École élémentaire Anatole France
Systèmes d'information

Septembre 2015

Réseau Neptune
Rapport d'installation

Alain & Antoine PERNOT

Réseau Neptune - Rapport d'installation

École élémentaire d'Is-sur-Tille - Systèmes d'information

28 septembre 2015

Préambule

L'actuel document présente l'infrastructure actuelle du réseau informatique de l'école élémentaire Anatole France d'Is-sur-Tille (21). Sa réalisation à été menée à bien par Antoine Pernot entre juillet 2012 et août 2015.

Ce document relate l'historique de réseau durant cette période afin de mettre en avant l'évolution de celui-ci avant de présenter la dotation matérielle offerte par le Centre Hospitalier Universitaire de Dijon et d'en estimer la valeur. Nous poursuivrons ensuite sur les composantes logicielles réalisées et implantées afin d'exploiter au mieux les ressources matérielles de cette infrastructure. Un point particulier sur la sécurité du réseau sera abordé avant de conclure sur les évolutions possibles du réseau.

Table des matières

Chapitre 1

Introduction

1.1 Périmètre de l'infrastructure

Le terme "INFRASTRUCTURE" désigne les ressources informatiques mises en place dans l'école élémentaire Anatole France d'Is-sur-Tille (21). Cela comprends :

- La baie informatique située dans le local informatique et son contenu (hors modem dont la propriété revient à France Télécom Orange).
- Les équipements informatiques installés dans la salle informatique dont l'imprimante (hors tableau blanc interactif et ordinateur portable affecté à son exploitation).
- Les équipements informatiques installés dans la bibliothèque dont l'imprimante (hors équipements audiovisuel, vidéoprojecteur et ordinateur portable affecté à son exploitation).
- Les équipements informatiques installés dans chaque salle de classe et mis à disposition par le service informatique (hors tableau blanc interactif, équipement audiovisuel, équipement d'impression et de reprographie et ordinateurs dont la propriété revient aux enseignants).
- Les équipements informatiques installés dans la salle des professeurs (hors équipements d'impression et de reprographie).
- Les équipements de réserve.

Ne sont pas compris dans l'infrastructure :

- Les équipements audiovisuels (dont vidéoprojecteurs).
- Les équipements d'impression et de reprographie sauf pour la salle informatique et la bibliothèque.
- Les équipements loués par l'opérateur téléphonique et le fournisseur d'accès à Internet pour le raccordement au réseau téléphonique public.
- Les équipements téléphoniques.
- Les équipements pédagogiques numériques (TBI ...).
- Les équipements informatiques situés dans le bureau du directeur.
- Les équipements informatiques dont la propriété revient aux enseignants.

1.2 Remerciements

L'intégralité des travaux effectués ont été supervisés par les équipes enseignante et technique de l'Institut Universitaire de Technologie d'Auxerre (antenne de Dijon), département Réseaux et Télécommunications.

Les travaux ont été également vus par des professeurs de l'école d'ingénieurs de l'Université de Technologie de Troyes, département Systèmes, Réseaux et Télécommunications.

Je remercie notamment les docteurs, ingénieurs, professeurs et techniciens en informatique, programmation, réseaux, télécommunications, sécurité informatique et architecture des systèmes informatiques qui m'ont conseillé et qui ont supervisé la réalisation de cette infrastructure.

Je remercie également l'équipe France Télécom Orange de Dijon (central téléphonique régional avenue Stalingrad) pour leur expertise sur les réseaux d'entreprises et le réseau d'opérateur, qui m'a notamment profité lors de la réalisation des travaux de déploiement du réseau VDI.

J'ai également été conseillé pour la réalisation de ce réseau par des collègues de ces formations que je remercie.

Chapitre 2

Évolution de l'infrastructure

2.1 État du réseau avant notre intervention

À notre arrivée, le réseau était constitué de 12 postes dont un poste était désigné comme "serveur". Sa fonction était inconnue car aucun poste n'exploitait ses capacités. 4 postes étaient déclarés "Hors service". Les postes étaient équipés de systèmes d'exploitation hétérogènes (Windows XP, Windows Vista et Mandriva Linux pour le serveur). Chaque poste avait un bouquet de logiciels (suite bureautique, navigateur Internet ...) hétérogène et il était fastidieux pour les usagers de l'exploiter :

- Pour mettre à disposition un fichier pour chaque élève, les enseignants devaient enregistrer le fichier dans les différents formats gérés par les divers programmes mis en place puis le copier sur chaque poste, un à un, à l'aide d'un support de stockage externe.
- La prise en charge de certaines technologies utilisées dans certaines pages Web dépendait des navigateurs Web installés.
- Aucune séparation des utilisateurs était en place. Une personne pouvait modifier à loisir les fichiers ne lui appartenant pas.
- Certains ordinateurs n'étaient pas équipés d'un antivirus valide. De ce fait, certains ordinateurs du réseau étaient infectés.
- L'impression de documents n'était possible que sur un poste. Pour imprimer un document depuis un autre poste, il était nécessaire de le copier sur un support de stockage externe et l'imprimer sur le poste raccordé à l'imprimante.
- Les données personnelles de chaque utilisateur étant stockés en local, chaque usager devait réutiliser le même poste pour modifier un document.
- Aucune structure n'était appliquée pour le stockage des données : les documents étaient disposés de manière épars dans les unités de stockage. Risque de duplicatas avec différentes version d'un même document.
- Le logiciel de bibliothèque était très archaïque et n'était pas très ergonomique à utiliser.

C'est pour cela que le corps enseignant a fait appel à mes services afin de rendre ce réseau plus ergonomique, plus performant et plus sûr.

2.2 Réseau 1 - Début de mise en réseau

Mes travaux débutent en juillet 2012. La mise en place de ce réseau s'est effectué comme suit :

- Remise en état des quatre postes déclarés "Hors service"
- Création d'une image système destinée à être clonée sur l'ensemble du parc informatique. De ce fait, tous les postes étaient équipés du même système d'exploitation (Kubuntu 12.04), de la même suite bureautique (LibreOffice) et du même navigateur Internet (Mozilla Firefox)
- Création à partir du poste le plus puissant du réseau du serveur utilisant Kubuntu 12.04 centralisant les fichiers de chaque utilisateur et les partageant avec tous les postes du réseau.
- Installation d'un serveur de partage de fichiers NFS.
- L'imprimante est connectée au serveur et est partagée avec tous les postes du réseau.
- Installation d'un poste connecté au photocopieur de la salle des professeurs afin d'imprimer directement sur ce dernier.
- Mise en place d'un serveur de messagerie instantanée XMPP, il n'a jamais été utilisé par les utilisateurs.

Ce réseau était ma première infrastructure à cette échelle. J'ai du corriger un ensemble de problèmes et de pannes survenues tout au long de l'année. Deux refontes de l'images système ont été nécessaires afin de corriger les erreurs et d'améliorer la rapidité du réseau, ajouter des fonctionnalités telles que des applications spécifiques à l'éducation. De nombreux déplacement sur site ont été effectués pour constater les problèmes rencontrés par les usagers, effectuer des tests et appliquer les correctifs nécessaires.

Le réseau 1 à été en service entre août 2012 et juillet 2013. Il à été remplacé par le réseau 2 qui corrige les anomalies rencontrées et apporte de nouvelles fonctionnalités.

2.3 Réseau 2 - Séparation des comptes et individualisation des données

Le réseau 1 comportait toujours des manques de fonctionnalités tels que :
- Tous les fichiers étaient accessibles par tous. Ils ont été simplement centralisés sur le serveur.
- Le système d'exploitation choisi pour les clients était trop gourmand en ressources au vue des équipements mis en place.
- De nombreux déplacements ont été effectués pour de petites opérations.

Ces différents problèmes ont été corrigés lors de la création du réseau 2. Les travaux préparatoires (recherches de technologies, tests sur simulateur et tests sur réseau d'essai) ont été effectués de mai 2013 à juillet 2013. En juillet 2013, le réseau 1 est arrêté et les opération suivantes sont effectués :
- Refonte des systèmes d'exploitation clients et serveur en utilisant respectivement Xubuntu 12.04 et Debian 7.
- Mise en place des services présents sur le réseau 1.
- Installation d'un service d'annuaire NIS pour le partage des sessions sur le réseau. Cela à permis la création de sessions individuelles sécurisées par un mot de passe.
- Mise en place d'un partage NFS avec gestion des droits d'accès.
- Création du logiciel de gestion de classes communiquant avec l'annuaire NIS.
- Recherches autour des quotas disques. Non implémenté car non souhaité par le corps enseignant.
- Mise en place de la télégestion et des maintenances automatiques.
- Mise en place de l'accès aux fichiers à distance avec net2ftp.
- Création du logiciel de modification de mot de passe à destination des enseignants.
- Automatisation de l'allumage et de l'arrêt des clients du réseau.

Ce réseau à profité de ma première année de formation en DUT réseaux et télécommunications et de mes recherches personnelles. Une refonte de l'image client à été nécessaire afin d'inclure de nouvelles fonctionnalités et des mises à jours.

Peu d'anomalies sont à signaler sur le réseau 2.

Le réseau 2 à été en service entre août 2013 et juillet 2014. Il à été remplacé par le réseau 3 qui corrige les anomalies rencontrées et apporte de nouvelles fonctionnalités.

2.4 Réseau 3 - Mise à niveau majeure et ajout de fonctionnalités

Le réseau 2 comportait toujours quelques lacunes :
- La technologie d'annuaire NIS est obsolète et peu sécurisée.
- Le matériel en service était vétuste.
- Aucune sauvegarde des données n'était effectuée.
- Le logiciel de bibliothèque (La BCD) accusait d'un état d'obsolescence avancé, n'était pas en réseau et nécessitait le maintien de deux bases de données identiques : l'annuaire central et la base de la bibliothèque.

