IMFT-SI

Application type Web au cœur du système d'information de l'IMFT (UMR5502)

Jean Pierre Bombaud
Institut de Mécanique des Fluides de Toulouse
Jean-Pierre.Bombaud@imft.fr

Gilles Martin
Institut de Mécanique des Fluides de Toulouse
Gilles.Martin@imft.fr

Charles Nicolas
Institut de Mécanique des Fluides de Toulouse
Charles.Nicolas@imft.fr

Résumé

L'évolution croissante des besoins informatiques au cours des dernières années a conduit le service informatique de l'IMFT à repenser sa stratégie d'organisation et de gestion des ressources. En quelques années le parc informatique a triplé et la gestion des utilisateurs a exigé des réactions rapides. L'idée qui prédomine dans la recherche d'une solution efficace et fiable, est basée sur la collecte et la centralisation des informations au sein d'une base de données unique. Le développement par module de l'application permet de traiter chaque situation comme un cas particulier, par exemple la gestion de l'infrastructure réseau ou des publications. L'ensemble des modules réunis au sein d'une seule application, IMFT-SI, contribue à doter le laboratoire d'un véritable système d'information accessible à tous. Cet article présente la démarche suivie et les solutions retenues.

Mots clefs

Système d'information, administration, VMPS, DHCP, PHP, PostgreSQL, IMFT-SI

1 Introduction

Ces dernières années, au sein de notre laboratoire, le nombre de plates-formes informatiques a suivi une croissance exponentielle : 250 micro-ordinateurs et 150 postes Unix-Linux à ce jour. Ce nouvel état de fait a exigé une gestion plus efficace et plus rapide des ressources informatiques. Ajoutons que l'obsolescence du parc de commutateurs, le nécessaire accroissement du nombre de prises banalisées réseau et téléphonie, 700 points d'accès à ce jour, ont conduit à repenser complètement l'architecture du réseau et son mode d'administration.

2 Présentation générale

2.1 Le Laboratoire

L'Institut de Mécanique des Fluides de Toulouse est une unité mixte de recherche placée sous la double tutelle : CNRS et Education Nationale (INPT[1] et UPS[2]). L'unité accueille 200 personnes : personnels administratifs et techniques, chercheurs, enseignants-chercheurs, doctorants et post-doctorants. A cet effectif, il faut ajouter chaque année 40 à 50 stagiaires.

Le site est composé de 5 bâtiments principaux, une soufflerie aérodynamique et de deux halls techniques. L'ensemble occupe une surface de 12 000 m².

2.2 Les besoins

Pour initialiser l'étude, les besoins ont été définis à partir de trois éléments basiques et fondamentaux :

- Une personne et son compte informatique

Toute personne accueillie au laboratoire possède un statut administratif et fonctionnel, est géographiquement localisée. Elle possède un compte et une adresse de courrier électronique, elle accède à une ou plusieurs plates-formes et utilise les ressources informatiques.

- Le parc informatique

Une plate-forme est achetée après validation du devis pour respecter les spécifications du service informatique. Après réception et contrôle, elle est installée et configurée. La

[1] Institut National Polytechnique de Toulouse

[2] Université Paul Sabatier

plate-forme est localisée dans le laboratoire : bâtiment, bureau, prise réseau.

- Les accès réseau et téléphonie

Un utilisateur identifié dispose d'un numéro de téléphone et d'un accès internet.

2.3 La stratégie retenue

L'analyse des besoins futurs et les difficultés croissantes rencontrées quotidiennement avec les méthodes de gestion et d'exploitation manuelles rendent cruciales une refonte complète de l'organisation. Pour mener à bien ce projet, trois priorités sont établies :

- Moderniser l'infrastructure réseau afin de diminuer les contraintes d'exploitation et offrir de meilleures performances.
- Développer des modules de gestion spécifique : mail, congés, publications, etc.
- Réunir l'ensemble des développements au sein d'une seule application, dénommée IMFT-SI, accessible par une interface Web pour tous les utilisateurs du laboratoire.

L'ordre des priorités est déterminant pour atteindre cet objectif. Tout en modernisant les éléments existants, elle a permis l'élargissement vers de nouvelles fonctionnalités et l'intégration de nouveaux services.

3 La nouvelle architecture réseau

3.1 Historique

En 1997, le besoin de mettre en place une architecture sécurisée conforme aux recommandations de l'UREC[3] et du CRU[4] se concrétisa par un découpage du réseau basé sur l'analyse des protocoles les plus consommateurs de bande passante.

