# ResEI 103 : Présentation du fonctionnement et de l'architecture du ResEI

Association ResEI
<gestion@resel.enst-bretagne.fr>

Réseau des Élèves de l'ENST Bretagne

25 octobre 2006

# Licence

Ces slides sont sous licence GPL (General Public Licence). Ils sont disponibles, avec leur code source sur le site de l'Association ResEl (http ://resel.enst-bretagne.fr).

Ils ont été créés à partir de logiciels libres (LaTeX-beamer).

Ce cours nécessite les notions de base abordées dans les cours ResEl 101 et ResEl 102.

# Plan

# Plan

# Historique (création du réseau)

- Le réseau arrive dans les chambres en même temps que le téléphone fin 1989
- 18 connectés en 1991 sur un réseau à 64 kF
- une fibre optique remplace la liaison 10 Mbps entre le ResEl et l'école en 1994
- le réseau ne servait qu'à se loguer sur les stations SUN de l'école

# Historique (évènements récents)

- Le club linux est créé en 1994, il devient rapidement le club ResEl
- Le budget servait à un abonnement à Linux Journal
- Une cinquantaine de personnes sont connectés en 1996, le club obtient un budget du BdE pour acheter une Slackware, mais passe rapidement à Debian sur le serveur 486 qui fait tourner un serveur DNS
- Le forum Meli-Melo apparaît
- La commande groupée apparaît en 1998
- Le réseau ne cesse de s'améliorer au niveau matériel

# Historique (ResEI 2)

- Suite à des problèmes avec la trésorerie du BdE, le ResEI prend son indépendance et l'Association « Réseau des Élèves de l'ENST Bretagne (ResEI) » est créée en Octobre 2002
- Grands changements en 2003/2004 (projet ResEI 2) :
  - le forum Meli-Melo est remplacé par Agora ;
  - la base LDAP est créée ;
  - le DHCP est mis en place, simplification de la connexion ;
  - le Whoswho est réécrit ;
  - le site web est refait de zéro ;
  - un nouveau système d'administration du réseau est écrit sous licence GPL (ResEIAdmin2).

# Principaux serveurs

- La DISI de Rennes a fait don au ResEI d'une vingtaine de stations sun Ultra5
- La plupart des serveurs ne sont pas récents, voici les principaux :
  - Noboot : serveur DNS, DHCP, ResEIAdmin2 ;
  - Baal : serveur web ;
  - Lily : passerelle et firewall IPv4 ;
  - Reactive11 : diffusion de la TNT ;
  - Venus : serveur de mails, mailing-list, forum ;
  - Alice : miroir des distributions et logiciels libres ;
  - Padova : serveur de sauvegarde ;
  - Anima : serveur IRC.

# Plan

# Débits Interne et externes

- Au niveau interne,
  - tous les bâtiments sont reliés par des fibres optiques Gigabit au I1 ;
  - les switches d'un même bâtiment sont reliés entre eux par un lien Gigabit ;
  - les chambres disposent de prises RJ45, reliées au switchs des bâtiments par des câbles catégorie 5 capables de supporter du 100 Mbps.
- Au niveau d'Internet, l'école dispose de 30 Mbps sur Megalis (réseau haut-débit Breton) :
  - entre 3 et 5 Mbps alloués pour le lien Brest - Rennes (suivant moment de la journée) ;
  - 10 Mbps réservés au ResEI ;
  - le reste est utilisé par l'école, ce qui explique le débit plus important du proxy.

# Plages d'adressage IP

- Le ResEI ne dispose que d'une adresse IP publique (192.44.76.8)
- Pour sortir, le NAT (*Network Address Translation*) est utilisé
- Les IP internes vont de 172.16.21.x à 172.16.30.x
  - 172.16.21.x est utilisé pour l'adressage des bornes Wifi
  - 172.16.22.x est utilisé pour le DHCP (personnes pas encore inscrites) et les switches
  - 172.16.23-29.x est utilisé pour les PCs des étudiants
  - 172.16.30.x est utilisé pour les personnes invitées
  - 192.168.0-1.x est utilisé pour le ResEI de Rennes
- Le ResEI dispose d'un /64 (pour le moment) en IPv6. L'IPv6 est en cours d'implémentation
- Le préfixe attribué est 2001 :660 :7302 :3

# DMZ

- Le ResEl dispose d'une zone démilitarisée (DMZ), qui sert de tampon entre l'extérieur et l'intérieur
- La DMZ est un VLAN sur un switch, c'est Lily qui fait le lien entre l'intérieur, l'extérieur et la DMZ (3 cartes réseau)
- Cette DMZ a l'IP 172.16.23.1 en interne, 192.44.76.8 sur internet, et 10.0.0.1 dans la DMZ
- Les machines dont les services doivent être accessibles de l'extérieur sont présentes : serveur mail, firewall, serveur web
- Depuis l'extérieur, on ne peut accéder qu'à la DMZ et pas à l'intérieur