Ces différents problèmes ont été corrigés lors de la création du réseau 3. Les travaux préparatoires (développement d'applications, recherches de technologies, tests sur simulateur et tests sur réseau d'essai) ont été effectués de mars 2013 à août 2013. En juillet 2013, le réseau 2 est arrêté et les opération suivantes sont effectués :
- Remplacement du parc informatique par les équipements donnés par le CHU (*voir page 27*).
- Refonte des systèmes d'exploitation clients et serveur en utilisant respectivement Xubuntu 14.04 et Debian 7.
- Mise en place des services présents sur le réseau 2.
- Migration de l'ancien annuaire NIS sur OpenLDAP.
- Refonte des applications de gestion de classes et de modification de mot de passe pour exploiter le nouvel annuaire.
- Création d'E-ADMIN, la console d'administration du réseau.
- Mise en place d'une journalisation des événements du réseau.
- Création d'un programme de messagerie interne.
- Installation d'un serveur de clonage des clients en PXE.
- Création d'un logiciel de signalement d'incidents.
- Amélioration des maintenances automatiques.
- Création d'un nouveau logiciel de bibliothèque basé sur l'export des données de l'ancien logiciel.
- Installation d'un système de supervision.
- Création d'un portail Web destiné aux enseignants leurs permettant d'accéder à distance à leurs données *via* net2ftp ainsi que de rechercher des contenus multimédias libres de droits pour enrichir leurs enseignements.
- Accès aux fichiers à distance pour les professeurs directement depuis un client FTP avec un client à installer sur l'ordinateur (tel que FileZilla).

Seule une microcoupure EDF survenue en janvier 2015 à interrompu intégralement le réseau durant les 5 minutes nécessaires à son redémarrage.

Ce réseau à profité de ma deuxième année de formation en DUT réseaux et télécommunications, de mon stage chez France Télécom Orange et de mes recherches personnelles.

Le réseau 3 à été en service entre août 2014 et juillet 2015. Il à été remplacé par le réseau 4 qui augmente sa taille et améliore sa fiabilité.

2.5 Réseau 4 - Agrandissement et fiabilisation

Le réseau 3 ayant fait preuve de sa grande fiabilité, le réseau 4 à hérité de l'ensemble de sa structure. Le réseau 4 est né des travaux effectués en juillet 2015 réalisés par Eiffage Energie. Cependant, certains éléments ont été revus afin de s'adapter à un réseau de cette ampleur :

- Refonte du système de clonage des clients en PXE.
- Factorisation du code entre la console d'administration et le logiciel de gestion des utilisateurs par la création d'une bibliothèque logicielle unifiée.
- Ajout de fonctionnalités au programme de bibliothèque (tri des listes, création d'étiquettes à codes-barres, renforcement de la sécurité, correction d'anomalies ...)
- Création d'un miroir local pour l'installation et la mise à jour de logiciels sur les clients.
- Refonte et allègement de l'image système client.
- Mise en place d'un serveur antivirus pour les fichiers.
- Raccordement des nouveaux postes clients au réseau.
- Installation du photocopieur en réseau.
- Ajout de fonctionnalités à la console d'administration.

Le réseau 4 est actuellement en service depuis août 2015.

Une démonstration en vidéo des procédures de démarrage, d'arrêt et un test de commande exécutée sur le réseau (jouer de manière synchrone la musique *Promenade* de Modeste Moussorgski sur tous les postes clients) est disponible ici :
http://polaris-server.tk/data/Demo-Neptune.mp4

Chapitre 3

Systèmes et réseau

3.1 Système d'exploitation client

Le système d'exploitation des postes clients est Xubuntu 14.04 *(fig. 4.1)*. Il embarque un bouquet homogène d'applications en plus des outils habituels dont :

- Une suite bureautique complète (traitement de texte, tableur, présentation, PAO, base de données, formules mathématiques)
- Un navigateur Web pré-configuré afin qu'il élimine les publicités présentes sur les pages Web et efface les cookies et l'historique de connexion à la fermeture.
- Un client de messagerie personnel pour que tout un chacun puisse configurer ses adresses courriel.
- Des logiciels éducatifs.
- Un atlas
- Un planétarium
- Des outils de dessin et de retouche d'images
- Un utilitaire pour numériser des documents
- Un outil pour apprendre la programmation
- Un créateur et correcteur de QCM.
- Un graveur de disques.
- Un lecteur multimédia.
- Des utilitaires (créateur d'étiquettes, logiciel de conjugaison ...)

Chaque client ne possède que le système d'exploitation et les applications. Il se connecte via le protocole NFS au serveur afin de gérer les données personnelles et parcours l'annuaire OpenLDAP pour l'authentification.

3.2 Système d'exploitation serveur

Le système d'exploitation pour le serveur est Debian 7. Véritable cœur du réseau, il remplit les fonctions suivantes :

- Hébergement et partage en réseau les données des utilisateurs en veillant aux droits d'accès.
- Assure le fonctionnement l'annuaire central de tous les utilisateurs, groupes d'utilisateurs et postes du réseau.
- Stockage de l'ensemble des base de données nécessaires aux applications.
- Hébergement le portail Web, l'accès aux fichiers à distance et le logiciel de bibliothèque.
- Assure le service de clonage en PXE.
- Propose la console d'administration du réseau E-ADMIN.
- Exécute les automates de maintenance du réseau.
- Réveille le réseau le matin ouvrés et pour les maintenances.
- Journalise les événements du réseau.

3.3 Miroir local de paquets

Le miroir local de paquets est une copie intégrale des dépôts de paquets Xubuntu utilisés par les postes clients. Cela permet de réduire drastiquement l'engorgement de la connexion à Internet lors de la mise à jour automatisée des postes clients.

3.4 Bases de données

Deux types de bases de données est en service sur le réseau :

Bases de données relationnelles SQL Propulsée par MySQL, ce système de gestion de base de données gère les bases de données suivantes :

- Bibliothèque : contient la liste des livres, les emprunts contractés et les avis des utilisateurs.
- Incidents : liste les tickets incidents créés par les usagers.
- Login : historique de connexion des utilisateurs sur les postes clients.
- Messagerie : stocke les messages envoyés depuis le logiciel de messagerie interne.
- Syslogng : journalise des événements sur le réseau.

Annuaire OpenLDAP Cette base de données est en charge de lister les utilisateurs, les groupes et les postes connectés sur le réseau. Elle sert de base pour l'authentification, la gestion des droits et les opérations sur les ordinateurs clients.

3.5 Contrôleur d'accès en télégestion

Un outil est en charge de contrôler les connexions faites sur l'interface de télégestion du réseau. Tout ordinateur tentant de se connecter 6 fois sans succès sur cette interface est banni à vie.

3.6 Supervision du serveur

Un ensemble de sondes sont mises en place sur le serveur afin de veiller à son bon fonctionnement. Ces sondes relèvent les mesures suivantes :

- Nombre de connexions sur le serveur Web.
- Nombre de sessions simultanées sur le serveur Web.
- Volume du trafic sur le serveur Web.
- Mesure des entrées/sorties des disques durs.
- Latence des disques durs.
- Taux d'utilisation des disques durs.
- Taux d'utilisation des nœuds d'index.
- Vitesse de traitement des disques durs.
- Taux d'utilisation des tampons de disques durs.
- Vitesse d'arrivée des messages d'alerte.
- Nombre de messages d'alerte.
- Temps de calcul du superviseur.
- Taux d'erreurs des communications réseau.
- Trafic réseau.
- Vitesse de traitement du pare-feux.
- Nombre d'hôtes bannis par le contrôleur d'accès en télégestion.
- Trafic du serveur d'échange de fichiers par type de requêtes.
- File d'attente du serveur d'impression.
- Nombre de processus.
- Nombre d'embranchement des processus.
- Classification de la priorité des processus.
- Utilisation de la mémoire virtuelle.
- Mesure de la température des BUS d'échange de RAM et de cœurs processeurs.
- Entropie disponible pour les algorithmes de chiffrement.
- Taux d'utilisation des cœurs processeurs.
- Utilisation de la table de fichiers.
- Mesure des interruptions systèmes individuelles.
- Taille de la table des nœuds d'index.
- Taux de charge général du serveur.
- Nombre d'utilisateurs connectés simultanément sur le serveur.
- Utilisation de la mémoire vive.
- Utilisation de la mémoire d'échange.
- Durée de fonctionnement du serveur.

Le résultat de ces mesures est consulté quotidiennement.

Voici un exemple des graphes obtenus *(fig. 4.3)*

3.7 Sauvegarde distante automatique

Afin de garantir la pérennité des données en cas de défaillance de plus de deux disques durs de données du serveur, une sauvegarde distante journalière est effectuée sur les serveurs de hubic, filiale cloud de l'hébergeur français OVH.

3.8 Clonage des clients en PXE

Le déploiement des images systèmes sur les postes clients est assuré par un système d'exploitation démarrable en réseau. Ce système réalisé en interne pour cette application s'intègre parfaitement aux besoins et remplit les fonctions suivantes dans cet ordre :

1. Récupère sur le serveur une adresse IP et un noyau contenant les outils de base pour continuer.
2. Récupère les outils supplémentaires et démarre l'automate de clonage.
3. L'automate de clonage va relever l'adresse matérielle de la carte réseau et consulter l'annuaire pour récupérer son numéro de poste. Si elle n'existe pas, l'utilisateur est invité à saisir le numéro du poste *(fig. 4.4)*.
4. Le poste est formaté et la dernière image du système d'exploitation client est installée.
5. L'automate va alors modifier les paramètres de cette installation afin de correspondre aux valeurs affectées à ce poste.
6. Il effectue une collecte des données utiles et met à jour l'annuaire.
7. Le système redémarre sur le système d'exploitation nouvellement installé.

Cette procédure entièrement automatique permet le déploiement rapide des nouvelles images systèmes.

3.9 Console d'administration du réseau E-ADMIN

Véritable plate-forme centrale de gestion du réseau, E-ADMIN *(fig. 4.5)* est un outil développé en interne permettant à l'administrateur de gérer rapidement et simplement la plupart des opérations courantes à effectuer sur le réseau. Voici la liste des opérations possibles depuis cette console :

- Créer une classe (de manière unique ou depuis un fichier CSV).
- Supprimer une classe.
- Exporter une classe au format CSV.
- Imprimer une liste d'utilisateurs.
- Purger les classes : révoquer les élèves qui les composent.
- Créer un compte élève.
- Supprimer un compte élève.
- Révoquer un élève.
- Intégrer un élève.
- Supprimer les élèves non-affectés.
- Réinitialiser la session d'un élève.
- Lire/éditer les tickets incidents.
- Imprimer les tickets incidents.
- Consulter l'état des postes (éteint, allumé et disponible, allumé et occupé par un utilisateur).
- Allumer les postes.
- Exécuter une commande système sur les postes du réseau.
- Mettre à jour et arrêter les postes.
- Arrêter les postes.
- Réinitialiser un mot de passe utilisateur.
- Consulter l'annuaire.
- Consulter la messagerie interne.
- Afficher l'historique de connexion.
- Prendre un cliché de l'écran d'un poste.
- Envoyer une fenêtre de notification à un utilisateur connecté.

