 - Mobilité sur le réseau local Wi-Fi

- La plupart des laboratoires déploient le Wi-Fi.
- Aspects sécurité
  - VLAN Wi-Fi isolé
  - Chiffrement WEP comme un pis-aller
  - Verrouillage par adresse MAC
  - WPA/TKIP

1 - Mobilité sur le réseau local Wi-Fi à l'IN2P3

- 50 bornes Wi-Fi en 2004, 122 en 2005



2 – Accès externes

- Tradition d’ouverture à l’IN2P3 (ouvert à l ’extérieur par défaut jusqu’en 2002)
- Accès SSH déployés dans l’IN2P3 depuis1998!
- SSH permet de « tunneler » n’importe quelle application TCP. Utilisé en particulier pour X11.

2 - Accès externes

Services SSL pour la messagerie

Objectif : lire et envoyer des mails à distance, depuis un portable, un PC ADSL ou même un cyber café.

Solutions :

- Webmail en HTTPS, mais moins ergonomique (plus de filtres, plus *d'address book* etc.)
- Services IMAPS ou/et POPS pour permettre la lecture sécurisée à distance.
- Pour SMTP l'utilisateur est le plus souvent obligé d'utiliser le serveur SMTP local du site depuis lequel il se connecte. Cette manipulation (changement de serveur SMTP) est source de pas mal d'ennuis.
- Quelques rares serveurs SMTPS avec authentification par certificat peuvent être utilisés à distance

2 - Accès externes

Services SSL pour la messagerie : SMTPS

- SMTPS est une implémentation de SMTP utilisant SSL/TLS
- Usuellement SMTP ne demande pas d'authentification pour relayer les mails.
- Si on installe SMTPS c'est en vue d'accepter de relayer des mails depuis l'extérieur vers l'extérieur (relai ouvert)
- Il est donc impératif de mettre en place une authentification des utilisateurs de ce service.
- L'authentification la plus rapide à mettre en place est une authentification par certificat.

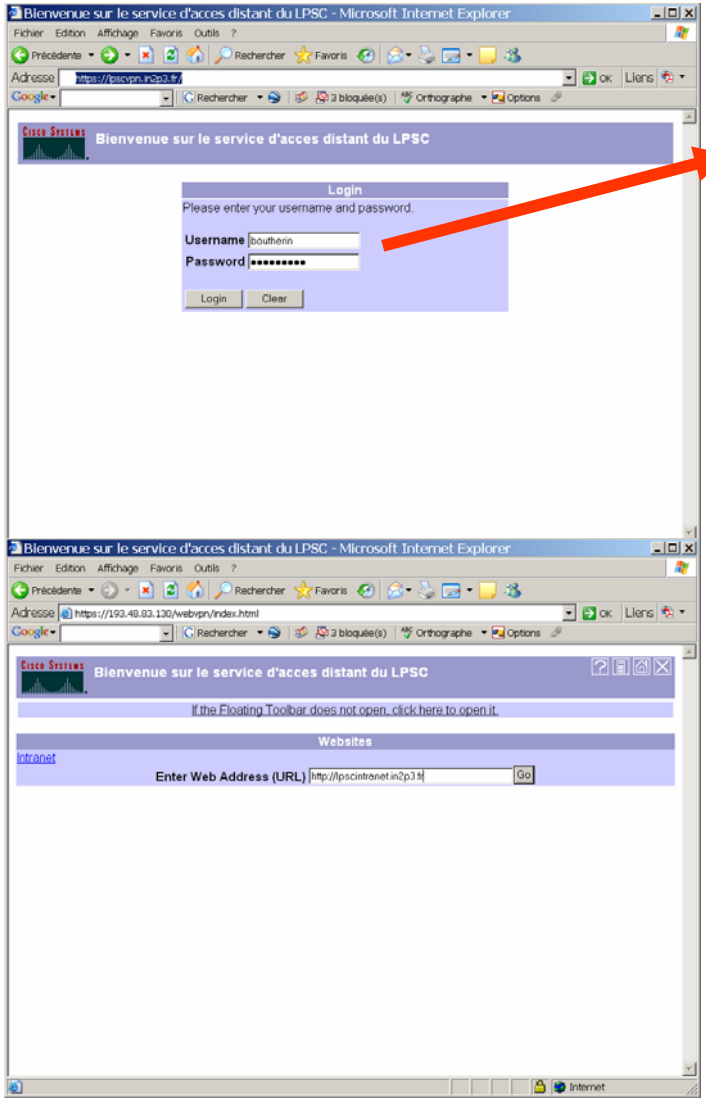
2 - Accès externes VPN

- Établit un tunnel chiffré entre la machine ADSL (par exemple) et le serveur VPN.
- Affecte à la machine ADSL une adresse IP (interface logique) appartenant au laboratoire.
- La connexion ADSL n'est utilisée que pour transférer les données via le tunnel vers l'adresse logique du laboratoire.
- Tout le trafic passe par l'adresse logique du laboratoire.
- Les droits obtenus sont ceux de l'adresse logique donc ceux d'une machine interne.