# Routage et filtrage

- Le réseau Interne de l'école ainsi que le ResEl de Rennes est disponible sans passer par la DMZ
- Les adresses en 172.16.21.x (switches), 172.16.22.x (DHCP) et 172.16.30.x (invités) ne peuvent pas communiquer avec le réseau interne de l'école, mais les invités peuvent accéder à Internet
- Les autres adresses peuvent aller partout
- Le TCP est peu filtré
- Tous les ports UDP sont bloqués par l'école

# Switches et câblage

- Le ResEI dispose de switches professionnels, fournis par la DISI :
  - des 3Com (3300 pour la plupart) ;
  - des Cisco 2950 et 2960, les plus récents ;
  - un Cisco 3750 Gigabit pour la liaison inter-bâtiments.
- Le fait d'avoir à la fois des 3Com et des Cisco complique l'administration automatisée de certaines fonctionnalités, comme les VLANs
- C'est également la DISI qui s'occupe du câblage des bâtiments

# Plan

# Présentation d'Open LDAP

- À l'origine, LDAP (*Lightweight Directory Access Protocol*) est un protocole permettant l'accès à des annuaires
- Standalone LDAP est un annuaire avec une base de données. Open LDAP est une implémentation libre de Standalone LDAP
- La base se présente sous la forme d'une arborescence hiérarchisée (contrairement à SQL)
- Le LDAP bénéficie d'un accès extrêmement rapide en lecture mais d'un accès lent en écriture (par rapport à une SQL par exemple)

# Présentation du LDAP du ResEl

Le LDAP du ResEl est constitué de 2 branches principales :

- `dc=maisel,dc=enst-bretagne,dc=fr` qui contient trois branches :
  - `ou=people` contenant toutes les personnes pouvant avoir une machine
  - `ou=anciens` contenant tous les anciens (promo antérieure à 2004) qui ne peuvent plus avoir de machine
  - `ou=clubs` qui contient les informations sur les clubs
- `dc=resel,dc=enst-bretagne,dc=fr` qui contient 4 branches :
  - `ou=machines` contenant toutes les machines enregistrées. Chaque machine fait référence à son propriétaire, et possède entre autres les attributs *macAddress* et *ipHostNumber*
  - `ou=admins` contenant les droits des administrateurs
  - `ou=reseau` contenant tous les ports des switches et les chambres auxquels ils correspondent
  - `ou=snmp` contenant les spécificités (MIB) des switches pour l'automatisation

# Les SQLs et leur rôle

- La SQL `cachePort`, sur Noboot, sert à faire la correspondance entre les adresses MAC et les ports des switches. En effet les adresses MAC qui ont circulé sur un port restent dans le cache de ce port un certain temps, et un script vient régulièrement relever les caches des ports (en SNMP) pour remplir cette SQL. Il y a également une notion de date pour savoir quand les gens sont partis
- La SQL `tresorerie` sert pour la gestion de la trésorerie

# Les logs

- De nombreux logs sont gardés par le ResEl :
  - net-acct tourne sur la passerelle : cela sauvegarde toutes les connexions passant par la passerelle : on peut donc voir qui a contacté quelle IP sur quel port à quel moment précis.
  - journaux de connexion du serveur SMTP
  - les logs sont analysés pour détecter les phénomènes suspects, et consultés a posteriori en cas d'intrusion

# Plan

# Scripts d'inscription

- Après une authentification basée sur le LDAP, le script d'inscription effectue plusieurs opérations :
  - obtient la MAC avec laquelle la personne est venue sur le site ;
  - si la mac est déjà enregistrée le script s'arrête ;
  - sinon le script demande le nom de machine désiré ;
  - une fois un nom d'hôte correct trouvé, l'attribut *reselPerson* est ajouté à l'entrée de l'utilisateur dans la branche people, et la machine est ajoutée dans la branche `ou=machines`, avec une IP libre.

# Whoswho, synchronisations

- L'annuaire LDAP du ResEl est synchronisé avec celui de l'école (disponible en accès anonyme) pour avoir les noms des personnes
- Un script intialise le mot de passe ResEl au mot de passe école (les hashs des mots de passe de l'école sont en accès libre)
- Pour le numéro de téléphone et le compte téléphonique, on se base sur le PABX de l'école, rempli par la MaisEl, sur lequel il est nécessaire de faire du reverse-ingeneering
- Tout ceci fait que parfois l'annuaire n'est pas à jour...