L'ensemble de ces actions permettent à l'administrateur d'intervenir sur le réseau et ainsi corriger un problème rapidement.

3.10 Maintenance automatisée

La maintenance automatique du réseau est effectuée sur des tranches horaires différentes : *(table 3.1)*

3.11 Automate de portage réseau 2 vers réseau 3

Lors de la refonte du réseau entre mars 2013 et août 2013, le remplacement de l'annuaire NIS par l'annuaire OpenLDAP à nécessité la migration des données et la reconstruction de l'arborescence des données personnelles. Afin de remplir cette tâche, un automate à été développé en interne et à porté avec succès les données et annuaire du réseau 2 vers le nouveau serveur.

3.12 Détecteur de sessions non clôturées

Lors de l'arrêt automatique des postes clients (cf. sous-section 3.10 et table 3.1), l'automate de détection des sessions non clôturées, réalisé en interne, vérifie sur chaque poste client si un utilisateur à omis de se déconnecter. Si c'est le cas, il le déconnecte et lui envoie un message sur la messagerie interne afin de lui rappeler qu'il doit se déconnecter lors de son départ du poste.

3.13 Constructeur d'arborescence

En cas de destruction partielle ou totale ou en cas de migration sur une nouvelle infrastructure, un constructeur d'arborescence permet de bâtir les répertoires de base et la structure des base de données du réseau. Réalisé en interne, il à été développé lors de la migration vers le réseau 3 et révisé pour le réseau 4.

3.14 Contrôleur d'attribution de droits d'accès

Afin de garantir les droits d'accès aux fichiers à leurs propriétaires, un automate de contrôle d'attribution des droits d'accès réalisé en interne est mis en place et exécuté toutes les minutes. Cela permet de respecter le schéma d'attribution des droits suivant *(table 3.2)*.

3.15 Automate de réveil du réseau

Pour que les postes clients soient facilement accessibles par les utilisateurs, ils sont préalablement démarrés tous les matins ouvrés à 7 :30. Cet automate, développé en interne, va consulter l'annuaire pour obtenir les informations sur les machine : chaque ajout ou remplacement de poste cloné avec l'outil de clonage (cf. 3.8) est automatiquement pris en charge par l'automate de réveil du réseau. Il est également actionné le soir à 21 :00 *(table 3.1)* pour la mise à jour des postes clients.

3.16 Outil de journalisation des connexion

Afin d'améliorer la qualité du dépannage et pour des raisons de traçabilité, un outil de journalisation des connexion développé en interne est mis en place. Il permet de savoir qui s'est connecté sur un poste du réseau, ainsi que l'horodatage de cette connexion.

Horaire	**Automate**	**Action**
Tous les jours à 03 :00	Synchronisation NTP	Synchronisation de l'horloge du serveur sur les horloges atomiques.
	Sauvegarde OpenLDAP	Sauvegarde de l'annuaire.
	Suppression `*.lock`	Suppression des résidus de fichiers de vérouillage LibreOffice.
	Upgrade serveur	Mise à jour logicielle du serveur.
	Freshclam	Mise à jour de la base antivirale ClamAV.
	Clamscan	Scan antiviral avancé de toutes les données du réseau.
	Backup	Sauvegarde des données sur le cloud Hubic.
Les jours ouvrés à 07 :30	Réveil réseau	Réveil des postes clients du réseau.
Tous les jours à 12 :00	Sync mirror	Synchronisation du miroir de paquets.
Tous les jours à 21 :00	Sync mirror	Synchronisation du miroir de paquets.
	Réveil réseau	Réveil des postes clients du réseau.
	Upgrade client	Mise à jour logicielle des clients.
Toutes les minutes	Contrôle droits	Passe du contrôleur d'attribution de droits d'accès.

TABLE 3.1 – Table des maintenances automatiques

Émetteur	**Propriétaire**			**Professeur**			**Classe**			**Autres profs**		
	R	W	X	R	W	X	R	W	X	R	W	X
Élève	•	•		•	•					•		
Professeur (répertoire personnel)	•	•		•	•					•		
Professeur (ressources)	•	•		•	•		•			•		
Ressources publiques	•	•	○	•		○	•		○	•		○
Autres utilisateurs (hors admin)	•	•										
Administrateur	•	•	○									

Légende :

• Appliqué à tous les fichiers.

○ Appliqué à certains fichiers.

R Droits en lecture (*Read*)

W Droits en écriture (*Write*)

X Droits en exécution (*eXecution*)

TABLE 3.2 – Table d'attribution des droits

Chapitre 4

Logiciels

4.1 Logiciel de bibliothèque

Le logiciel de bibliothèque remplace le logiciel La BCD, installé auparavant sur le poste de bibliothèque. Il ne donnait pas entière satisfaction pour les causes suivantes :

- L'interface du programme n'était pas ergonomique. L'utilisation était sans cesse interrompue par des fenêtres d'informations bloquant l'action en cours.
- Son schéma de base de données était obsolète. son
- Il comportait sa propre base de données élèves, indépendante de l'annuaire central. Sa mise à jour était fastidieuse.
- Il s'agit d'un *shareware* : un logiciel qui peut être utilisé gratuitement durant une certaine période ou avec des fonctionnalités limitées. Après cette période d'essai, l'utilisateur doit rétribuer l'auteur s'il veut continuer à utiliser le logiciel ou avoir accès à la version complète.
- Il était mis à disposition sur un seul poste. Il était impossible de le déployer en réseau.

Nous avons donc procédé à un export des données contenues dans ce logiciel et l'importer dans une base de données dans le serveur. Nous avons développé un nouveau logiciel disponible sur l'intranet afin d'exploiter cette base de données *(fig. 4.2)*. Ce programme remplit des fonctions suivantes :

- Enregistrer rapidement des emprunts de livres en respectant le quota maximal de livres, défini par la bibliothécaire.
- Retourner chaque livre en renseignant son numéro et demande l'avis de l'emprunteur sur l'ouvrage.
- Rechercher rapidement un ouvrage dans la collection des livres papier ainsi que dans les ressources numériques du domaine public.
- Rechercher avec plusieurs critères dans la collection des livres papier et imprimer le résultat des recherches.
- Demander une recommandation de lecture, obtenue à partir des anciens emprunts et des emprunts des autres utilisateurs.
- Lister, ajouter, modifier les différents livres de la collection et imprimer la liste des ouvrages.
- Lister et imprimer la liste des livres empruntés et des emprunts retardataires.
- Imprimer les étiquettes des livres avec code-barre. Le logiciel est prêt à accueillir un lecteur de code-barres pour faciliter la saisie des emprunts et des retours.
- Configurer les préférences du programme (nombre de résultats par page ...)

4.2 Portail Web interne/externe

Le portail Web, développé en interne, offre divers services aux utilisateurs et aux visiteurs. Ce portail s'adapte en fonction de votre lieu de connexion :

Mode interne Disponible dans le réseau *intra muros*, il permet d'accéder au logiciel de bibliothèque, à la documentation du réseau, au moteur de recherche de ressources et aux sites des classes.

Mode externe Disponible depuis l'Internet, il permet d'accéder au service d'accès aux fichiers à distance, au moteur de recherche de ressources et aux sites des classes.

4.3 Accès aux fichiers à distance net2ftp

L'accès aux fichiers à distance pour les professeurs peut se faire de deux manières :

- Connexion en FTP vers le serveur de l'école.
- Gestion depuis l'interface Web net2ftp *(fig. 4.6)*.

La seconde option permet de se connecter simplement et sans l'ajout de programmes supplémentaires depuis n'importe que ordinateur doté d'un navigateur Internet récent et connecté à Internet. Depuis cette interface, modifiée pour les besoins spécifiques du réseau, les enseignants et le personnel de l'école peut télécharger et téléverser de fichiers entre son ordinateur personnel, sa

tablette, son smartphone . . . vers le serveur central. Elle permet également de copier, déplacer, supprimer directement sur le serveur central mais en respectant toujours les droits d'accès.

4.4 Sites Internet pour les classes

Afin d'étoffer les supports d'enseignements et permettre aux classes de communiquer de manière indépendantes, chaque classe dispose d'un espace de stockage sur le serveur afin d'héberger un site Internet. Cela peut constituer un projet pédagogique afin de familiariser les élèves aux outils actuels de l'informatique, un espace d'échange pour les professeurs ou enfin d'un support de cours.

Un site Web créé à partir d'un logiciel de création de site Web (Kompozer (installé sur les postes du réseau), nvu, Dreamweaver . . .) ou codé manuellement peut être hébergé (HTML 5, CSS 3). Le serveur peut accueillir également des pages PHP 5 et une base de données MySQL peut-être ouverte sur demande.

4.5 Gestionnaire de classes

Il était nécessaire de permettre aux professeurs de gérer eux-même les élèves qui composent leurs classes. C'est pourquoi le programme de gestion des classes *(fig. 4.7)*, développé en interne, permet de réaliser les tâches suivantes :

- Créer une classe.
- Supprimer une classe.
- Créer un compte élève.
- Supprimer un compte élève.
- Révoquer un élève.
- Intégrer un élève.
- Supprimer les élèves non-affectés.
- Réinitialiser la session d'un élève.
- Imprimer une liste d'utilisateurs généré automatiquement.

4.6 Moteur de recherche pour ressources multimédia libres

La mise à la disposition de ressources multimédias libres de droits aux enseignants est assurée par les moteurs de recherche de ressources du portail *(fig. 4.8)* qui permettent de parcourir :

- des images (Images gratuites Pixabay)
- des articles encyclopédiques (Encyclopédie Wikipedia)
- des livres (Textes Wikisource)
- des cartes géographiques (Cartographie OpenStreetMap)
- des définitions de dictionnaire (*Dictionnaire de la langue française*, Émile Littré)

4.7 Messagerie interne

Cet outil permet aux différents utilisateurs du réseau de communiquer via un système de messagerie interne *(fig. 4.9)*, réalisé en interne. Cet outil permet également de former les élèves aux courriels, sans risque car le système est sciemment conçu pour ne pas communiquer avec d'autres services de messagerie tiers et sans configuration préalable car il se configure automatiquement. Ce système permet à tout utilisateur d'échanger des messages selon les droits suivants : *(table 4.1)*. Le système de messagerie est également utilisé par l'automate de détection de sessions non clôturées.