En effet, l'utilisation de clients X-Window (Terminaux X ou émulation X) est connue pour accroître la charge d'un réseau. La démarche choisie permit de regrouper les plates-formes partageant les mêmes protocoles de communication dans un même segment physique. Elle optimisa la gestion de l'activité réseau et limita la charge du routeur d'interconnexion Cisco 4500.

Le plan d'adressage était constitué de 3 classes C officielles associées à 3 segments physiques. On a défini ainsi :

- Un réseau bureautique : constitué de postes Macintosh et PC
- Un réseau Unix : stations de travail et serveurs Unix, terminaux X et imprimantes
- Un réseau ZMS[5] : serveurs Unix accessibles depuis l'extérieur : Mail, FTP, Web

Au quotidien, cette répartition s'est révélée rigide et peu adaptée à l'évolution croissante du parc. Notamment par l'obligation de gérer un brassage distinct pour chacun des réseaux et par la pénurie d'adresses engendrée par l'apparition des portables.

En 2000, la conception de la nouvelle architecture se devait de faire abstraction des critères physiques pour chercher à regrouper logiquement les utilisateurs. Elle reproduit ainsi l'organisation fonctionnelle du laboratoire :

- Groupes de recherche
- Services d'intérêts généraux

La future architecture doit apporter une réponse satisfaisante à deux situations fréquentes :

- Les visiteurs : personnes accueillies pour une courte période (maximum une semaine)
- Les personnes administrant leur poste de travail.

3.2 Analyse des besoins

3.2.1 Les groupes de recherche

Un groupe de recherche est constitué de 15 à 30 personnes. Les personnels ont pour origine le CNRS et l'Education Nationale. Effectif : 160 personnes.

Les besoins informatiques sont essentiellement :

- Les applications scientifiques
- Les applications bureautiques
- Les applications réseau : courrier électronique, Web, impression, etc.

3.2.2 Les services d'intérêt général

Cette appellation regroupe : les services administratifs, les services techniques. Effectif : 35 personnes.

Les besoins informatiques sont essentiellement :

- Les applications administratives et comptables
- Les applications bureautiques
- Les applications réseau : courrier électronique, Web, impression, etc.

3.2.3 Les autonomes

Concerne les utilisateurs autorisés à gérer leur plate-forme dans un cadre légal. Effectif à déterminer.

Les besoins informatiques sont essentiellement :

- Les applications scientifiques

[3] Unité REseaux du CNRS

[4] Comité Réseaux des Universités

[5] Zone de Machines Sécurisées

- Les applications bureautiques
- Les applications réseau : courrier électronique, Web, impression, etc.

3.2.4 Les visiteurs

Le laboratoire doit permettre un accès sécurisé et restreint à des services de base pour une personne présente pendant une courte période. C'est une situation de plus en plus fréquente. Effectif : moins de 10 personnes.

Les besoins informatiques seront strictement limités à la navigation, l'accès aux services FTP anonymous, impression et courrier électronique. L'accès au réseau ne sera autorisé que pendant les horaires d'ouverture du laboratoire.

3.3 Solution et démarche

La solution retenue introduit l'exploitation des réseaux virtuels (VLAN[6]) permettant de regrouper logiquement les utilisateurs par profils.

Les contraintes d'exploitation quotidiennes sont allégées par l'utilisation de mécanismes automatiques d'assignation de VLAN (VMPS[7]) et d'assignation d'adresses réseaux dynamiques (DHCP[8]). Les serveurs nécessaires à l'exploitation sont redondants et les mises à jours sont réalisées par des scripts exploitant les informations stockées dans une base de données. L'objectif est d'attribuer un espace d'adressage unique pour chacune des situations. Le choix d'un adressage utilisant plusieurs classes privées évite les risques de pénurie. L'indépendance des réseaux et la mise en place de listes de contrôles d'accès (ACL[9]) spécifiques à chacun des VLAN renforcent la sécurité.

3.3.1 Règles de fonctionnement

- Toutes les plates-formes sont administrées par le service informatique.
- Tous les utilisateurs et toutes les plates-formes sont référencés dans la base de données du futur système d'information.

Pour répondre aux nouvelles demandes, elles sont complétées par deux nouvelles règles :

- Après accord de la direction et sous certaines conditions, un personnel permanent peut être administrateur de sa plate-forme.
- Un matériel inconnu est placé automatiquement sur un VLAN proposant des services limités.