# Firewall

- Le firewall est situé sur la passerelle (Lily)
- C'est un simple `iptables` dont les tables sont regénérées souvent
- Seuls les couples IP/MAC inscrits peuvent passer le firewall
- À chaque inscription les tables sont regénérées pour contenir toutes les MAC enregistrées

# DNS

- Le DNS utilisé au ResEl est `bind9` de l'Internet Systems Consorsium (ISC)
- Il est présent sur Noboot (DNS primaire) et Lily (DNS secondaire)
- Les bases de données sont mises à jour à partir de la branche machine : un script (`ldap2dns.pl`) regarde toutes les entrées de la branche machines du LDAP et fait correspondre toutes les IP et les noms de machine (ainsi que les alias)
- À chaque inscription ce script est relancé

# DHCP

- Le DHCP du ResEl est `dhcp3-server` également de l'Internet Systems Consorsium (ISC), installé sur Noboot
- Le DHCP se sert également du LDAP : il attribue l'IP automatiquement en fonction de la MAC du demandeur, et la correspondance est établie dans une table qui est refaite à chaque inscription
- Le DHCP communique également l'emplacement des deux DNS, du masque de sous-réseau et de la passerelle Internet, pour faciliter la connexion

# Plan

# TNT

- Une machine sert à diffuser la télé : TV (ancienne machine RéActiVE), elle est munie de quatre cartes TNT Nova-T
- Mumudvb sert pour le moment à faire le streaming DVB en Multicast (logiciel mumudvb)
- Chaque chaîne est diffusée sur une adresse multicast
- Les annonces SAP (correspondance entre le nom d'une chaîne et son adresse) sont broadcastées souvent
- MiniSAPServer sert à diffuser les annonces SAP des webradios (diffusées par Icecast) et de la TNT
- Chaque carte TNT peut recevoir un seul multiplexe

# Wifi

- Les bornes
  - Il y a, pour le moment, une borne Wifi par bâtiment
  - Toutes les chambres ne sont pas couvertes =¿ installation de bornes en plus. Mais où ?
- Identification
  - La connexion utilise le protocole d'identification 802.1x
  - Un serveur Radius (sur Noboot) gère les demandes de connexions
  - L'authentification se fait grâce au login/mdp ResEl (le serveur interroge le LDAP)

# Le miroir

Le miroir contient principalement quatre types de fichiers :

- Les logiciels libres Windows, mis à jour à la main, grâce à un abonnement à des listes de diffusions de logiciels libres
- Les isos de distributions mises à jour de temps à temps (peu de variations majeures au cours du temps)
- Les noyaux de kernel.org dont la mise à jour est quotidienne et automatique
- Les paquets des distributions, mis à jour automatiquement 1 à 4 fois par jour

# Le site

- Le site est hébergé sur Baal, dans la DMZ
- La carte réseau possède deux adresses IP : une pour l'intérieur, une pour l'extérieur
- des Rewrite-Rules apache convertissent l'URL `http://resel.fr/coin/coin.xml` en `http://resel.fr/Index.php?page=coin/coin.xml` sans que cela se voie dans le navigateur : cela clarifie les URLs et permet d'inclure les en-têtes et les pieds de page automatiquement
- Constitué d'un répertoire `int/` (accessible de l'intérieur et de l'extérieur lorsqu'on est identifié en httpS) et d'un répertoire `ext/` (accessible de l'extérieur) contenant des liens vers le répertoire `int/` , cela permet de contrôler ce que l'on met ou pas sur le site extérieur

# Les sites des clubs

- Les clubs ont un compte sur le serveur web, dont leur shell est `/usr/bin/passwd`, donc ils ne peuvent pas directement accéder au serveur en lui-même, mais seulement changer leur mot de passe lorsqu'ils utilisent `ssh`
- Leur dossier home est la racine de leur site
- Proftpd est configuré pour que les utilisateurs puissent accéder à leur dossier home en FTP, avec leur login et mot de passe
- `pam_ldap` identifiera dynamiquement les clubs à partir de la branche du LDAP, au lieu de leur donner un compte

# Listes de diffusion et Agora

- Les mails, les listes de diffusion et le forum Agora sont sur Venus, dans la DMZ
- Le forum Agora est géré par `inn2`
- L'envoi et la réception de mail se fait par `postfix`
- La gestion des boîtes aux lettres `@resel.tb` se fait par `courrier-imap` et `courrier-pop`
- Les listes de diffusion sont gérées par `sympa` (interface web et moteur)

# Plan

# Administration des switches

- Il y a trois façons d'administrer les switches :
  - en telnet (ou ssh sur les Cisco) : on a accès à toutes les fonctions du switch, aux statistiques, etc. dans une interface console ;
  - en http : une interface web de gestion des switches est disponible, mais jamais utilisée ;
  - en SNMP (*Simple Network Management Protocol*) : protocole permettant une administration automatique, dans des scripts, mais nécessitant d'avoir des MIB (correspondance entre les messages snmp et les commandes correspondantes) qui sont parfois propriétaires.