2 - Accès externes VPN

- Accès aux intranets par VPN HTTPS
- Plein accès par VPN IPSEC.

2 - Accès externes VPN SSL



- Authentification Radius / Active Directory

2 - Accès externes VPN SSL

- Pas d’installation sur le poste client.
- Nécessite un simple navigateur
- Fonctionne quelque soit l’environnement
- Répond à tous les besoins concernant le Web : Intranet, réservation, agenda interne soit 90% de la demande!

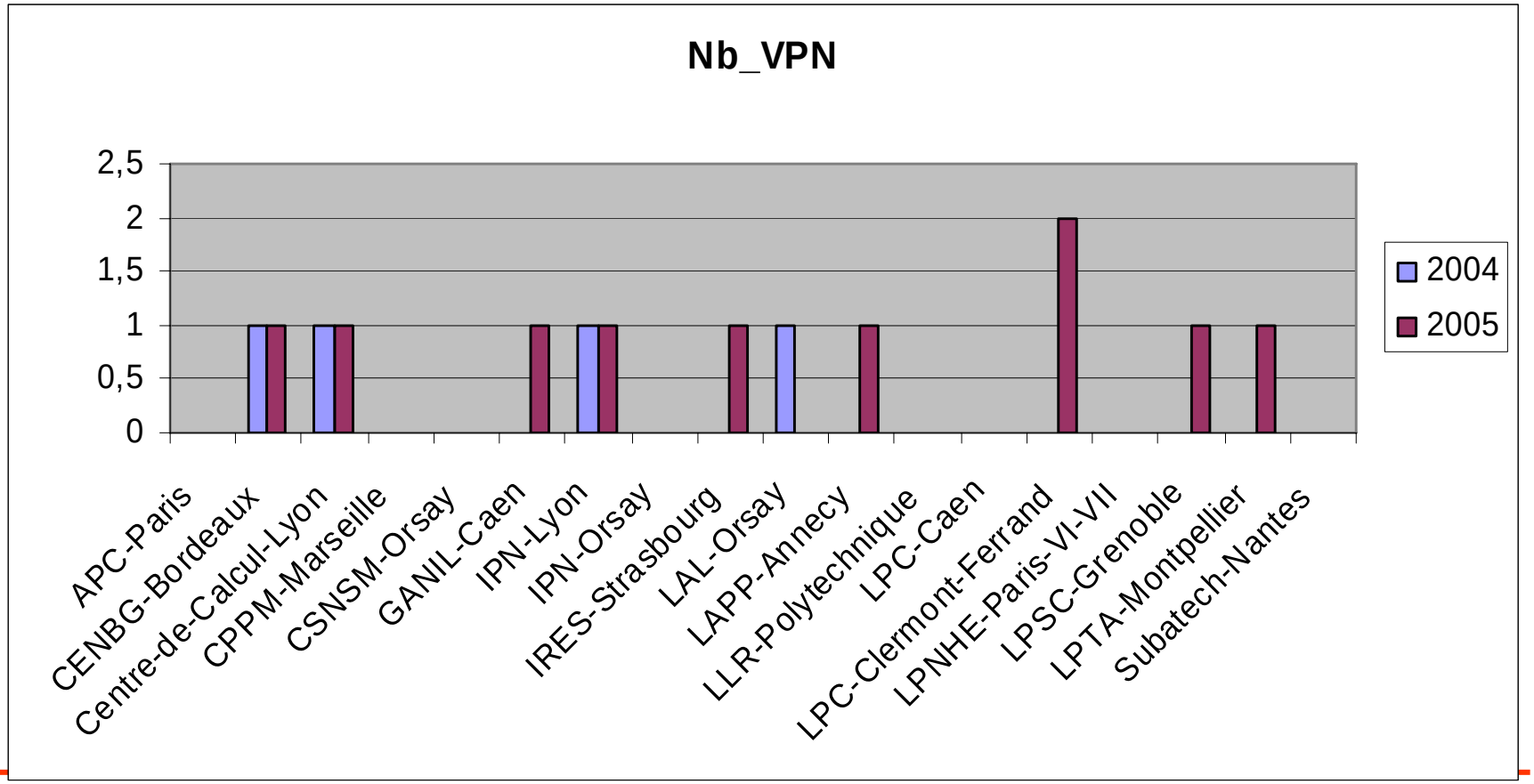
2 - Accès externes VPN IPSEC

- Nécessite l’installation et la configuration d’un logiciel client sur les postes.
- Implémentation délicate sous Linux.

- Plein accès IP, montage des disques des serveurs centralisés, synchronisation des postes, accès aux licences site.

