Le système d'information du réseau Osiris : de la fibre optique jusqu'aux services

Pierre David
Centre Réseau Communication, Université Louis Pasteur
Pierre.David@crc.u-strasbg.fr

Jean Benoit
Centre Réseau Communication, Université Louis Pasteur
Jean.Benoit@crc.u-strasbg.fr

Résumé

Avec une complexité technique croissante et une attente de fiabilité de plus en plus forte des utilisateurs, les opérateurs des réseaux universitaires sont obligés d'industrialiser leur mode de gestion.

Le CRC, gestionnaire du réseau métropolitain strasbourgeois Osiris, s'est engagé dans une démarche pour élaborer un système d'information complet, avec comme objectifs de permettre la délégation des opérations, l'automatisation des tâches d'exploitation, la documentation des informations et la visibilité vers les correspondants réseau.

Partant de la base de l'application WebDNS, nous montrons comment notre approche s'est progressivement structurée pour constituer à terme un ensemble complet et cohérent. Intégrant un élément souvent oublié, les configurations des équipements actifs, nous sommes à mêmes d'envisager des applications innovantes, comme par exemple la production automatique de schémas du réseau ou la vérification de cohérence de certains points.

Notre approche est tournée vers l'ensemble de la communauté universitaire, puisque certains des outils sont déjà diffusés et les autres le seront si l'intérêt le justifie.

Mots clefs

Système d'information réseau, documentation, schémas réseau, organisation

1 Introduction

Comme tous les exploitants de réseaux, qu'ils soient publics ou privés, les universités sont confrontées à un défi grandissant : répondre à l'attente toujours plus importante des utilisateurs en matière de fiabilité, avec des réseaux qui se complexifient et des équipes qui n'augmentent pas en proportion.

Ce défi pousse naturellement les opérateurs de réseaux universitaires à rationaliser les moyens et les méthodes. Ce processus d'« industrialisation » de l'exploitation est, à notre avis, inéluctable pour répondre aux attentes des utilisateurs.

La construction d'un système d'information constitue une des voies les plus efficaces de cette industrialisation. Schématiquement, il s'agit de rassembler en un emplacement unique (une base de données, en pratique) l'ensemble des données manipulées afin de faciliter l'exploitation du réseau. La difficulté principale d'un tel projet consiste à faire coller le système d'information au terrain, c'est à dire que les données restent toujours cohérentes par rapport à la configuration des objets concernés (équipements, fibres optiques, etc.).

Le CRC (Centre Réseau Communication), le service chargé de l'exploitation du réseau métropolitain strasbourgeois Osiris (17 établissements distincts, dont les 3 universités, environ 50 000 utilisateurs et 25 000 machines enregistrées dans le DNS) s'est engagé dans cette démarche de construction d'un système d'information. L'originalité de notre démarche tient en plusieurs points :

- nous avons initialement cherché à satisfaire un besoin ponctuel (rédiger une application de gestion du DNS) et, pour ce faire, nous avons posé les bases du système d'information ;
- cette application a bénéficié d'extensions ultérieures, qui ont renforcé l'aspect « système d'information » ;
- nous avons structuré notre démarche au fur et à mesure de l'avancement ;
- notre conception du système d'information est incrémentale ; il ne s'agit aucunement d'un projet de type « cathédrale » construit dès le départ en pensant à la dernière pierre de l'édifice.

Nous avons respecté deux règles fondamentales tout au long de l'avancement du projet :

- généricité : nos outils doivent *in fine* être utilisés dans d'autres environnements. C'est ainsi que l'application WebDNS ([1]) a été diffusée après le très positif retour des participants aux JRES 2003, et est maintenant utilisée dans des environnements très divers ;
- dérivation automatique du maximum d'informations : en particulier, les équipements actifs contiennent énormément d'informations que l'on peut réutiliser. Tout ce qui peut y être trouvé doit être exploité.

Les composants que nous présentons dans cet article sont à des états d'avancement divers. Toutefois, il nous a semblé important de profiter des JRES pour présenter notre vision du système d'information, et de susciter une dynamique au-

tour de cette question. De plus, comme nous le soulignerons ultérieurement, nous sommes loin d'avoir exploité toutes les potentialités des outils rédigés, et nous avons souhaité que l'ensemble de la communauté puisse profiter dès que possible des idées développées ici.

Après avoir donné les éléments du contexte Osiris qui ont fondé notre démarche, nous abordons les lignes directrices que nous avons suivies. Nous présentons ensuite le système d'information dans sa globalité, puis nous explorons plus en détail les grandes parties qui le composent actuellement : le cœur, et la topologie. Nous terminons par la dernière grande partie, l'infrastructure physique, actuellement encore en chantier.