# Les langages utilisés

- Les principaux langages utilisés sont perl et php
- PHP est utilisé pour les interfaces web : le site, l'inscription, ResElAdmin2
- Perl est utilisé pour les scripts lancés à l'inscription (firewall, DNS, DHCP), ainsi que pour les petits scripts comme arpkiller, les script de parsage des logs pour la surveillance
- Quelques scripts bash sont utilisés pour la surveillance de la taille des partitions, les mises à jour automatiques du miroir, etc.

# ResElAdmin2

- Logiciel développé par Milton Yates (président 2003/2004) sous licence GPL (crédits AEP) : interface Web de gestion du ResEl écrite en php, basée sur l'ancien ResElAdmin
- Logiciel non-portable (développé pour le ResEl), mais incluant beaucoup de fonctionnalités :
  - gestion des switches (3Com et Cisco de façon transparente) : reboot, état des ports, fermeture des ports, etc. ;
  - gestion de la trésorerie ;
  - une recherche universelle sans restrictions et possédant des liens directement vers le port du switch de la personne recherchée ;
- énormément de nouvelles fonctionnalités à développer

# Subversion

- Subversion (SVN) est un gestionnaire de version de fichiers
- le dépôt du ResEI contient 5 branches :
  - `asso` : contient les documents relatifs à l'association (Comptes-rendus, statuts, etc.)
  - `conf` : contient les fichiers de configuration crutiaux
  - `dev` : contient les programmes de développement (ResEIAdmin2)
  - `script` : contient tous les scripts développés au ResEI
  - `webresel` : contient tout ce qui touche au site
- La structure du SVN est visible depuis la MaisEI à l'adresse `http://trac.maisel.enst-bretagne.fr`

# Trac

Trac est un outil d'administration libre écrit en python, qui gère plusieurs services :

- un Wiki pour toute la documentation que les gens du ResEl peuvent écrire
- un navigateur svn très simple, avec coloration syntaxique et diffs visuels pour bien voir ce qu'ont modifié les différentes mises à jour
- un système de tickets pour les administrateurs : lorsqu'une tâche importante est identifiée, un ticket est ouvert (et un mail est envoyé), et lorsqu'on a terminé la tâche, le ticket est fermé. On peut donc avoir une idée précise des tâches à accomplir, avec leur priorité

# Plan

# arpkiller

- `arpkiller` est un script récent, écrit en perl pour empêcher la propagation de virus
- Il fait fonctionner `tcpdump` en permanence et regarde les requêtes ARP (qui sont broadcastées)
- Il trie ensuite les requêtes sur des IP hors-range
- Au bout de 50 requêtes sur des IP hors-range (virus), le script coupe automatiquement le port de la machine en question, grâce à SNMP
- En cas de coupure le script envoie un mail au coupé et à `virus@resel`

# Surveillance des pannes : Nagios

- Nagios est un outil permettant de vérifier à intervalles réguliers si un service, un switch, une machine est actif
- Lorsqu'un service ou une machine tombe, un bot IRC nous donne une alerte sur le canal (privé) `#resel2`, pour une plus grande réactivité, et un mail est envoyé
- Pour les admins utilisant le protocole de messagerie Jabber, possibilité de recevoir ces annonces par ce biais
- Quand les onduleurs prennent la main sur l'alimentation (en cas de coupure de courant), Nagios nous prévient

# Filtrage Peer to Peer, surveillance du traffic

- La passerelle Internet a un noyau compilé avec les modules ip-p2p
- Elle effectue un string-match sur tous les paquets, afin de filtrer certains mots qui aparaîssent dans les entêtes des paquets P2P
- Ce filtrage permet d'avoir de meilleures relations avec la DISI et de pouvoir avoir moins de restrictions au niveau d'Internet
- Un script comptabilise à la fin de la journée le traffic de chaque machine grâce à ipfm et nous prévient des téléchargements importants

# Conclusion : l'avenir du ResEI

- Vous !
- Beaucoup de projets et de services à offrir aux utilisateurs, il y a du boulot pour tout le monde :
  - ajout de chaînes satellite ;
  - ajout de fonctions et portabilité de ResEIAdmin2 ;
  - système de tickets utilisateurs pour faciliter la gestion des requêtes.
- Amis cyborgs, à vos claviers !