4.8 Outil de modification de mot de passe

L'outil de modification de mot de passe *(fig. 4.10)* permet aux professeurs de modifier leur mot de passe de session, conformément à la politique de sécurité appliquée aux mots de passe du réseau. Il intègre également un générateur de mot de passe aléatoire aisément mémorisable, basé sur trois mots courants aléatoires concaténés par un caractère spécial (espace - _ .) suivis de trois chiffres aléatoires *(fig. 4.11)*.

4.9 Outil de signalement d'incidents

Pour une gestion plus efficace des tickets utilisateurs, un outil de signalement d'incidents *(fig. 4.12)*, développé en interne permet de créer rapidement un ticket incident et de le suivre. Le logiciel collecte automatiquement des données supplémentaires pour améliorer le traitement du ticket (horodatage, utilisateur, numéro de poste émetteur). Ces données permettent d'accéder à la journalisation de l'incident afin de le corriger au mieux.

Expéditeur ↓	Élèves (classe)	Élèves (tous)	Enseignant (classe)	Enseignant (tous)	Directrice et admin.
Élève	•		•		
Enseignant	•	•	•	•	•
Directrice et admin.	•	•	•	•	•

Légende :

- Autorisé

TABLE 4.1 – Droits d'envois selon l'expéditeur

FIGURE 4.1 – Capture d'écran d'un poste client.

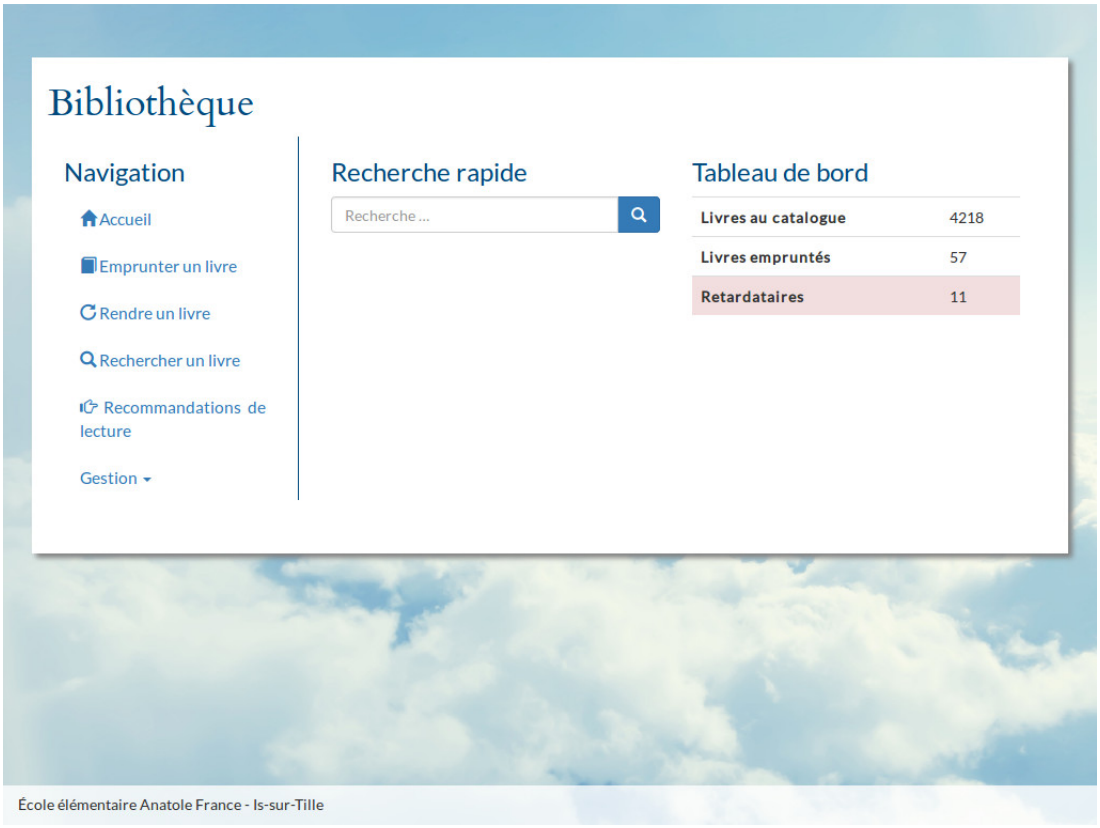

FIGURE 4.2 – Capture d'écran du logiciel de bibliothèque.

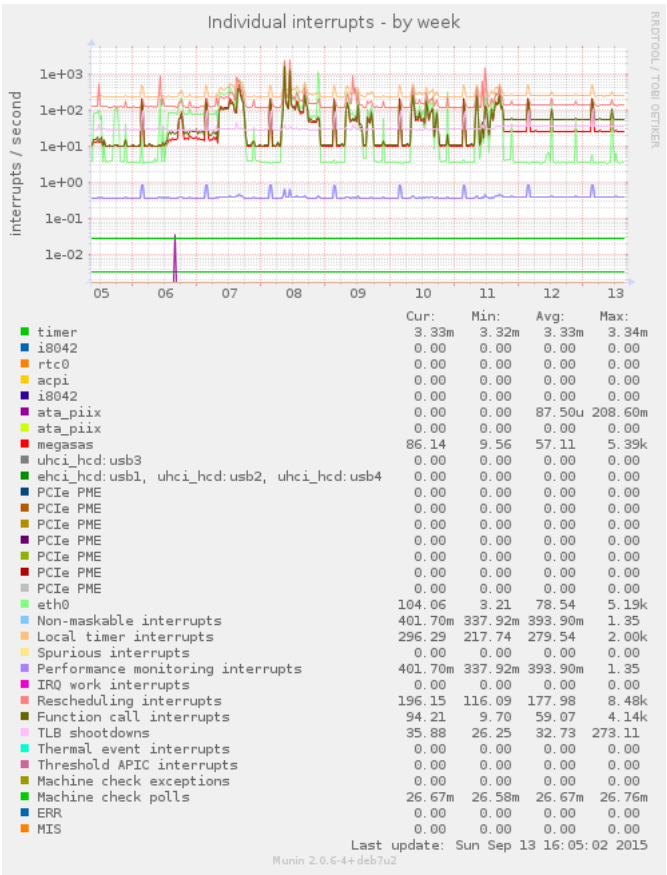

FIGURE 4.3 – Exemple de graphes obtenu par le superviseur.

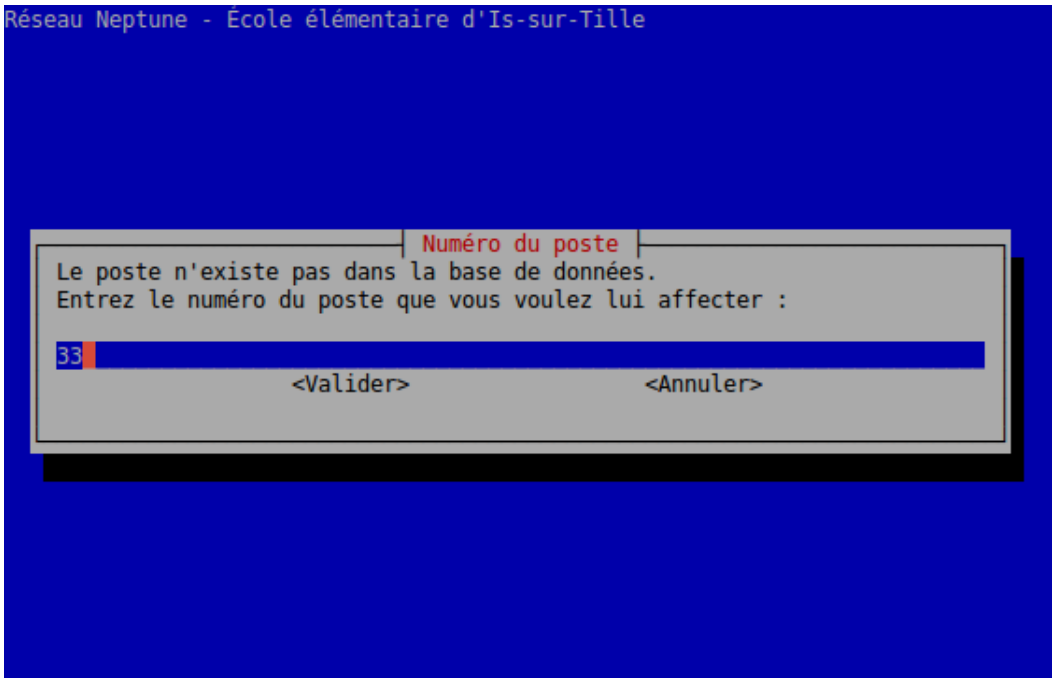

FIGURE 4.4 – Le cloneur en réseau demandant le numéro du poste.

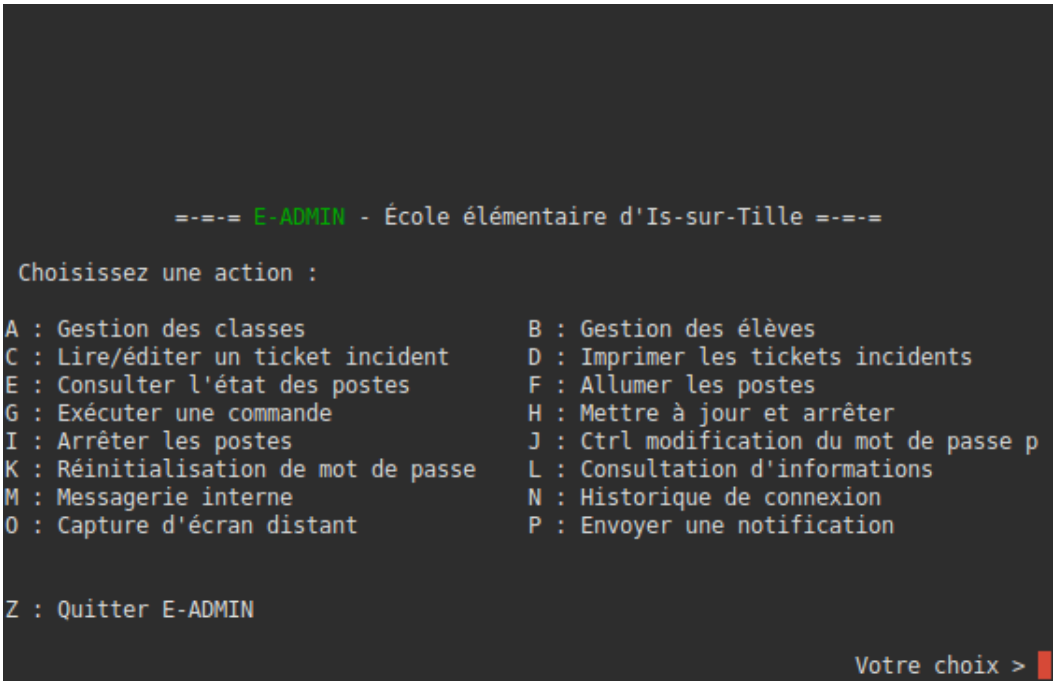

FIGURE 4.5 – Console d'administration du réseau E-ADMIN.