2 Contexte

Un certain nombre de facteurs ont permis l'éclosion du projet de système d'information au sein du CRC. Certains sont d'origine technique, et d'autres sont clairement organisationnels. La connaissance du contexte apporte un éclairage sur nos motivations et notre démarche.

2.1 Le réseau Osiris et le CRC

Une des caractéristiques d'Osiris, parmi les réseaux métropolitains universitaires français, est le grand nombre de ses points de présence sur le territoire strasbourgeois : 110 bâtiments sont reliés directement à 1 Gb/s (ou 100 Mb/s) sur la dorsale multi-gigabits. Chaque bâtiment abrite un commutateur d'extrémité Osiris (amenant un ou plusieurs Vlans) et un onduleur, tous deux gérés par le CRC.

Cette dimension est la conséquence d'une mutualisation très tôt comprise par les établissements, qui s'est traduite pour la quasi-totalité d'entre eux par la centralisation au CRC d'un grand nombre de services d'infrastructure réseau :

- routage : le CRC amène une connectivité de niveau 2 dans chaque bâtiment, soit un ou plusieurs Vlans. Ces Vlans peuvent être spécifiques au bâtiment (cas le plus répandu), mais également distribués sur plusieurs bâtiments ou campus. Hormis quelques cas très particuliers, les sites connectés n'ont pas besoin de déployer une infrastructure de routage ;
- DNS : le CRC opère les serveurs de noms principaux d'Osiris, que ce soit pour la zone `u-strasbg.fr` (23 000 noms) ou pour les zones particulières de quelques établissements ;
- routage de messagerie : là encore, le CRC opère les serveurs SMTP en entrée d'Osiris, avec anti-virus, liste grise et marquage de spams ;
- d'autres dispositifs (réseau sans-fil, VPN, hébergement de la messagerie) sont également mutualisés.

L'avantage de cette mutualisation n'est pas tant l'économie réalisée [2] que la meilleure qualité de service apportée à l'ensemble des utilisateurs (voir par exemple [3]).

Cette mutualisation entraîne une multiplication du nombre d'interlocuteurs : actuellement, le CRC n'a pas de contact direct avec les utilisateurs, mais seulement avec une centaine de « correspondants réseau » répartis dans les bâtiments. Avec l'ajout de nouveaux services (hébergement de 50 000 boîtes aux lettres, réseau sans-fil, VPN, etc.), le CRC sera vraisemblablement de plus en plus amené à dialoguer directement avec les utilisateurs.

La centralisation consécutive à la forte mutualisation sur Osiris a entraîné une prise de conscience, au niveau politique, de l'enjeu stratégique que représente le réseau. C'est donc ainsi que les politiques ont fixé l'objectif de disponibilité de 99,9 % du réseau, qui guide toutes les actions du CRC depuis 2001.

Le facteur humain intervient également : le CRC a connu une forte croissance de l'équipe (passage de 3 ingénieurs réseau fin 2001 à 7 en 2005), et va voir prochainement le départ à la retraite de personnes dont la mémoire est précieuse.

2.2 Les problèmes soulevés

Ces dimensions, fruits de la mutualisation, sont donc importantes dans tous les domaines : nombre d'interlocuteurs, nombre d'équipements à gérer, de machines sur le réseau, de points d'accès sans-fil, etc. Avec la taille arrive rapidement la complexité de gestion :

- complexité de l'infrastructure réseau ;
- gestion d'un très grand parc ;
- grand nombre de cas particuliers ;
- diversité de problèmes due au nombre d'interlocuteurs ;
- etc.

Le facteur humain est également source de problèmes. La difficulté quotidienne, au sein d'une équipe, est la gestion du savoir :

- apprentissage de l'infrastructure par les « nouveaux » ;
- transmission de la connaissance du terrain par les « anciens », notamment à l'approche de la retraite ;
- individualités parfois plus motivées par les défis techniques que par la rédaction de documentations ;
- difficulté de maintenir les documentations à jour ;
- partage de l'information dans l'équipe.

Enfin, tout s'est précipité lorsque, fin 2001, un crash disque a provoqué l'arrêt définitif de la base de données hébergeant les déclarations DNS, entraînant la perte des données. Le mainteneur de l'application ayant quitté l'équipe, et le savoir n'ayant pas été transmis, il a rapidement fallu trouver une solution.

3 Vers un système d'information

Le but premier du système d'information du CRC est de faciliter l'organisation et le travail du service, afin de fournir une meilleure qualité de service aux utilisateurs. À cette fin, nous avons identifié les lignes directrices, ou les objectifs suivants.

3.1 Délégation

Le premier objectif est pouvoir déléguer le maximum d'opérations vers les correspondants réseau. Par le passé, ceux-ci ont pu se sentir lésés par une « perte de contrôle » sur des opérations qui leur échappaient. Par la délégation, le CRC souhaite leur donner le maximum de contrôle.