[6] Virtual LAN

[7] VLAN Membership Policy Server

[8] Dynamic Host Configuration Protocol

[9] Access Control List

3.3.2 Inventaire des applications

On recense l'ensemble des applications utilisées au laboratoire afin de déterminer la nature des échanges, les protocoles réseaux et la future cartographie des communications.

Fonctionnalités et accès fournis	**Applications Serveurs**	**Applications clientes**
Services web	HTTP HTTPS	Internet Explorer Netscape, Mozilla
Services messagerie	POP, SMTP, IMAP, webmail	Eudora, Netscape Mozilla
Serveurs de Fichiers	FTP samba, NFS, appleshare	Filezilla, NFS Wsftp, Fetch
Applications réseau	Base laboratoire, NIS[10], LDAP, Telnet, SSH, X	Navigateurs Putty, Winscp, Nifty-telnet Cygwin-xfree, Exceed
Impression	LPD/ LPR, CUPS	IPP
Jetons de licence	Flexlm	Logiciels clients
Temps	NTP	NTP, Anachron
Sauvegarde	Librairie IBM + TSM[11]	Clients TSM
Domaine imft.fr	DNS	Clients DNS
Applications		Antivirus, Bureautique
Systèmes d'exploitation	Linux, IRIX, AIX, SOLARIS	Mac OS 9 à Mac OSX, toutes versions Windows clientes

Tableau 1 - *Liste des services*

3.3.3 Déclaration des profils

Une nouvelle notion est introduite : le profil utilisateur. C'est un statut qui détermine dans quelle catégorie sera affecté un utilisateur en fonction de sa situation administrative et de l'utilisation des ressources informatiques. Un profil est caractérisé par une appellation de VLAN et une classe d'adresses. Il peut être constitué de plusieurs VLAN dont le nom et la classe d'adresses sont distincts.

Trois types de profils sont proposés :

[10] Network Information Services

[11] Tivoli Storage Manager

- Standard

Concerne les groupes de recherche et les services généraux.

Pour simplifier la gestion future de l'architecture, tous les services d'intérêts généraux (reprographie, bâtiment, direction, informatique) sont regroupés dans un seul VLAN. Ils partagent avec les 5 groupes de recherche le même profil mais chacun possède une appellation et une classe réseau distincte. L'utilisateur et le matériel sont connus du service informatique. Il représente 85% des effectifs.

- Autonome

Personnel permanent administrateur de sa plate-forme. Les utilisateurs et le matériel sont connus du service informatique. Il représente 10 % des effectifs.

- Visiteur

Nouvelle notion, personne extérieure au laboratoire et accueillie pour une courte durée (une semaine). L'utilisateur et le matériel sont inconnus du service informatique. Il représente 5% des effectifs.

Critères	**Standard**	**Autonome**	**Visiteur**
Compte utilisateur	Identifié	Identifié	Inconnu
Inventaire équipement	Oui	Oui	Non
Gestion de l'équipement	Service informatique	Utilisateur après accord de la direction	Utilisateur
Population ciblée	5 groupes et les services généraux	Personnel Permanent	Invité, visiteur
Assignation d'adresse	DHCP statique	DHCP statique	DHCP dynamique
Remarques particulières	L'échange de données entre les groupes est permis	L'accès aux réseaux internes IMFT est restreint	L'accès aux réseaux internes IMFT est interdit
Appréciation des risques	Faible	Moyenne	Elevée

Tableau 2 - *Liste des profils*

Conclusion : dans les profils autonome et visiteur, les équipements sont considérés comme potentiellement compromis. La règle appliquée par défaut sera d'interdire tous les services sauf ceux qui sont autorisés par nécessité. Cette règle est mise en œuvre par la gestion des listes de contrôles d'accès (ACL).

3.3.4 Organisation du plan d'adressage

Les groupes ont des effectifs réduits, en estimant les besoins de 3 adresses IP par personne (un poste fixe, un portable, un futur équipement réseau (téléphone IP, imprimantes,...) il est décidé d'allouer une classe C privée pour chacun des groupes.

Les profils autonome et visiteur reçoivent chacun une classe C. Finalement, c'est 16 classes C non routables qui sont déployées.

N° de vlan	**Préfixes génériques DNS des machines**	**Nom du VLAN**
1		default
3		unix3
4		bur4
5		zms
10	serv	services
12	com	commun
13		inter13
20	emt	emt2
30	gemp	gemp
40	hydre	hydre
41	ghap	ghappe
50	inter	interfa
60	eec	eec
90	visit	visiteur
91	auto	autonome
100	test	test
909		equ909

Tableau 3 - *Liste des VLAN*

3.4 Originalités de l'architecture réseau

Elle repose sur l'exploitation de deux mécanismes d'assignation.

