Gérer son système d'information réseau avec Netmagis

Pierre David
Université de Strasbourg – UFR de mathématique et d'informatique

Jean Benoit
Université de Strasbourg – Direction Informatique

Sébastien Boggia
Université de Strasbourg – Direction Informatique

Résumé

Netmagis (pour Network Management Information System) est un nouveau logiciel, basé sur WebDNS déjà présenté lors de précédents JRES et maintenant sous licence CeCILL-B. Netmagis est destiné à faciliter différents aspects de la gestion d'un réseau.

Netmagis permet de déléguer simplement des opérations sur le « système d'information réseau » à des correspondants : gestion IPv4 et IPv6, DNS, DHCP, routage de messagerie, gestion des exceptions dans un environnement SMTP authentifié, vision de la topologie réseau, configuration de ports d'équipements réseau multi-constructeurs (Cisco, Juniper et HP), métrologie, etc.

Ce logiciel a été conçu pour fonctionner sur de petits comme sur de grands réseaux. À titre d'exemple, Netmagis est utilisé sur le réseau métropolitain strasbourgeois Osiris pour gérer plus de 400 sous-réseaux et près de 1500 équipements, délégués à environ 200 correspondants réseau.

La gestion du référentiel réseau est au cœur de Netmagis. Il contient l'ensemble des données du système d'information réseau (réseaux, adressage, vlan, etc.) et permet notamment de visualiser la disponibilités des blocs d'adresses. Il maintient de manière centralisée les différents acteurs (client, correspondants) et les informations et les ressources qui leur sont associées (réseau, adresses, etc.).

Une partie du référentiel est constituée par une modélisation du réseau sous forme de graphe, dérivée automatiquement des configurations des équipements (commutateurs, routeurs). Par exemple, sur Osiris, de simples commentaires de l'administrateur réseau dans les équipements génèrent automatiquement plus de 15 000 sondes interrogées périodiquement.

Grâce à la cohérence du référentiel, à la délégation d'opérations et à l'automatisation de nombreuses tâches, Netmagis est l'outil indispensable pour une gestion rigoureuse et efficace du réseau.

Mots clefs

Système d'information réseau, gestion de configuration, référentiel, gestion de réseau

1 Introduction

Netmagis (pour Network Management Information System) est un nouveau logiciel destiné à faciliter différents aspects de la gestion d'un réseau. Placé sous licence libre (CECILL-B), il a été développé dans le contexte d'un grand réseau universitaire, le réseau Osiris, qui comporte plus de 400 sous-réseaux et près de 1 500 équipements réseau, dont la gestion est déléguée à environ 200 correspondants dans les bâtiments et les laboratoires. Environ 15 000 sondes de métrologie sont gérées automatiquement par Netmagis.

La version 2.0 de Netmagis est annoncée à l'occasion de ces JRES. Cet article a pour but de présenter les principales fonctionnalités du logiciel, son architecture ainsi que les évolutions d'ores et déjà prévues.

2 Netmagis et WebDNS

Le socle sur lequel Netmagis a été conçu repose sur WebDNS, application Web présentée aux JRES 2003 [1]. Devant l'intérêt suscité à l'époque, un effort particulier avait été fait pour la diffuser et pour valider son ouverture sous licence CECILL-B. Le logiciel a ensuite été enrichi avec de nouvelles fonctionnalités, comme celles présentées lors des JRES 2005 [2] : informations de topologie réseau et génération de graphes de niveau 2 et 3 (topologies de commutation et de routage).