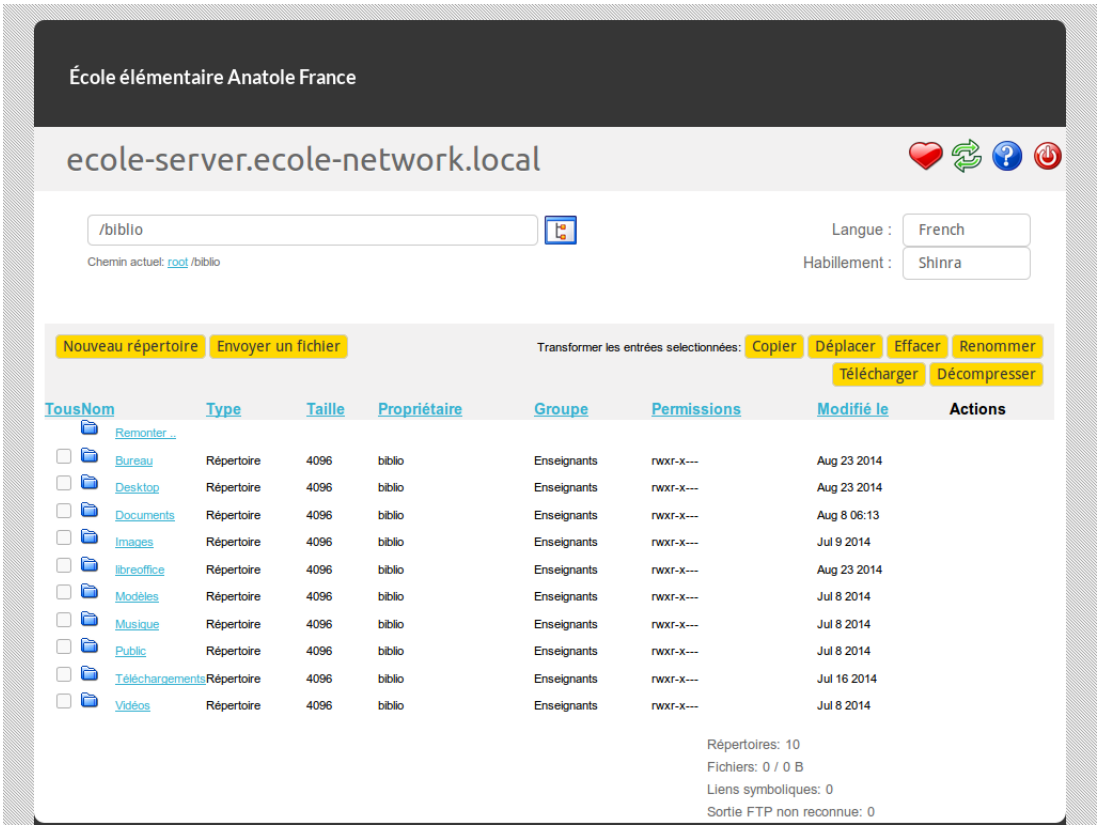

FIGURE 4.6 – Interface d'accès aux fichiers à distance net2ftp.

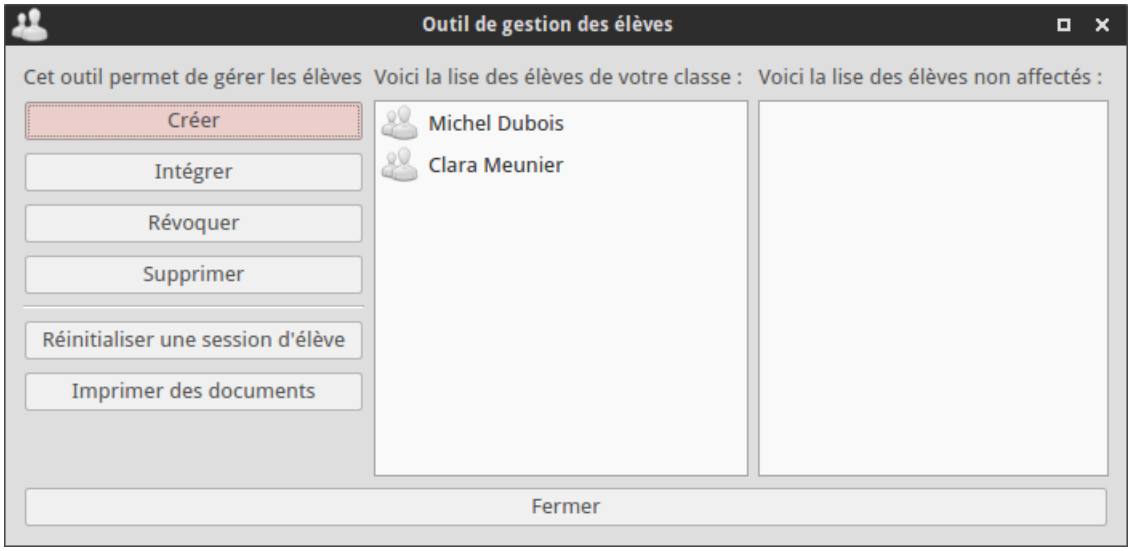

FIGURE 4.7 – Gestionnaire d'utilisateurs.

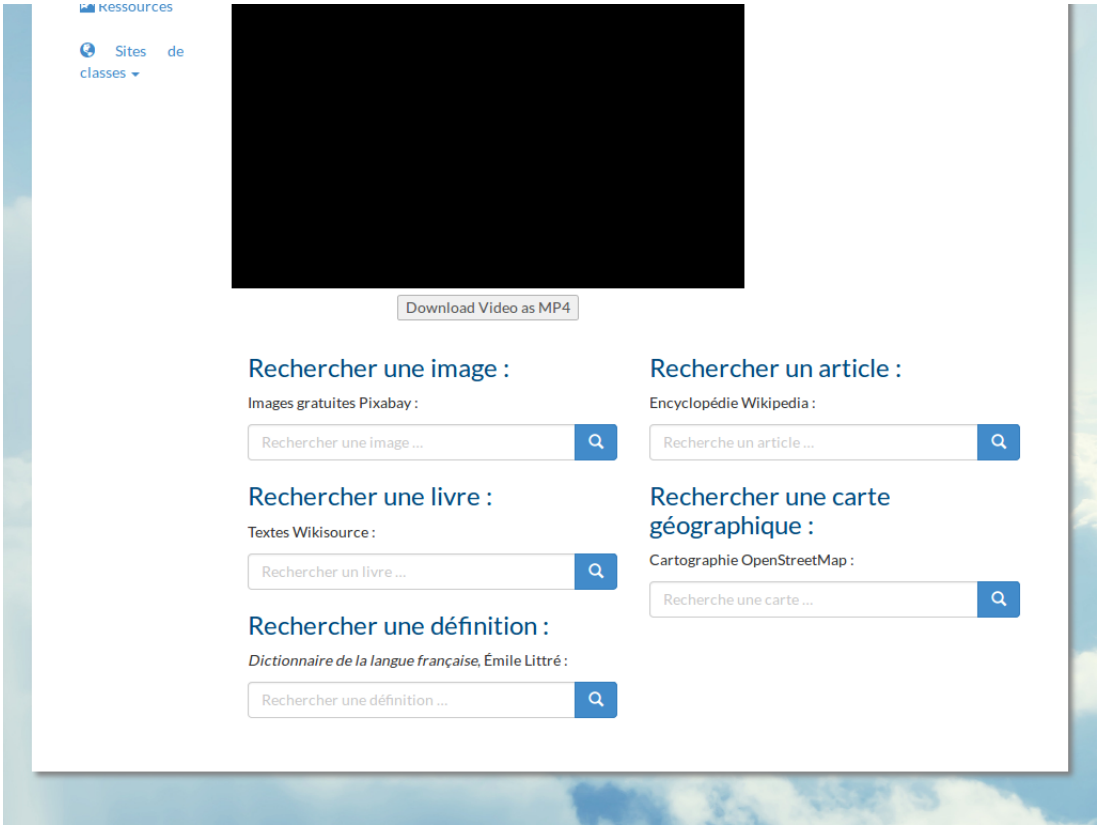

FIGURE 4.8 – Moteurs de recherche de ressources libres de droits.

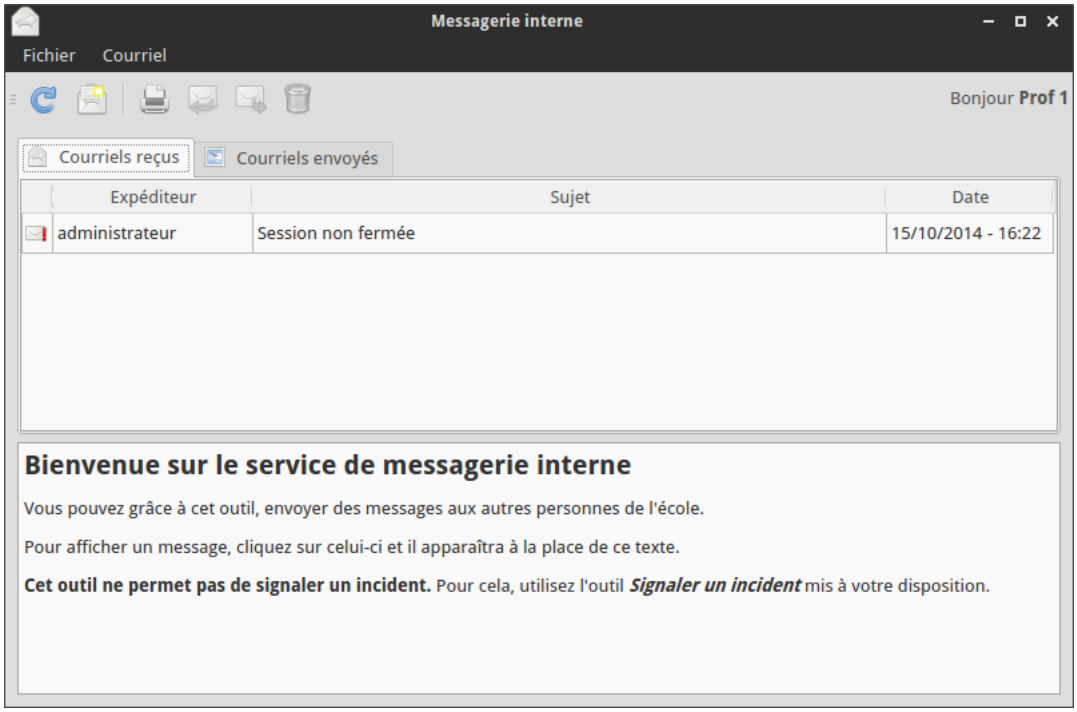

FIGURE 4.9 – Client de messagerie interne.