VMPS : VLAN Membership Policy Server. C'est une méthode d'affectation d'un port de commutateur à un VLAN basée sur la lecture de l'adresse matérielle de l'équipement connecté. Nous avons choisi l'implémentation libre Open VMPS dans sa version 1.3.

Lorsqu'un port de commutateur est activé, l'équipement interroge un service VMPS hébergé par un serveur Unix. Le démon recherche dans son fichier de configuration l'entrée correspondante à l'adresse matérielle transmise. Il retourne le nom du VLAN qui lui est associé et le commutateur bascule le port dans ce VLAN. La possibilité de définir un VLAN par défaut a permis d'affecter

automatiquement toutes les machines inconnues de nos inventaires dans le VLAN visiteur.

Le service DHCP est connu depuis longtemps pour sa robustesse et sa facilité d'emploi. Par souci de sécurité, chaque machine connue et inventoriée reçoit toujours la même adresse IP. Un triplet d'informations (nom, adresse_ matérielle, adresse_IP) caractérise l'équipement. La configuration particulière des serveurs DHCP permet l'attribution d'une adresse à une machine inconnue dans la classe d'adresses réservée aux visiteurs.

L'association de ces 2 mécanismes contribue à la sécurité de l'architecture réseau en réduisant les risques d'intrusion d'un tiers. L'enregistrement systématique des activations d'un port de commutateurs permet de localiser instantanément un équipement (bâtiment, bureau, prise). Le traitement de cette activité permet de proposer une solution satisfaisante pour les profils visiteur. Les accès sont permis sur l'ensemble du site avec un compromis convenable entre la sécurité et des besoins utilisateurs.

4 La nouvelle application : IMFT-SI

4.1 La solution retenue

Pour faciliter et automatiser la gestion, la décision de faire converger l'ensemble des développements vers une seule application a été retenue. C'est ainsi qu'a démarré le projet de développement de IMFT-SI. Il a été réalisé, au cours des dernières années, par les différents stagiaires accueillis et encadrés par les ingénieurs du service.

Cette application permet de centraliser dans plusieurs tables d'une base de données unique, les informations indispensables à la gestion des comptes utilisateur et des plates-formes, ainsi que l'infrastructure réseau et les accès afférents.

L'interactivité de IMFT-SI permet la génération automatique et instantanée des fichiers nécessaires au fonctionnement général. L'information ainsi diffusée est mise en exploitation immédiatement.

Par ailleurs, la remontée automatique d'évènements, localisation en temps réel, d'une machine, par exemple, permet une auto alimentation de la base de données. L'historique de l'activité est présenté sous forme de tableaux de bord et archivé, avec la préoccupation permanente du respect des contraintes sécuritaires.

Pour garantir l'évolution de l'application dans les meilleures conditions, le développement de IMFT-SI s'appuie sur des produits open-source : Linux, Apache, PostgreSQL, PHP.

4.2 Règles de gestion du système d'information

IMFT-SI a été conçue pour être au coeur du système d'information du laboratoire : toute personne non renseignée dans l'application ne pourra pas accéder aux ressources informatiques du laboratoire. De même, tout équipement non référencé, n'aura pas de connectivité réseau. La seule exception concerne les visiteurs de courte durée qui bénéficient de services minimum.

Ces contraintes ont été définies afin d'assurer la cohérence et la mise à jour des données. Elles donnent à l'application toute sa valeur grâce à la fiabilité des informations stockées. Elles permettent l'automatisation de nombreuses opérations et la génération des fichiers destinés au système d'information.

4.3 Les utilisateurs de l'application

4.3.1 Les profils

Tout le personnel du laboratoire est susceptible d'utiliser l'application. Pour cela, des profils utilisateur ont été définis :

Profil	**Droits**
employé	Il peut consulter sa fiche personnelle, modifier certaines informations et le cas échéant, visualiser sa fiche d'absence.
groupe **(secrétaire de groupe)**	Donne accès aux fiches d'absences, aux calendriers des congés ainsi qu'aux états récapitulatifs. Peut saisir des congés.
admin **(secrétaire principale)**	Donne tous les droits sur la gestion des congés.
super **(superviseur de l'application)**	Donne tous les droits sur l'application.