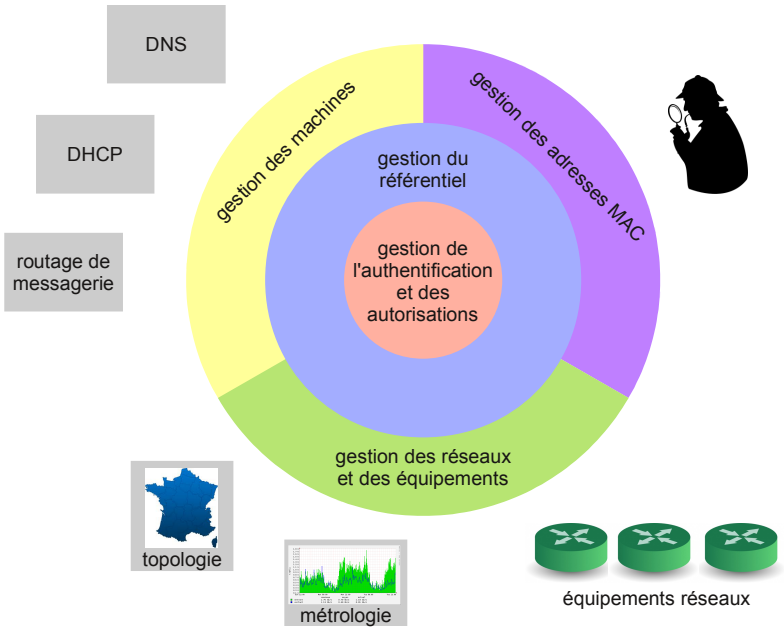
Convaincus de l'intérêt de ce logiciel pour la communauté des gestionnaires de réseaux, nous avons entrepris un travail important pour en élargir la diffusion :

- renommage en Netmagis, nettement moins réducteur que l'ancien nom WebDNS et reflétant mieux la nature de « système d'information réseau » de l'ensemble ;
- élimination des spécificités propres à l'enseignement supérieur et à la recherche, dans le but d'élargir la communauté des utilisateurs et également des contributeurs ;
- internationalisation de l'application et du code : l'application est accessible en anglais et en français, l'ajout d'autres langues est bien évidemment possible, toujours dans le but d'élargir la communauté des utilisateurs et des contributeurs ;
- migration du code d'un gestionnaire de version privatif de l'université de Strasbourg vers une forge (github) accessible et ouverte à d'autres contributeurs ;
- simplification radicale de l'installation des différents composants du logiciel.

L'objectif initial de WebDNS était de déléguer simplement la gestion du DNS à des correspondants réseau ou à des gestionnaires de parc. Pour ce faire, il a fallu formaliser plusieurs notions essentielles : les réseaux, les adresses, les correspondants, les domaines, les machines etc. WebDNS/Netmagis, est devenu à la fois un fédérateur et un catalyseur pour le développement de plusieurs outils. Nous avons alors progressivement constitué autour du logiciel et de sa base de données un véritable système d'information réseau.

3 Fonctionnalités

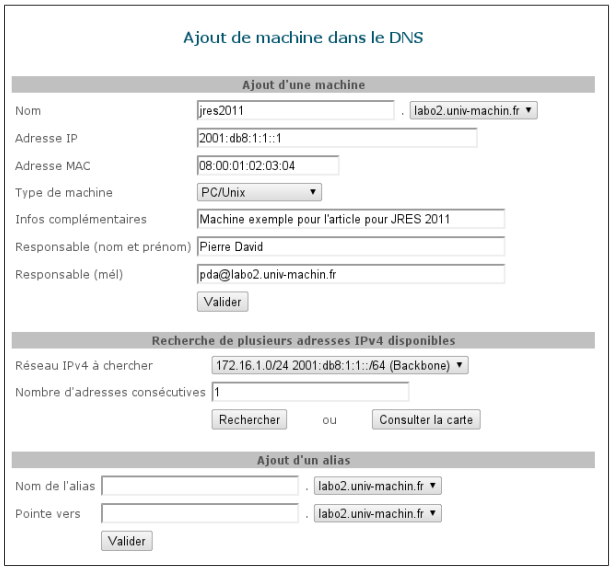
Les fonctionnalités actuelles de Netmagis sont réparties en cinq grands domaines comme décrit dans le schéma ci-dessous :

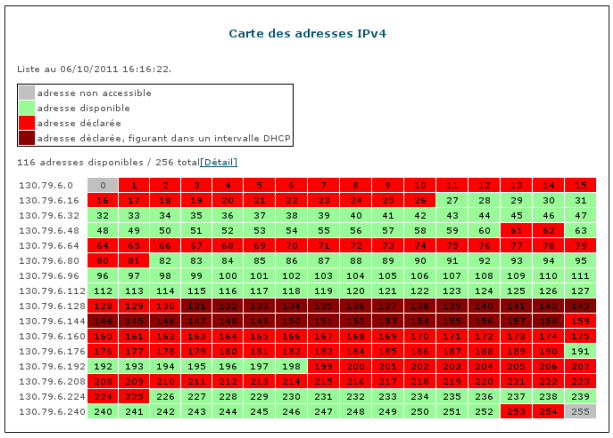


Ces grands domaines sont décrits plus en détail dans le reste ce chapitre.