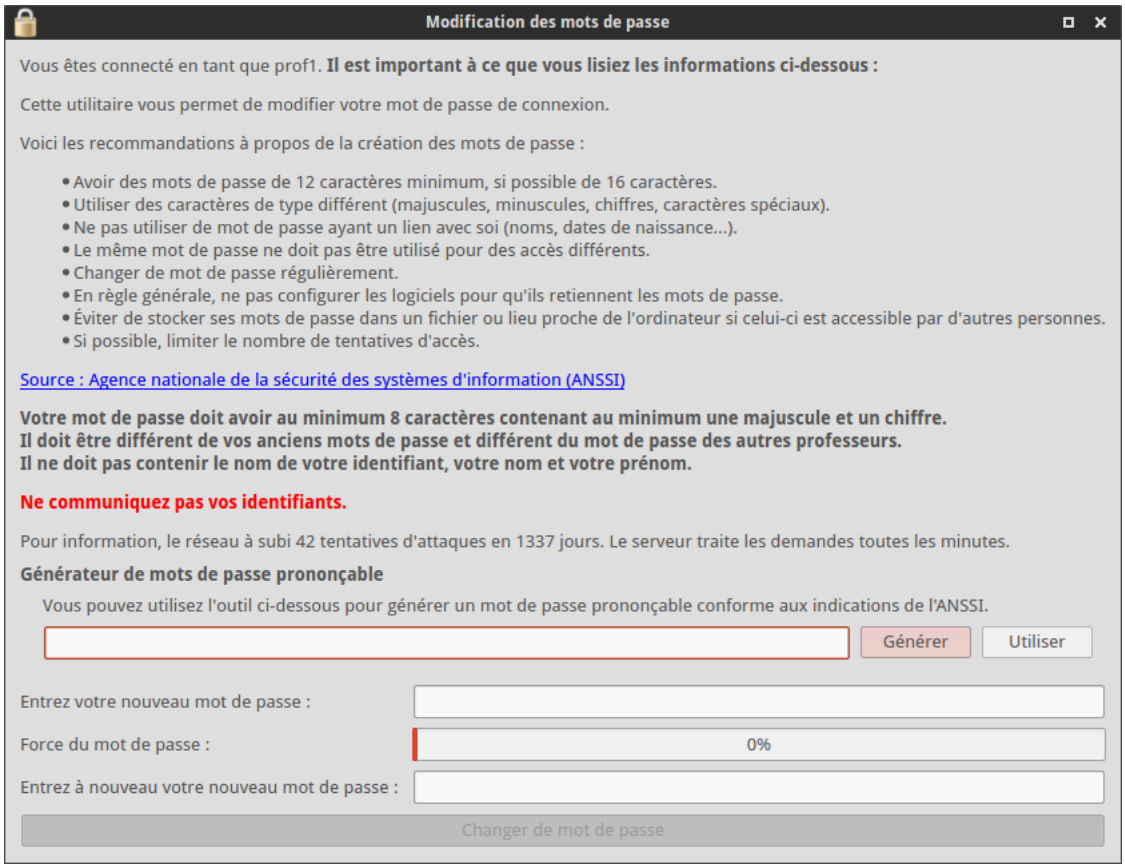

FIGURE 4.10 – Outil de modification de mot de passe.

```
Cloche_Puzzle_Car_627
Bec-Cahier-Ferme-265
Carotte.Plume.Plage.194
Sable Ciel Col 003
Liquide_Pluie_Lecture_318
Cube_Vitre_Journaux_066
Lundi-Paysage-Vase-768
Marchand_Poutre d'équilibre_Épluchure_096
Chasseur-Dessert-Goût-032
Jean Marionnette Châtaigne 728
```

FIGURE 4.11 – Exemples de mots de passes générés.

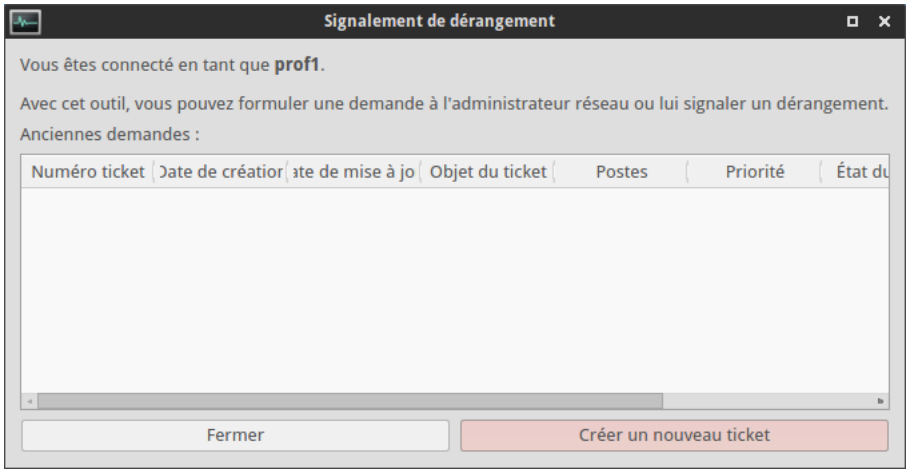

FIGURE 4.12 – Outil de signalement des incidents.

Chapitre 5

Sécurité

La sécurité du réseau est un des objectifs principaux lors de la réalisation des différentes versions du réseau. Les objectifs en terme de sécurité sont les suivants :

- Protéger les infrastructures des attaques intérieures et extérieures.
- Garantir la disponibilité du service en évitant les erreurs et les opérations malines des utilisateurs.
- Garantir la confidentialité des données de chacun dans son espace personnel.
- Protéger le réseau contre les attaques visant à le transformer en *botnet* (ici, le mot *botnet* désigne les réseaux de machines zombies, utilisés pour des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DoS) ...)

Cela se traduit par la mise en place des systèmes suivants :

- Mise à jour quotidienne des systèmes d'exploitations clients et serveur afin de corriger rapidement les erreurs et les failles de sécurité. Cela permet de réduire le temps d'exposition à l'exploitation des exploits.
- Restrictions d'accès à SSH. Seul l'administrateur, *via* une session spécialisée et dénuée de droits sur le réseau, peut se connecter avec un certificat RSA de 2048 bits. L'escalade vers le compte administrateur permettant d'opérer sur le réseau se fait au moyen d'un mot de passe dont la taille est supérieure à 20 caractères. Toute tentative infructueuse bannit automatiquement et de manière irrévocable l'ordinateur source.
- L'administration des clients depuis le serveur se fait *via* SSH avec un second certificat RSA de 2048 bits. Une session de maintenance sur site est également protégée par un mot de passe.
- La salle serveur est protégée physiquement par une porte verrouillée à clef.
- Chaque utilisateur n'est doté que des droits nécessaires afin de mener à bien ses travaux quotidiens. Aucun droit supplémentaire n'est octroyé. Toute erreur ou action malicieuse effectuée depuis un compte utilisateur ne peut affecter le fonctionnement logiciel d'un poste client ni de l'ensemble du réseau.
- Séparation des sessions de chaque individu pour lui garantir un espace personnel de travail. Il peut ainsi le personnaliser à loisir sans qu'il soit altéré par un utilisateur tiers.
- La supervision régulière du réseau permet de relever rapidement toute anomalie de fonctionnement caractéristique d'une attaque.
- La sauvegarde des données permet en cas de perte de données de les restaurer.
- La journalisation des événements permet de retracer l'historique des postes et de déterminer si il y à eu attaque, par quel moyen, de la contrer et de s'en prémunir.
- La politique sur les mots de passe impose pour les professeurs l'usage d'un mot de passe robuste et la modification régulière de celui-ci afin de prévenir les attaques effectuées depuis leurs comptes car ils ont accès au service d'accès aux fichiers à distance.
- L'accès aux bases de données est sécurisé par l'utilisation de comptes spécialisés, associés à des droits restreints, réservées aux applications. L'accès direct aux bases de données par les utilisateurs est proscrite.

L'application de cette politique de sécurité à permis de contrer le grand flot d'attaques (960 attaques produites par 160 attaquants bloqués en 43 jours *(fig. 5.1)*), principalement en provenance d'automates d'attaque visant dans discernement l'ensemble des ordinateurs connectés à Internet.

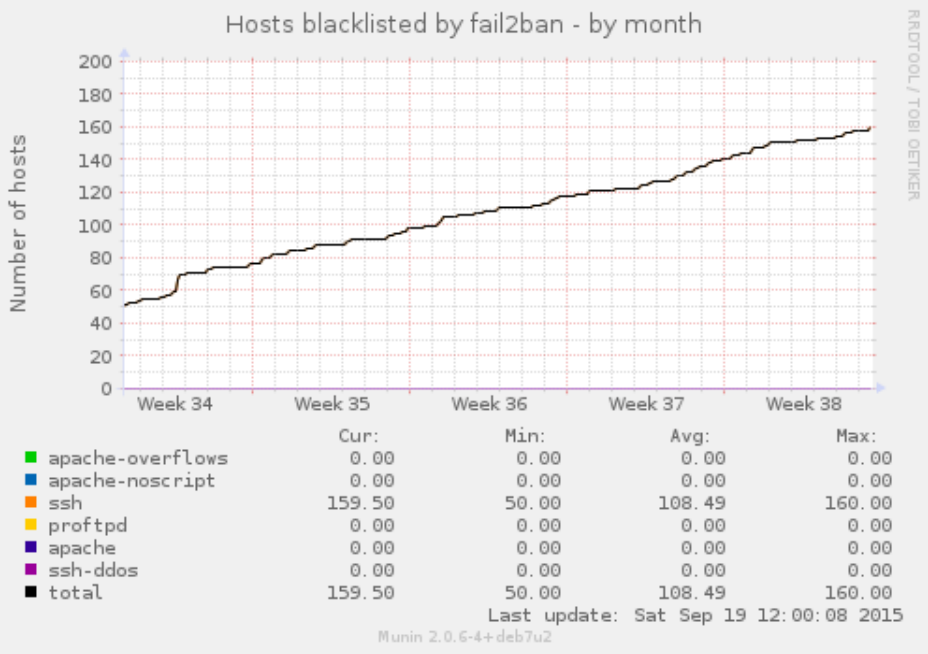

FIGURE 5.1 – Évolution du nombre d'attaquants bannis pendant un mois.