Tableau 4 - *Liste des profils et permissions associées*

4.3.2 Authentification

Le personnel, après signature de la charte informatique est autorisé à saisir son mot de passe qui sera stocké dans la base de données sous différentes formes hachées ou chiffrées : DES[12], NTLM[13], SHA1[14], MD5[15]. L'authentification à l'IMFT repose sur le système NIS (chiffrement DES). Le fait de stocker les mots de passe sous différentes formes permet potentiellement de générer les fichiers d'authentification pour de nombreux systèmes différents.

[12] Data Encryption Standard

[13] New Technology Lan Manager

[14] Secure Hash Algorithm version 1

[15] Message Digest version 5

Une nouvelle forme de hachage ou de chiffrement peut être ajoutée à la base de données. Dans ce cas, lors de la première connexion de l'utilisateur à IMFT-SI, le champ manquant sera renseigné automatiquement.

4.4 Les modules de l'application et leurs fonctionnalités

4.4.1 Gestion du personnel

Ce module de l'application est destiné à gérer les personnels du laboratoire. Il permet de gérer tous les types de personnels ainsi que leurs caractéristiques associées : positionnement administratif, fonctionnel et géographique dans le laboratoire, ainsi que les congés et absences.

A partir des caractéristiques des personnels, le login, l'uid et l'adresse email sont automatiquement générés.

4.4.2 Courrier électronique

La création d'un nouvel utilisateur implique la génération de nouveaux fichiers destinés aux serveurs de courrier électronique. Les alias de mail et les listes de diffusion, par bâtiment, service, statut, etc. sont automatiquement générés à partir de l'application.

IMFT-SI s'interface directement avec le serveur IMAP (Cyrus IMAP) du laboratoire. La création d'un personnel crée automatiquement son compte sur le serveur IMAP et un sous module de l'application permet des gérer les quotas de chaque utilisateur.

4.4.3 Gestion des équipements

Ce module de l'application permet de gérer l'ensemble du parc informatique du laboratoire.

- **Gestion administrative**

A l'arrivée d'un nouveau matériel, et pendant toute sa durée de vie, les informations principales sont consignées : date de livraison, fin de garantie, numéro de série, fournisseur ainsi que certains documents papier scannés (bon de livraison, devis, intervention, etc.).

- **Gestion informatique**

Le sous module de gestion informatique repose sur l'exploitation du mécanisme d'assignation automatique de VLAN et d'adressage. Lorsqu'un équipement est inventorié, l'adresse physique de la carte réseau est saisie et l'utilisateur associe l'équipement à un VLAN. L'application propose automatiquement une adresse réseau IP et un nom DNS. Il est possible de modifier ces informations.

Le type d'équipement, et le système d'exploitation sont également renseignés.

- **Accès aux équipements**

L'accès aux équipements informatiques du laboratoire repose sur le système des « netgroup » NIS. Tout utilisateur désirant se connecter à un serveur Unix-Linux, doit être renseigné dans le fichier « netgroup ».

Les plates-formes Windows et Macintosh sont aussi concernées par ce module de l'application.

4.4.4 Création des états récapitulatifs

Pour la gestion du personnel et des équipements, des requêtes prédéfinies ont été écrites qui permettent rapidement d'imprimer ou de télécharger au format « CSV[16] » des états à partir de la base de données.

4.4.5 Gestion administrative de l'application

Ce module permet de gérer les droits d'accès des utilisateurs sur l'application. Il permet aussi de consulter l'historique des modifications effectuées sur la base de données.

4.4.6 Gestion des publications

La production scientifique du laboratoire conditionne sa notoriété et son avenir. L'application de gestion des publications, en s'appuyant sur la base de données IMFT-SI, permet la création et la modification des publications.

Son moteur de recherche accessible depuis le site Internet du laboratoire, permet la consultation et le référencement de toute la production scientifique sur les moteurs de recherche (Google, etc.). Il permet aussi l'exportation sous les formats texte, « CSV », Endnote et Bibtex des références bibliographiques.

Enfin, la centralisation de toute la production scientifique du laboratoire permet l'extraction de l'ensemble des informations de la base de données en vue de son importation dans les bases du CNRS.

4.4.7 Génération automatique des fichiers

La validation de la saisie provoque un traitement de mise à jour des serveurs en plusieurs étapes :

- génération instantanée des fichiers nécessaires
- propagation de ces fichiers vers les serveurs respectifs (recopie par « scp »)
- Redémarrage des services réseau (traitement immédiat de la nouvelle information)

La progression de ces étapes est visualisée dans l'écran de validation. Le temps nécessaire pour la prise en compte des modifications par les différents serveurs est d'environ dix secondes.