3.1 Gestion des machines

La fonctionnalité de base est la délégation à des correspondants réseau de la déclaration, de la modification ou de la suppression de machines dans le DNS, que ce soit en IPv4 ou en IPv6. Une « carte » simplifie la recherche d'une adresse IPv4 libre. En indiquant l'adresse MAC, la déclaration est propagée vers le ou les serveurs DHCP, de même que les intervalles d'adresses IP dynamiques spécifiés par les correspondants dans leurs réseaux. Les copies d'écran ci-dessous montrent la page d'ajout de machine ainsi que la carte des adresses IPv4 d'un réseau :



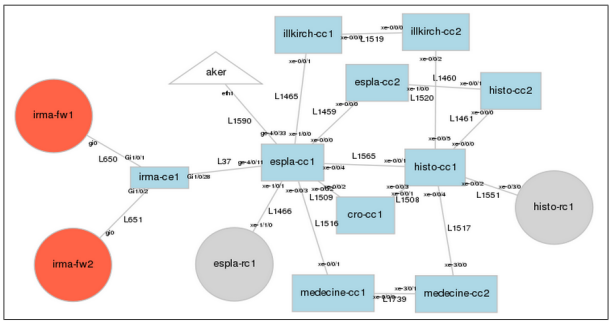


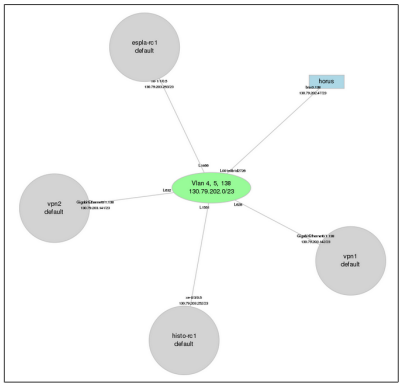
Le logiciel gère également des domaines de messagerie et publie automatiquement des enregistrements de type MX dans le DNS et des règles internes de routage de messagerie utilisables par Sendmail ou Postfix. Dans les environnements utilisant SMTP authentifié [3], il est également possible de gérer des exceptions à l'authentification comme c'est souvent nécessaire pour les copieurs expédiant les numérisations de documents par mail.

3.2 Gestion du réseau et des équipements réseau

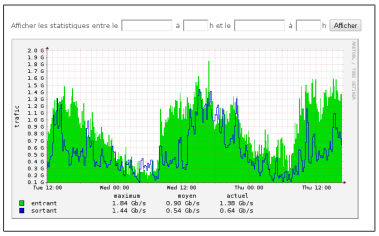
Si l'administrateur du site souhaite davantage de fonctionnalités, il peut activer en complément :

- le module de topologie réseau, qui a pour but de présenter des cartes réseau cliquables de niveau 2 et de niveau 3 comme illustré sur les deux figures ci-après :





- le module de métrologie, qui présente les courbes de trafic obtenues par interrogation SNMP des équipements identifiés dans le module de topologie :



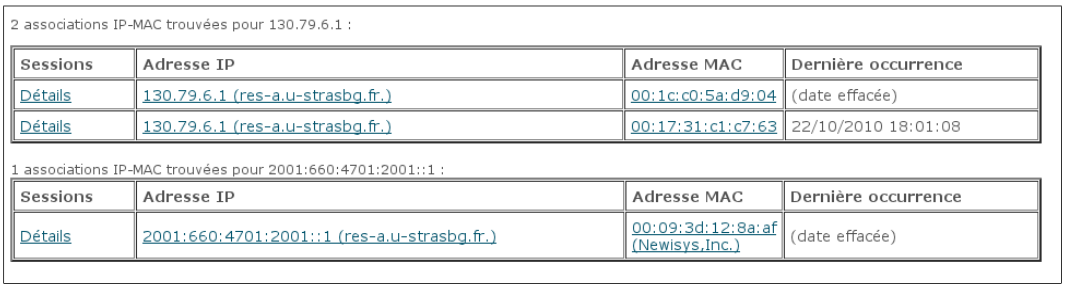
- la modification des interfaces des équipements : un correspondant réseau peut ainsi modifier l'affectation d'une interface à un VLAN (incluant les VLAN pour la ToIP) ainsi que sa description. Cette possibilité est offerte dans un environnement multi-constructeurs (pour le moment : Cisco, Juniper, HP) :