Chapitre 6

Améliorations possibles du réseau

Des services et des fonctionnalités supplémentaires peuvent être mises en place afin d'améliorer la qualité, l'ergonomie, la sécurité de l'infrastructure. Voici une liste non exhaustive des améliorations pouvant être apportées :

- Mise en place d'un serveur mandataire.
- Ajout de la fonctionnalité multicast sur l'outil de clonage réseau.
- Portage de certaines applications sous la forme d'applications Web.
- Création d'un logiciel d'examen.
- Mise en place d'une carte à code-barre par utilisateur et d'une étiquette à code-barre par livre pour accélérer l'emprunt et le retour des ouvrages.
- Rendre la messagerie interne disponible à distance.
- Mettre en place un logiciel de supervision de la classe pour qu'un enseignant puisse voir en temps réel l'écran de chaque élève.
- Virtualiser l'infrastructure sur un cluster pour augmenter la disponibilité.

L'ensemble des fonctionnalités principales sont en service et ne nécessitent pas de refontes totales telles que rencontrées lors du passage du réseau 1 au réseau 2 et lors du réseau 2 vers le réseau 3.

Chapitre 7

Conclusion

Cette installation est conçue sur mesure et à l'échelle de cette école et permet d'exploiter au mieux toutes les ressources matérielles en place en apportant la souplesse de la mise en réseau des équipements. Cela à permis de s'affranchir de l'ancienne architecture "un poste = une fonction" qui induisait une faible disponibilité de la ressource et la multiplication des points individuels de défaillance. La mise en réseau à réduit cette vulnérabilité et permet d'accéder à un programme ou une donnée depuis le réseau *intra muros* et depuis l'extérieur.

La conception d'applications sur-mesure et l'intégration des produits existants ont permis de fournir un bouquet cohérent d'applications ayant pour socle les bases de données centrales, permettant une convergence des données, évitant les redondances et permettant des mises à jour aisées et rapides.

La mise en place de divers outils de travail à distance (portail, accès aux fichiers à distance ...) permet une plus grande souplesse dans les emplois du temps des enseignants qui peuvent désormais accéder aux services depuis n'importe quel ordinateur connecté à Internet et allège de ce fait les contraintes liées à la nécessité de se trouver sur le site sur le poste contenant la ressource pour pouvoir travailler. Cela est le commencement du télétravail pour les enseignants.

La fiabilisation et l'harmonisation de l'infrastructure globale a simplifié les contraintes aux utilisateurs. Il est désormais plus aisé par exemple d'imprimer un document sur le photocopieur ou de consulter la liste des ouvrages emprunts pour une classe.

Enfin, il est à noter que ces travaux ont permis d'améliorer la qualité de l'enseignement dispensé aux élèves en matière d'informatique et ont fournis aux enseignants un outil fiable et facile d'utilisation pour la gestion de l'information.

Annexe A

Schéma de l'infrastructure actuelle

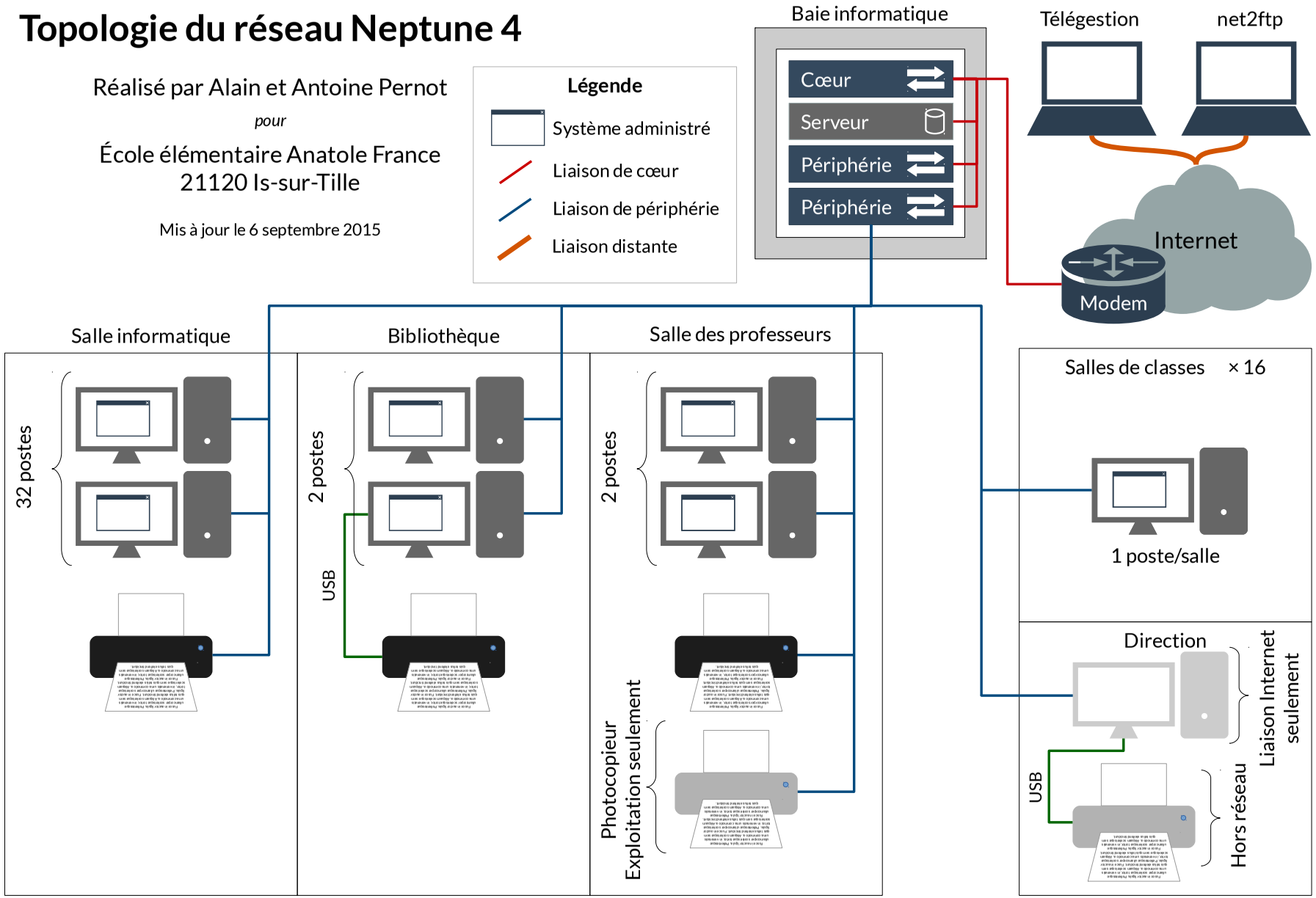

FIGURE A.1 – Topologie actuelle du réseau

Glossaire

ClamAV (« Clam AntiVirus »), est un logiciel antivirus pour UNIX. Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant des virus. Les virus ciblés sont très majoritairement des virus s'attaquant au système d'exploitation Microsoft Windows et non pas aux systèmes sur lesquels ClamAV s'installe, qui sont peu menacés par les virus. 11

CSS Les feuilles de style en cascade, généralement appelées CSS de l'anglais Cascading Style Sheets, forment un langage informatique qui décrit la présentation des documents HTML et XML. Les standards définissant CSS sont publiés par le World Wide Web Consortium (W3C). Introduit au milieu des années 1990, CSS devient couramment utilisé dans la conception de sites web et bien pris en charge par les navigateurs web dans les années 2000.

L'un des objectifs majeurs des CSS est de permettre la mise en forme hors des documents. Il est par exemple possible de ne décrire que la structure d'un document en HTML, et de décrire toute la présentation dans une feuille de style CSS séparée. Les styles sont appliqués au dernier moment, dans le navigateur web des visiteurs qui consultent le document. Cette séparation fournit un certain nombre de bénéfices, permettant d'améliorer l'accessibilité, de changer plus facilement de présentation, et de réduire la complexité de l'architecture d'un document. 14

CSV Comma-separated values, connu sous le sigle CSV, est un format informatique ouvert représentant des données tabulaires sous forme de valeurs séparées par des virgules.

Ce format n'a jamais vraiment fait l'objet d'une spécification formelle. Toutefois, la RFC 4180 décrit la forme la plus courante et établit son type MIME « text/csv », enregistré auprès de l'IANA.

Un fichier CSV est un fichier texte, par opposition aux formats dits « binaires ». Chaque ligne du texte correspond à une ligne du tableau et les virgules correspondent aux séparations entre les colonnes. Les portions de texte séparées par une virgule correspondent ainsi aux contenus des cellules du tableau.

Une ligne est une suite ordonnée de caractères terminée par un caractère de fin de ligne (line break - CRLF), la dernière ligne pouvant en être exemptée. 9

Debian désigne les systèmes d'exploitations développés par l'organisation communautaire éponyme, réunit autour d'un noyau de système d'exploitation de nombreux éléments pouvant être développés indépendamment les uns des autres, pour plusieurs architectures matérielles. Ces éléments, programmes de base complétant le noyau et logiciels applicatifs, se présentent sous forme de « paquets » qui peuvent être installés en fonction des besoins. L'ensemble système d'exploitation plus logiciels s'appelle une distribution. 4, 7

DoS Une attaque par déni de service (denial of service attack, d'où l'abréviation DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier ;
- également le fait d'envoyer des milliards d'octets à une box internet.

L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriel dans une entreprise.

L'attaquant hacker n'a pas forcément besoin de matériel sophistiqué. Ainsi, certaines attaques DoS peuvent être exécutées avec des ressources limitées contre un réseau beaucoup plus grand et moderne. On appelle parfois ce type d'attaque « attaque asymétrique » (en raison de la différence de ressources entre les protagonistes). Un hacker avec un ordinateur obsolète et un modem lent peut ainsi neutraliser des machines ou des réseaux beaucoup plus importants.