Il ne s'agit pas pour le CRC de transférer une charge de travail aux correspondants, mais plutôt :

– d'éliminer les opérations pour lesquelles le CRC n'a pas de valeur ajoutée ;
– d'avoir une plus forte réactivité.

L'exemple typique est la gestion du DNS : comme dans beaucoup d'endroits, la gestion du DNS est centralisée par le CRC et les correspondants font des demandes de modification. Dans bon nombre d'autres sites universitaires français, ces demandes de modification sont encore traitées manuellement par l'opérateur du DNS, qui est souvent le CRI d'établissement. Quelle est la valeur ajoutée pour les uns et les autres de ce traitement manuel ? Quelle latence ce traitement introduit-il ?

Pour le correspondant réseau, une automatisation du processus ne demanderait pas plus de travail, puisque les informations doivent être renseignées de toutes manières. La latence de prise en compte des modifications sur Osiris est au maximum de 10 minutes, 24 heures sur 24 et 365 jours par an, inégalable par un traitement manuel. Le correspondant réseau a ainsi le contrôle total sur les informations qu'il place dans le DNS et une réactivité accrue. Le résultat net est une meilleure qualité des informations renseignées.

Pour le CRC, cette automatisation a ôté une tâche sans intérêt, consommatrice de ressources et peu gratifiante. Nous avons alors pu nous intéresser à d'autres actions, comme la fiabilisation de l'hébergement DNS.

Ce qui a été dit sur la gestion du DNS s'applique également à d'autres tâches, dont la délégation profite aux deux parties : gestion des filtres sur les routeurs, hébergement de la messagerie, etc.

3.2 Automatisation de l'exploitation

Le deuxième objectif consiste à automatiser autant que faire se peut les tâches quotidiennes de l'exploitation. Au delà d'une certaine dimension de réseau, l'automatisation n'est plus une option, mais devient une obligation. De plus, l'automatisation garantit un réseau plus fiable : quand quelque chose est traité automatiquement, rien n'est oublié et le modèle est uniformément appliqué.

Ce domaine est sans doute celui dans lequel nous pouvons faire des progrès, mais il faut pour cela que le matériel s'y prête : possibilité d'interfaçage des équipements par ligne de commande (voire par langage de type XML) et non par interface Web inutilement complexe, régularité du langage de configuration, équipements toujours accessibles, etc.

Parmi les exemples de tâches actuellement automatisées, nous pouvons citer le routage de messagerie sur les relais (cette information est injectée dans la table de routages de `sendmail` à partir des indications fournies par le correspondant via le système d'information, sans intervention du CRC) ou le nommage des routeurs (inscription dans le DNS des interfaces des équipements identifiés comme tels).

Un autre exemple intéressant est le traitement des incidents liés à la sécurité, pour lequel le gain de temps est précieux et la fiabilité du processus renforcée par l'automatisation. À partir du moment où nous avons connaissance d'un incident de sécurité, la chaîne de traitement est automatisée (avec supervision des tâches par une expertise humaine toutefois) : filtrage de la machine sur les routeurs de cœur, redirection vers un portail captif indiquant à l'utilisateur de prendre contact avec son correspondant réseau, signalement au correspondant réseau concerné, au CERT et ouverture d'un ticket dans notre base d'incidents. Beaucoup de ces actions ont été rendues possibles par la mise en place de notre système d'information.

3.3 Documentation

Pour un service d'exploitation, la documentation est un outil de travail primordial. De sa justesse et de sa précision dépendent la rapidité et l'efficacité des interventions.

La documentation concerne à la fois des objets graphiques (divers plans du réseau, des locaux techniques, etc.), mais également des objets plus immatériels (quel réseau est affecté à quel établissement, quel correspondant réseau s'occupe de telle machine, etc.).

Jusqu'à la mise en place du système d'information, toutes les documentations produites par le CRC étaient générées manuellement, à partir de relevés sur le terrain (dans les locaux, les chambres de tirage, ou sur les équipements). Ces documents représentent une charge de travail lourde, fastidieuse et ingrate, et leur qualité s'en ressent.

La mise en place du système d'information a eu comme effet d'éliminer des listes réparties à divers endroits (feuilles de calcul diverses et variées, fichiers de zones DNS, mémoire de certaines personnes), et de concentrer bon nombre de ces informations dans une seule base de données, ce qui en facilite et rationalise la gestion.

L'autre aspect de la documentation est graphique : une partie des schémas réseau est maintenant produite automatiquement à partir du système d'information. Faut-il le préciser, aucun membre de l'équipe ne songerait ne serait-ce qu'une seconde à revenir en arrière !

3.4 Visibilité

Enfin, la visibilité des informations est le dernier objectif de nature organisationnelle. Il s'agit d'offrir une fenêtre sur les informations suivant la catégorie d'utilisateur (l'équipe du CRC a accès à toutes les informations, mais les correspondants réseau n'ont que celles qui les concernent, par exemple).