Ces trois fonctionnalités sont optionnelles, l'administrateur de Netmagis peut choisir ou non de les activer. De plus, le système de droits permet une délégation assez fine et souple. Par exemple, un correspondant réseau pourrait consulter la carte du réseau incluant tous les équipements traversés par ses VLAN (y compris les équipements de cœur) et la métrologie de son VLAN sur les équipements qui lui sont accessibles, mais il ne pourrait modifier que les équipements de son bâtiment. Sur un autre site, on pourrait imaginer que le correspondant n'ait accès qu'à la cartographie de son propre réseau, sans accès ni à la métrologie ni à la modification des interfaces des équipements.

3.3 Gestion des adresses MAC

La gestion des adresses MAC a pour but de localiser des machines dans le réseau et dans le temps. Des programmes de collecte sondent à intervalle régulier les équipements réseau et enregistrent dans la base de données des associations :

- entre des adresses IP et des adresses MAC : pour retrouver l'adresse MAC qui a éventuellement usurpé une adresse IP, ou retrouver l'adresse MAC qui a été associée à une adresse IP donnée par DHCP lors d'un incident de sécurité :



- entre des adresses MAC et des interfaces d'équipements : pour localiser l'adresse MAC recherchée à un instant donné ;

Ces associations sont conservées avec une date de début et une date de fin pour permettre la recherche d'événements passés. De plus, ces informations sont utiles pour déterminer les adresses inactives depuis un certain temps et ainsi libérer des déclarations d'adresses IP.

3.4 Gestion du référentiel réseau

La gestion du référentiel réseau est au cœur de Netmagis. Le référentiel contient l'ensemble des données du système d'information réseau :

- noms de domaine : nom et relais de messagerie pour les adresses du domaine ;
- zones DNS : nom DNS, domaine ou réseau IP à générer, prologue de la zone ;
- réseaux : nom, préfixes IPv4 et IPv6, typologie du réseau, entité (laboratoire, établissement, etc.), informations DHCP, réseau utilisé ou libre ;
- profils DHCP : configuration spécifique (comme le serveur et l'image de boot pour des terminaux) à installer dans le fichier dhcpd.conf, qui doit être validée par l'administrateur ;
- VLANs : nom, numéro et type (utilisé pour la VoIP, ce qui permet à un correspondant de configurer une interface avec le VLAN « voix » en plus du VLAN normal) ;
- équipements réseau : nom de l'équipement, type (Cisco, Juniper, etc.) et statut. Un statut « actif » provoque l'interrogation de la configuration de cet équipement pour la cartographie du réseau et l'identification des points de métrologie ;
- configuration du logiciel : modules activés ou non, paramètres DHCP par défaut, délai de conservation des informations de métrologie après la disparition de l'équipement, etc. ;
- correspondants et groupes : tout correspondant appartient à un et un seul groupe. Ces aspects sont détaillés dans la section suivante.

La formalisation des informations dans un référentiel unique oblige à une certaine rigueur, notamment lors de l'installation du logiciel. En revanche, cette formalisation amène beaucoup d'avantages par rapport à une situation sans système d'information réseau :