Les fichiers générés sont les suivants :

- Serveur NIS : fichier « passwd », fichier « netgroup »
- Serveurs SMTP et IMAP : fichiers « aliases », listes de diffusion
- Serveurs DNS : fichiers de la zone « imft.fr »

[16] Comma Separated Values

- Serveurs DHCP : fichier « dhcpd.conf »
- Serveurs VMPS : fichier « vmps.conf »

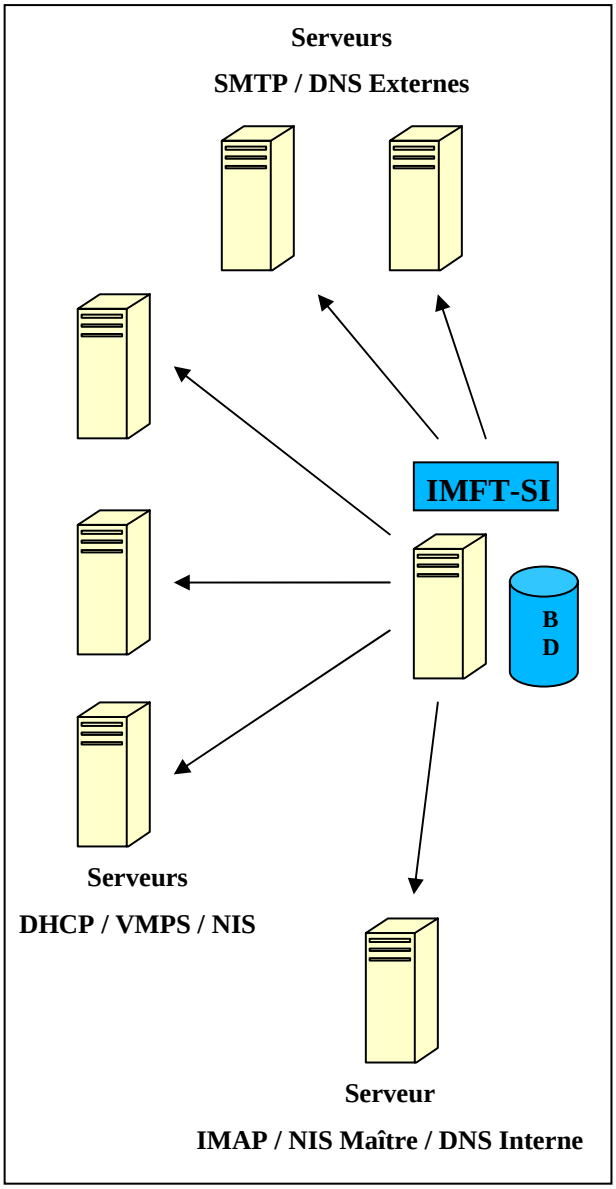

Figure 1 - *Architecture de propagation des fichiers*

La structure de l'application permet d'interfacer très rapidement de nouveaux services. Il est prévu dans un futur proche d'exporter les données vers un annuaire LDAP.

4.4.8 Gestion du brassage des équipements (informatique et téléphone)

Depuis la réorganisation de l'architecture chaque bâtiment est équipé d'un local réseau. Les prises murales RJ45 supportent les connexions des téléphones ou des équipements informatiques. L'ensemble converge vers un panneau de brassage unique.

- **Réseau informatique**

L'application gère pour chacun des bâtiments la disponibilité des ports par commutateur. On obtient une représentation graphique des façades des commutateurs qui affiche l'état de remplissage. L'administrateur renseigne pour chacun des ports utilisés, le numéro de prise associée.

L'interrogation d'un port permet d'obtenir son état :

- Non brassé et aucun équipement connecté
- Brassé et aucun équipement connecté

  Le n° de prise est affiché
- Brassé et un équipement connecté

  Le n° de prise, le nom et l'adresse MAC de l'équipement connecté sont affichés.

  L'adresse MAC est extraite de l'analyse des alarmes remontées par le service VMPS.

La mise à jour de l'affichage est automatique.

- **Téléphonie**

La démarche est différente, mais exploite une interface graphique pour la gestion et l'attribution d'un numéro de téléphone.

Nous retrouvons les opérations classiques :

- Ajout
- Suppression
- Modification

Ces opérations sont distinctes de la gestion de l'autocommutateur téléphonique. Les changements effectués dans la base n'ont aucun effet sur le fonctionnement de l'autocommutateur à l'heure actuelle.