2 - Accès externes VPN à l'IN2P3

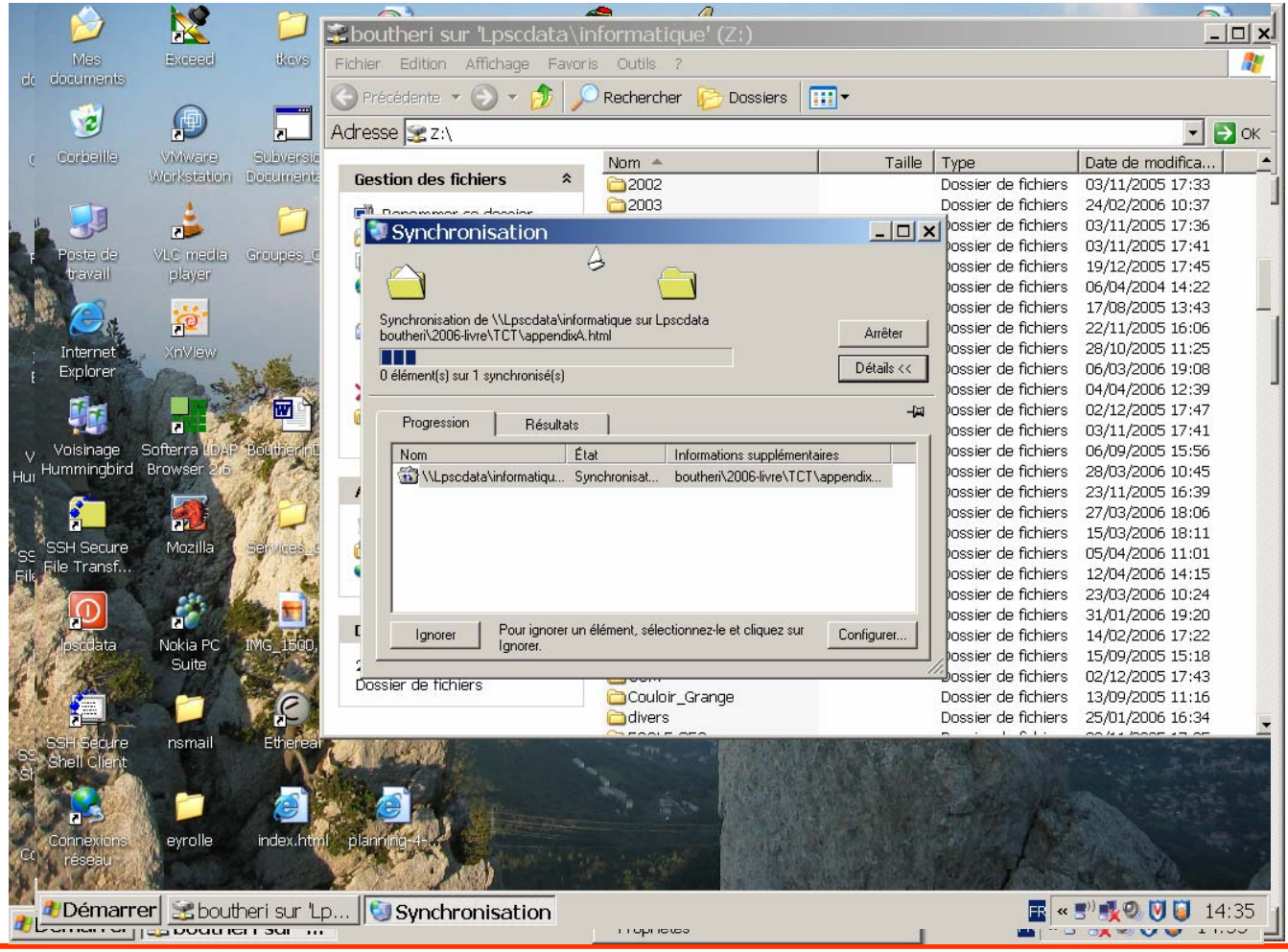
- 4 serveurs VPN en 2004, 10 en 2005



3 – Fonctionnalités Windows

Forêt Active Directory

3 – Fonctionnalités Windows
Synchronisation des portables



Conclusion

- Il existe un panel de fonctionnalités à la disposition des utilisateurs.
- La mobilité pose des problèmes de sécurité des données, des systèmes et du réseau.
  - Données, solution de synchronisation satisfaisante sous Windows, existence d'utilitaires de synchronisation sous MacOS, plus difficile sous Linux.
  - Des systèmes, exposition à l'extérieur, contamination, risque de cheval de Troyes.
  - Des réseaux, Wi-Fi insecure (WEP), ou peu interopérable (802.1x)
- IN2P3 :
  - Déployer des solutions imparfaites ou risquer d'être doublé par les utilisateurs (VMPS, Wi-Fi)