- *documentation explicite* des informations : le simple fait d'identifier tous les objets et leurs relations amène naturellement une documentation de toutes les informations gérées. Par exemple, déclarer une machine nécessite que le réseau soit créé dans le référentiel, qu'un correspondant ait les droits sur la plage d'adresse concernée, et qu'une zone DNS « consomme » cette machine. Toutes ces associations entre objets doivent être explicitées dans la base, ce qui conduit à déclarer tous les réseaux dans le référentiel, constituant ainsi la documentation exacte et à jour ;
- cette documentation, du fait de sa *centralisation dans le référentiel*, est partagée par tous les acteurs, rendant ainsi obsolètes les listes de réseaux que les différents administrateurs peuvent maintenir « manuellement » de manière le plus souvent privative ;
- ce référentiel permet l'*automatisation* de nombreuses tâches : la génération de zones DNS et de configurations DHCP en est l'exemple originel, mais d'autres actions peuvent être également automatisées : routage de messagerie, traitement d'incidents de sécurité par l'identification du correspondant responsable d'une machine compromise, vérification de cohérence du réseau, etc. ;
- le référentiel étant facilement accessible (pour l'administrateur), cohérent et complet, il ouvre de *nouvelles possibilités* qui n'étaient pas réalisables sans référentiel : statistiques sur l'espace d'adressage, déclarations automatiques des interfaces des routeurs, autorisation de modifier les filtres sur des pare-feux, etc.

3.5 Authentification et autorisations d'accès à l'application

L'authentification des utilisateurs est réalisée soit via un annuaire LDAP, soit sur la base PostgreSQL intégrée pour les sites qui ne disposent pas d'annuaire LDAP. Il est également possible d'utiliser le module de SSO CAS d'Apache pour s'interfacer à un ENT d'établissement.

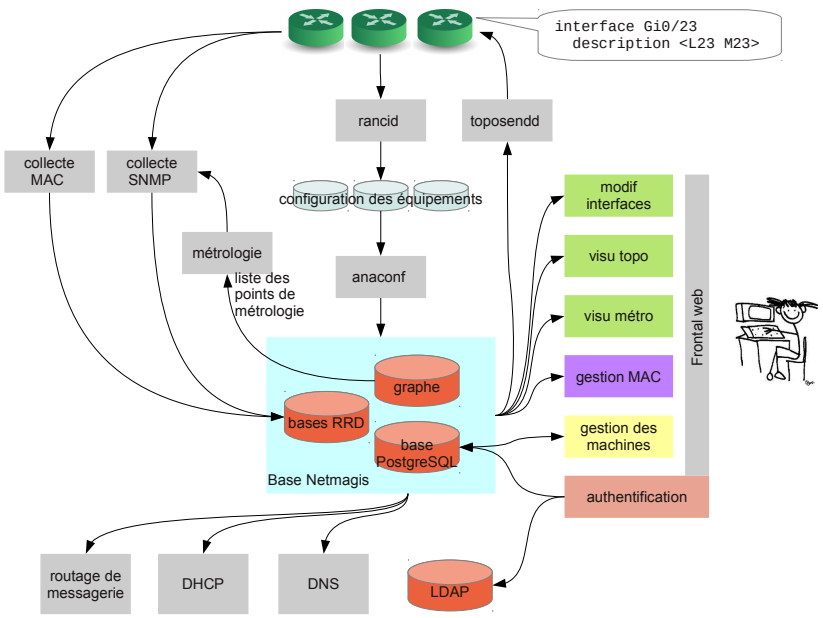
L'administration des accès à l'application, très liée au référentiel gère l'appartenance d'un correspondant à un groupe et attribue des droits d'accès fins à un groupe :

- domaines et réseaux accessibles ;
- droits d'accès aux adresses IP, définis par une succession de préfixes autorisés ou interdits ;
- profils DHCP accessibles ;
- visibilité des équipements et des réseaux dans la cartographie ;
- équipements pour lesquels la modification des interfaces est autorisée.

4 Architecture interne

4.1 Principes

Netmagis est conçu pour s'intégrer à une infrastructure existante : serveurs DNS, DHCP, routage de messagerie, équipements réseau. Le schéma ci-après décrit l'architecture interne de Netmagis :



Les données sont au cœur de Netmagis. Celles-ci sont composées :

- du référentiel et des données dans un SGBDR (PostgreSQL) ;
- d'une base d'authentification, qui peut être interne (hébergée dans le SGBDR) ou externe (serveur LDAP existant) ;
- de la modélisation du réseau sous forme d'un graphe, placé dans un fichier binaire pour des raisons de performances lors des parcours ;
- des informations de trafic issues des collectes de la métrologie.