- **Détection et historique d'activation des prises**

L'analyse des alertes du service VMPS permet un traitement particulièrement original pour la maintenance de nos inventaires. A chaque activation d'un port, le service enregistre les informations suivantes :

Date, heure, adresse réseau du commutateur, adresse physique de l'équipement connecté, nom du VLAN associé.

Un script analyse cette remontée d'information et réalise plusieurs traitements :

- Historique sous forme calendaire des connexions visiteurs.
- Mise à jour des plans de localisation des équipements.
- Maintenance des états d'occupation des commutateurs.

5 Cas concrets d'utilisation de l'application

5.1 Création d'un nouveau personnel

A l'arrivée d'un nouveau personnel au laboratoire, à partir de l'application IMFT-SI, une nouvelle fiche est créée.

L'objectif principal du module « personnel » est la gestion des comptes informatiques des utilisateurs. D'autres modules de l'application s'appuient sur les informations collectées : module « accès aux équipements informatiques », module « publications » et module « congés ».

Les données suivantes sont renseignées :

- Nom, prénom
- Etablissement d'appartenance (INPT, CNRS, etc)
- Fonction (Professeur, Doctorant, etc.)
- Bâtiment
- Numéro de bureau
- Groupe de recherche auquel la personne est rattachée

Ces informations permettent à l'application de générer les paramètres du compte informatique :

- « uid », « gid » sont imposés et dépendent directement du groupe de recherche et du statut.
- « login », alias de mail sont proposés automatiquement, mais peuvent être modifiées.

La création d'un utilisateur dans l'application entraîne systématiquement :

- La création de son compte mail sur le serveur Cyrus IMAP.
- La génération et la propagation du fichier « passwd » pour le système d'authentification NIS.
- La génération et la propagation des fichiers (« aliases », listes de diffusion) pour les relais de mail.

Enfin, les plans des bâtiments accessibles sur le serveur Intranet du laboratoire permettent, à partir des informations saisies, de localiser la personne dans un bureau avec son numéro de téléphone.

L'ensemble de ces opérations, saisie, création et propagation est réalisé en deux minutes.

5.2 Création d'un équipement

Etape 1 : initialisation des informations.

Données fournies :

- « MAC address » de la carte réseau
- VLAN de destination
- Type d'équipement
- Système d'exploitation et version
- Date de livraison
- Durée de garantie
- Nom fournisseur
- Numéro de série
- Téléchargement des documents scannés

  Devis

  Bon de livraison
- Champs facultatifs : remarques, descriptions….

Etape 2 : génération des paramètres réseau

Données proposées et modifiables :

- Nom du matériel
- Adresse IP

Etape 3 : mise à jour

Les fichiers suivants sont reconstruits et propagés vers les serveurs dédiés :

- vmps.conf : nom_du_vlan, mac_adresse
- dhcp.conf : nom_equipement, mac_adresse, adresse_IP
- named.conf et les fichiers « reverses » : nom_equipement, adresse_IP

L'ensemble de ces opérations, saisie, création et propagation est réalisé en deux minutes. L'équipement peut accéder au réseau et être opérationnel dans la minute qui suit. Les informations de localisation sont automatiquement renseignées dans la base de données et apparaissent sur les plans des bâtiments.

5.3 Suivi des connexions des « visiteurs »

Une personne en visite au laboratoire pour une durée limitée peut se connecter sur le réseau avec son portable, sans en aviser le service informatique. Elle bénéficie d'un certain nombre de services réseau : accès Web, envoi du courrier électronique par l'intermédiaire du serveur SMTP local, impressions, serveur FTP anonyme local.

Sur l'Intranet, grâce aux plans des bâtiments, il est possible de connaître l'état des prises (brassées ou inactives). Lors de la connexion du portable à la prise réseau, le port du commutateur concerné est automatiquement basculé dans le VLAN « visiteur » par le service VMPS. Il obtient une adresse IP par le service DHCP.

Un suivi de ces connexions est possible via le tableau de bord de l'application, qui donne pour chaque adresse MAC non référencée dans la base de données, le nombre de connexions, par jour, sur 3 mois glissants.

En cas d'abus, un blocage de l'adresse MAC peut être réalisé par l'intermédiaire du serveur VMPS.