Les attaques en déni de service se sont modifiées au cours du temps. Tout d'abord, les premières n'étaient perpétrées que par un seul « attaquant » ; rapidement, des attaques plus évoluées sont apparues, impliquant une multitude de « soldats », aussi appelés « zombies ». On parle alors de DDoS (distributed denial of service attack). Ensuite, les attaques DoS et DDoS étaient perpétrées par des hackers seulement attirés par l'exploit et la renommée. Ainsi, certains hackers se sont spécialisés

dans la « levée » d'armées de « zombies », qu'ils peuvent ensuite louer à d'autres hackers pour attaquer une cible particulière. Avec la forte augmentation du nombre d'échanges commerciaux sur Internet, le nombre de chantages au déni de service a très fortement progressé (un cracker lance une attaque en DoS ou DDoS contre une entreprise et lui demande une rançon pour arrêter cette attaque). 21

FTP File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. 4, 13

HTML L'Hypertext Markup Language, généralement abrégé HTML, est le format de données conçu pour représenter les pages web. C'est un langage de balisage permettant d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des programmes informatiques. Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec des langages de programmation (JavaScript) et des formats de présentation (feuilles de style en cascade). HTML est initialement dérivé du Standard Generalized Markup Language (SGML). 14

Kubuntu est un système d'exploitation libre de type GNU/Linux. C'est un projet visant à utiliser l'environnement graphique KDE à la place de Unity au sein d'Ubuntu. Le projet Kubuntu n'est pas une distribution dérivée d'Ubuntu, car tous deux partagent exactement la même base, les mêmes logiciels, les mêmes dépôts APT, le même nom de code et le même cycle de développement. 3

Mandriva Linux (anciennement Mandrakelinux) est un système d'exploitation développé par l'entreprise Mandriva de 1998 à 2012. Ciblant à la fois le grand public et les professionnels, cette distribution GNU/Linux est construite autour de l'environnement graphique KDE.

Mandriva ayant abandonné le projet, il est devenu entièrement communautaire, repris par l'association OpenMandriva pour devenir OpenMandriva LX. 3

multicast Le multicast (qu'on pourrait traduire par « multidiffusion ») est une forme de diffusion d'un émetteur (source unique) vers un groupe de récepteurs. Les termes « diffusion multipoint » ou « diffusion de groupe » sont également employés.

Les récepteurs intéressés par les messages adressés à ce groupe doivent s'inscrire à ce groupe. Ces abonnements permettent aux switchs et routeurs intermédiaires d'établir une route depuis le ou les émetteurs de ce groupe vers les récepteurs de ce groupe.

Ce système est plus efficace que l'unicast pour diffuser des contenus simultanément vers une large audience. En streaming unicast, on enverrait l'information autant de fois qu'il y a de connexions, d'où gaspillage de temps, de ressources du serveur et surtout de bande passante. Au contraire, en multicast, chaque paquet n'est émis qu'une seule fois et sera routé vers toutes les machines du groupe de diffusion sans que le contenu ne soit dupliqué sur une quelconque ligne physique ; c'est donc le réseau qui se charge de reproduire les données.

Le multicast permet de développer des applications interactives de groupe, comme la visioconférence, le partage de tableau, etc. 23

MySQL est un serveur de bases de données relationnelles SQL développé dans un souci de performances élevées en lecture, ce qui signifie qu'il est davantage orienté vers le service de données déjà en place que vers celui de mises à jour fréquentes et fortement sécurisées. Il est multi-thread et multi-utilisateur.

C'est un logiciel libre, open source, développé sous double licence selon qu'il est distribué avec un produit libre ou avec un produit propriétaire. Dans ce dernier cas, la licence est payante, sinon c'est la licence publique générale GNU (GPL) qui s'applique. 7, 14

net2ftp est une interface Web qui permet de se connecter à un espace FTP depuis n'importe quel navigateur, d'uploader des fichiers et dossiers, de créer des fichiers, les éditer. 4, 13

NFS Network File System (ou NFS, système de fichiers en réseau) est à l'origine un protocole développé par Sun Microsystems en 1984 qui permet à un ordinateur d'accéder à des fichiers via un réseau. Il fait partie de la couche application du modèle OSI et utilise le protocole RPC. 3, 4, 7

NIS Network Information Service (NIS) nommé aussi Yellow Pages est un protocole client serveur développé par Sun permettant la centralisation d'informations sur un réseau UNIX.

Son but est de distribuer les informations contenues dans des fichiers de configuration contenant par exemple les noms d'hôte (/etc/hosts), les comptes utilisateurs (/etc/passwd), ... sur un réseau.

Un serveur NIS stocke et distribue donc les informations administratives du réseau, qui se comporte ainsi comme un ensemble cohérent de comptes utilisateurs, groupes, machines, ... 4, 9

NTP Le Protocole d'Heure Réseau (Network Time Protocol ou NTP) est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.

La version 4 de NTP est une révision importante publiée dans la RFC 5905 en juin 2010.

Le NTP est un protocole permettant de synchroniser l'horloge d'un ordinateur avec celle d'un serveur de référence. NTP est un protocole basé sur UDP et utilise le port 123.

Le protocole NTP comprend :
- une partie architecture,
- une partie messagerie,
- et une partie algorithmique.

Sans une bonne synchronisation des horloges de tous les systèmes communicants entre eux, certains services ne sont pas utilisables correctement. C'est ainsi que rapidement, il a été nécessaire de définir des méthodes permettant de synchroniser les horloges sur une heure de référence. Dans le cas de NTP, ce dernier utilise le temps universel coordonné (UTC). 11

OpenLDAP est une implémentation libre du protocole LDAP maintenue par le projet OpenLDAP et distribuée selon les termes de la licence OpenLDAP Public Licence.

Lightweight Directory Access Protocol (LDAP) est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs. LDAP est moins complexe que le modèle X.500 édicté par l'UIT-T. 4, 7–9, 11

PHP PHP : Hypertext Preprocessor, plus connu sous son sigle PHP (acronyme récursif), est un langage de programmation libre principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet comme C++.

PHP a permis de créer un grand nombre de sites web célèbres, comme Facebook, YouTube, Wikipedia, etc. Il est aujourd'hui considéré comme la base de la création des sites Internet dits dynamiques. 14

PXE L'amorçage PXE (sigle de Pre-boot eXecution Environment) permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur.

L'image ainsi récupérée peut être le système d'exploitation brut ou bien le système d'exploitation personnalisé avec des composantes logicielles (suite bureautique, utilitaires, packs de sécurité, scripts, etc.).

Une fois cette image « pré-chargée », elle peut éventuellement, en fonction des paramétrages passés à cette image sur le serveur, être installée sur la machine qui a été amorcée en PXE.

Il permet également d'installer de manière automatique et à distance des serveurs sous divers OS.

Les nouvelles technologies VDI permettent également de « streamer » un OS complet ainsi que ses applications associées, directement sur la station de travail sans disque dur, en bootant préalablement avec le PXE.

Pour activer le PXE, il faut auparavant le configurer dans le BIOS. L'option se trouve fréquemment dans un menu concernant la carte réseau.

L'amorce par PXE s'effectue en plusieurs étapes :
- recherche d'une adresse IP sur un serveur DHCP/BOOTP ainsi que du fichier à amorcer ;
- téléchargement du fichier à amorcer depuis un serveur Trivial FTP ;
- exécution du fichier à amorcer.

La taille du fichier à amorcer ne permet pas de « booter » directement un noyau Linux, par exemple, mais il faut que le logiciel à amorcer le télécharge et l'exécute lui-même. 4, 5, 7

RSA Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. RSA a été breveté par le Massachusetts Institute of Technology (MIT) en 1983 aux États-Unis. Le brevet a expiré le 21 septembre 2000.

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message. 21

SQL (sigle de Structured Query Language, en français langage de requête structurée) est un langage informatique normalisé servant à exploiter des bases de données relationnelles. La partie langage de manipulation des données de SQL permet de rechercher, d'ajouter, de modifier ou de supprimer des données dans les bases de données relationnelles.

Outre le langage de manipulation des données, la partie langage de définition des données permet de créer et de modifier l'organisation des données dans la base de données, la partie langage de contrôle de transaction permet de commencer et de terminer des transactions, et la partie langage de contrôle des données permet d'autoriser ou d'interdire l'accès à certaines données à certaines personnes.

Créé en 1974, normalisé depuis 1986, le langage est reconnu par la grande majorité des systèmes de gestion de bases de données relationnelles (abrégé SGBDR) du marché. 7

SSH Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Le protocole SSH a été conçu avec l'objectif de remplacer les différents programmes rlogin, telnet, rcp, ftp et rsh. 21

Virtualiser La virtualisation consiste à faire fonctionner un ou plusieurs systèmes d'exploitation / applications comme un simple logiciel, sur un ou plusieurs ordinateurs - serveurs / système d'exploitation, au lieu de ne pouvoir en installer qu'un seul par machine. Ces ordinateurs virtuels sont appelés serveur privé virtuel (Virtual Private Server ou VPS) ou encore environnement virtuel (Virtual Environment ou VE). 23

XMPP Extensible Messaging and Presence Protocol (qu'on peut traduire par « Protocole extensible de présence et de messagerie »), souvent abrégé en XMPP, est un ensemble de protocoles standards ouverts de l'Internet Engineering Task Force (IETF) pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données. XMPP est également un système de collaboration en quasi-temps-réel et d'échange multimédia via le protocole Jingle, dont la voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.

XMPP est constitué d'un protocole TCP/IP basé sur une architecture client-serveur permettant les échanges décentralisés de messages instantanés ou non, entre clients, au format Extensible Markup Language (XML). XMPP est en développement constant et ouvert au sein de l'IETF. 3

Xubuntu est une variante d'Ubuntu, elle reprend donc les mêmes concepts de base. La différence la plus visible est l'utilisation de l'environnement de bureau Xfce à la place de Unity. La base est la même (noyau, gcc, xorg . . .), seule l'interface diffère.

L'un des buts de Xubuntu est d'offrir une distribution plus légère qu'Ubuntu, pouvant s'installer sur des ordinateurs plus anciens, et avec du matériel moins performant. L'environnement Xfce a été choisi dans ce but, ainsi que les applications installées par défaut. 4, 7