Les informations sur les machines sont saisies par les correspondants réseau via une interface Web. Ces données sont inscrites dans le SGBDR. Des scripts extraient ces données pour générer des fichiers ad-hoc pour le serveur DNS, le serveur DHCP, le relais de messagerie, etc. Il suffit à l'administrateur du système d'activer ou non ces scripts pour bénéficier de la fonctionnalité correspondante (i.e. je n'ai pas besoin d'activer le script de génération DHCP si je n'ai pas de serveur DHCP).

La gestion des équipements réseau, fonctionnalité optionnelle, repose également sur une infrastructure existante. Celle-ci s'appuie sur « Rancid[1] » qui entre autre collecte les configurations des équipements réseau dans des fichiers. Ces configurations sont analysées par Netmagis (programme anaconf) pour produire le graphe modélisant le réseau, où sont représentés les équipements, les interfaces, les vlans, les instances de routage, les instances de commutation et les liens entre ces différents éléments. Les connexions entre équipements doivent être matérialisées par un numéro de lien figurant dans la configuration des deux équipements (« L23 » dans le schéma). Lorsqu'une modification de configuration est effectuée sur un équipement, elle est notifiée via Syslog, ou Radius si l'équipement n'est pas capable de notifier les modifications de configuration. La notification déclenche toute la mécanique de collecte pour ce seul équipement ainsi que la reconstruction du graphe.

[1] http://shrubbery.net/rancid

Si l'utilisateur a le droit de modifier la configuration d'un équipement via Netmagis, la modification est traduite et placée dans une file d'attente dans le SGBDR. Le démon « toposendd » se charge d'envoyer les commandes à l'équipement. Une fois les commandes envoyées, la mécanique de collecte est relancée, grâce à la notification de modification, afin d'avoir un graphe toujours à jour.

Si dans la configuration de l'équipement, l'administrateur réseau a indiqué un point de métrologie (« M23 » dans le schéma), celui-ci est intégré dans le graphe, puis communiqué au module de métrologie qui va mettre en œuvre une interrogation périodique des équipements. Netmagis comporte un collecteur SNMP, basé sur « RRDTool[2] », optimisé pour un grand nombre de points de métrologie (15 000 sur Osiris). La collecte des adresses MAC, également optionnelle, fonctionne de manière analogue : les associations IP-MAC et MAC-Interface sont enregistrées dans le SGBDR.

4.2 Implémentation des différents éléments

Les différents éléments de Netmagis peuvent être installés sur différentes machines en fonction de considérations de performances, de sécurité, etc. Parmi toutes les possibilités, un extrême serait de tout concentrer sur une seule machine. L'autre extrême consisterait à mettre chacun des éléments suivants sur des serveurs distincts :

- frontal Web et scripts CGI ;
- SGBDR ;
- détection des modifications des équipements ;
- gestion des équipements réseau : analyse des configurations, gestion du graphe modélisant le réseau, et envoi des commandes aux équipements ;
- métrologie et MAC.

Par ailleurs, des scripts de Netmagis doivent être installés sur l'infrastructure existante : serveur DNS, serveur DHCP, relais de messagerie, serveur Syslogd, serveur Radius, etc.

Sur Osiris, le choix a été de tout séparer pour les raisons explicitées ci-après :

- le frontal Web est sur un serveur fournissant un service mutualisé avec tout l'hébergement Web de l'université ;
- le SGBDR est également hébergé sur un serveur de bases de données mutualisé pour l'ensemble des applications utilisant PostgreSQL ;
- la détection des modifications des équipements est installée sur deux serveurs existants : le serveur Syslog central d'Osiris ainsi que le serveur Radius central ;
- la gestion des équipements réseau est placée sur un serveur dédié pour des raisons de performance (le graphe représente 1 500 équipements) et de sécurité (l'accès aux configurations est sensible) ;
- la métrologie est placée sur un serveur dédié pour des raisons de performance (15 000 points de métrologie sont collectés) et de sécurité (la machine est dans le VLAN d'administration des équipements) ;
- Les services DNS et DHCP sont hébergés sur la même machine (redondée) ;
- Le service de relais de messagerie est hébergé sur un cluster dédié de 8 serveurs.