6 Unités concernées et perspectives de développement.

6.1 Rappel

IMFT-SI a été développée pour répondre aux besoins de l'unité. Les caractéristiques essentielles du laboratoire sont les suivantes :

Unité mixte de recherche, l'IMFT accueille des personnels d'origines très diverses : CNRS, Education Nationale (INPT, UPS), CEMAGREF, étudiants, stagiaires, etc.

Les statuts du personnel sont multiples et la durée d'accueil varie de quelques jours à plusieurs années.

Cette diversité explique la difficulté d'obtenir des sources d'informations fiables et complètes recouvrant tout l'ensemble du personnel.

La formation est organisée en groupes de recherche et services d'intérêt général.

La nécessité de gérer la totalité des situations a conduit au développement de l'application.

6.2 Formations concernées

Toute unité dont le modèle organisationnel est du même type que l'IMFT, peut utiliser cette application sans modifications majeures. Actuellement l'application gére 250 comptes et 400 plates-formes. Il nous semble raisonnable que l'on puisse multiplier ces valeurs par trois ou quatre. L'efficacité de la gestion est simplement liée aux performances du serveur et du réseau.

Pour apporter une solution satisfaisante et réduire les contraintes d'exploitation et de gestion, certaines corrections mineures peuvent être effectuées en fonction de besoins ponctuels.

Rappelons que le code est très structuré. Le remplacement ou l'ajout de certaines fonctionnalités ne présente aucune difficulté.

6.3 Exploitation

Le coût de développement de l'application est minime. Elle a été réalisée par les stagiaires accueillis au sein du service informatique, encadrés par les ingénieurs permanents.

L'ensemble repose sur l'utilisation de logiciels libres :

- Base de données PostgreSQL
- Serveur Web Apache
- Langages de développement : PHP, HTML, Javascript

La plate-forme d'exploitation est un serveur Pentium IV, 2 GHz sous Linux, muni de 1 Go de RAM et d'un espace de stockage de 80 Go en Raid 5.

6.4 Perspectives

Les principales évolutions envisagées de l'application sont de trois types :

- Ajout et gestion de nouvelles informations, en priorité :

  - Licences logicielles

  - Certificats électroniques

  - Autocommutateur.

  Ces données étant disponibles, les fichiers de mise à jour seront générés automatiquement. Cela permettra également de faire évoluer des services déjà existants, ou bien d'en envisager de nouveaux, annuaire LDAP en particulier.

- Délégation vers les secrétariats de groupe des opérations de saisie. L'information sera ensuite validée par les administrateurs. Cette méthode évitera les doubles saisies, gain de temps et diminution du risque d'erreur. Cette évolution ne présentera guère de difficulté dans la mesure où des profils de gestion hiérarchisés sont déjà opérationnels dans l'application.

- Basée sur le même principe des profils, offrir à l'ensemble du personnel de l'unité, une plus grande accessibilité à l'information disponible de la base de données.

7 Conclusion

L'application IMFT-SI répond aux besoins actuels de l'IMFT. La gestion centralisée, la mise à jour des informations et la propagation automatique ont considérablement simplifié et amélioré l'accès et la sécurisation de l'utilisation des ressources informatiques.

Les utilisateurs peuvent, en fonction de leur profil, modifier leur mot de passe ainsi que des informations personnelles : adresse, téléphone, etc. Ils peuvent consulter leur fiche ainsi que l'état de leurs congés ; saisir et extraire leur production scientifique.

L'originalité de cette application repose sur la mise à disposition instantanée de nouvelles informations et sur sa capacité à s'autoalimenter à partir des événements collectés. Elle permet ainsi de mieux contrôler l'afflux des micro-ordinateurs portables qui se connectent sur le réseau par le VLAN « visiteur ».

Enfin, les modules de l'application IMFT-SI permettent l'extraction de données à destination des systèmes d'information de l'université (INPT) et pour la partie production scientifique vers la base documentaire du CNRS.

Il reste, toutefois, encore nombre de fonctionnalités à ajouter. Certaines sont déjà clairement identifiées, comme la gestion des licences logicielles, la mise en place d'un système d'authentification centralisé commun aux plates-

formes Unix - Linux, Windows et Macintosh, la gestion automatisée de la téléphonie et synchronisation automatique de l’autocommutateur.

L'évolution vers de nouveaux services ne demandera que peu de développement dans la mesure où toute l'information est déjà disponible ou facilement intégrable. IMFT-SI a été développée pour les besoins spécifiques du laboratoire. Cependant, le code développé est structuré et modulaire. Il offre la possibilité de s’adapter à un autre établissement.