Au delà de cet exemple, il est important de préciser que les constituants de Netmagis sont très peu gourmands en ressources matérielles et peuvent être hébergés sans aucun problème sur une ou plusieurs machines virtuelles. Par exemple, sur Osiris, le SGBDR, le frontal Web et la gestion des équipements réseau étaient jusqu'à très récemment placés sur la machine généraliste du service gestionnaire du réseau, sur laquelle tournaient beaucoup d'autres applications. La charge occasionnée par les générations (DNS, DHCP, routages, etc.) est marginale. Seules la gestion des équipements réseau et la métrologie nécessitent davantage de ressources (chacune utilise un serveur dédié sur Osiris) : nous ne disposons pas encore d'éléments pour évaluer dans quelle proportion la dimension du réseau et la quantité de points de métrologie influent sur les ressources matérielles nécessaires.

[2] http://oss.oetiker.ch/rrdtool/

5 Évolutions prévues

Outre les fonctionnalités présentées dans cet article, de nombreuses autres évolutions sont prévues à moyen terme :

- localisation géographique des équipements afin de générer automatiquement des plans d'implantation ;
- convergence entre la gestion des machines, des adresses MAC et des équipements, pour offrir de nouvelles possibilités comme par exemple l'affichage des noms et des adresses des machines connectées sur les interfaces d'un équipement donné ;
- augmentation de la fréquence des mises à jour des zones DNS afin de diminuer la latence entre une modification dans la base et la répercussion sur les serveurs DNS : l'objectif est de passer de quelques minutes à quelques secondes ;
- vérification a priori des configurations DNS et DHCP afin d'éviter toute erreur lors d'une modification manuelle de prologue de zone DNS ou de profil DHCP ;
- API de type REST pour faciliter l'accès aux fonctions et aux données du SI réseau à d'autres applications ;
- extension des fonctions de métrologie sur les équipements réseau par l'ajout de nouveaux types de graphes (taux de broadcast, taux d'erreur sur les interfaces etc.) et l'intégration automatique dans une plateforme de supervision de type Nagios.

6 Disponibilité de Netmagis v2.0

La documentation, le logiciel lui-même ainsi qu'une version de démonstration sont disponibles sur http://www.netmagis.org. Les sources ainsi que le gestionnaires de bogues sont accessibles sur http://github.com/pdav/netmagis. La forge github a été choisie pour sa facilité d'intégration des contributions qui, nous l'espérons, seront nombreuses. La liste de diffusion est également un bon vecteur pour participer au développement et à l'amélioration de Netmagis.

À l'heure où nous écrivons ces lignes, les collecteurs utilisés pour la métrologie et la gestion des adresses MAC sont inclus dans les sources de Netmagis, mais ils ne sont pas encore totalement intégrés à la mécanique d'installation.

7 Conclusion

Netmagis, dont le développement a commencé en 2001, bénéficie de l'expérience de l'exploitation d'un réseau conséquent. L'apport de nouvelles fonctionnalités rend très attractif la nouvelle version pour la communauté universitaire.

Au delà du logiciel, le plus important reste la démarche de mise en place d'un système d'information réseau. L'expérience accumulée dans la gestion du réseau Strasbourgeois Osiris montre que la dimension et la complexité du réseau et des services ne laissent que peu de place à l'improvisation. La démarche de modélisation et de mise en cohérence des diverses données facilite l'automatisation des tâches, ce qui augmente la fiabilité par la réduction des erreurs humaines. Netmagis ne fait qu'accompagner cette démarche en fournissant l'outil indispensable pour atteindre ces gains d'efficacité et de cohérence dans l'exploitation quotidienne.

En annonçant la version 2 de Netmagis lors de ces JRES, nous espérons que ce logiciel puisse être utile à d'autres, et nous souhaitons vivement que les utilisateurs nous fassent part de leurs retours d'expérience, de leurs suggestions et de leurs contributions.

8 Bibliographie

[1] David P. et Benoit J., Une application pour décentraliser la gestion du DNS. Dans *Actes du congrès JRES2003*, http://2003.jres.org/actes/paper.144.pdf

[2] David P. et Benoit J., Le système d'information du réseau Osiris : de la fibre optique jusqu'aux services. Dans *Actes du congrès JRES2005*, http://2005.jres.org/paper/82.pdf

[3] David P., Zamboni A., Pegon P. et Benoit J., Évolution de l'architecture de messagerie d'Osiris, Dans *Actes du congrès JRES2009*, http://2009.jres.org/planning_files/summary/html/124.htm