Le système d'information a été construit prioritairement pour améliorer l'efficacité du CRC. Dans un premier temps, il est donc normal que la visibilité des données soit restreinte à l'équipe du CRC. C'est ainsi que les membres de l'équipe peuvent avoir accès par exemple à l'ensemble des réseaux (utilisés ou libres), l'ensemble des zones DNS gérées, l'ensemble des plages DHCP définies, la configuration de tous les routeurs ; etc. Cette visibilité peut s'étendre à d'autres programmes : c'est ainsi que le logiciel de métrologie NetMET reçoit du système d'information, pour chaque établissement, la liste des réseaux routés sur Osiris.

La visibilité est ensuite étendue à l'ensemble des correspondants réseau, ce qui permet à chacun d'avoir un meilleur contrôle sur les informations qui le concernent, et d'offrir un meilleur service à ses utilisateurs. En retour, l'autonomie gagnée par les correspondants permet de détecter plus rapidement les problèmes potentiels. Par exemple, un correspondant réseau intrigué par le comportement d'une machine distante sur Osiris peut aisément retrouver, en totale autonomie, le correspondant responsable de cette machine. Parmi les projets qui seront réalisés à court terme, chaque correspondant pourra avoir accès à la métrologie (graphes RRDTools) qui le concerne sur les ports des équipements par lesquels ses flux transitent.

3.5 Vers un intranet des correspondants

La réalisation d'un système d'information se concrétise par la mise en place d'un « intranet des correspondants réseau ». Cet espace Web rassemble en un point unique toutes les briques accessibles du système d'information.

4 Le système d'information Osiris

Cette section décrit le système d'information dans sa globalité : démarche, domaines fonctionnels, outils et état de réalisation.

4.1 Démarche

À l'inverse d'autres projets de système d'information pour la gestion d'un réseau universitaire présentés aux précédentes JRES ([4] et [5]), conçus comme des monolithes pour couvrir un ensemble de besoins spécifiques, notre démarche se veut à la fois plus modeste et plus ambitieuse.

Avec des moyens en termes de ressources de développement plus limités, nous avons entrepris la construction d'un système d'information au rythme des besoins les plus immédiats. Notre système d'information est constitué d'un ensemble de modules relativement autonomes, mais utilisant une base commune. À l'heure actuelle, tout n'est pas encore réalisé, mais nous connaissons la direction. Certains projets nécessitent de rassembler des données, ces collectes constituant elles-mêmes des tâches de grande ampleur (voir section 7).

L'ambition réside dans la volonté de pouvoir distribuer nos outils. Le credo utilisé dans les développements consiste à « mettre la politique dans les données, et pas dans le code ». C'est ainsi que la première des applications, WebDNS, peut être utilisée dans d'autres environnements très différents d'Osiris. La démarche de publication d'un outil est toutefois très lourde, car passer d'un code « bien écrit » à un logiciel librement téléchargeable demande un effort de documentation, de test et de validation très important.

Cet effort est toutefois récompensé par l'intérêt que la communauté y trouve, et la mise en commun de nos outils nous permet d'avoir des logiciels globalement plus fiables.

4.2 Les domaines fonctionnels

Le système d'information, réalisé en partie et planifié pour le reste, est divisé en grands domaines fonctionnels comme résumé sur la figure 1.

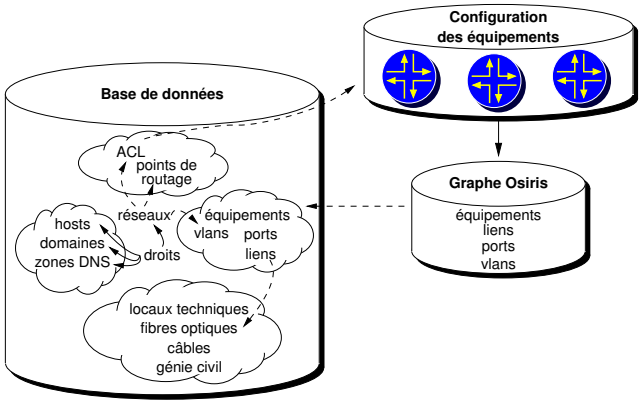

Figure 1 – *Le système d'information dans sa globalité*

Le cœur actuel du système d'information est constitué par la base de données de l'application WebDNS. Cette application est née d'un besoin immédiat de gestion de l'enregistrement des machines dans le DNS. L'accent a été mis lors de la conception sur la délégation de l'enregistrement vers les correspondants réseau. Par la suite, d'autres fonctionnalités sont venues étendre cette application, comme la gestion de DHCP, des rôles de messagerie et bientôt la gestion du filtrage (*access lists*, ou *ACL*) sur les routeurs.

En réalité, comme le précise très rapidement la documentation de l'application, WebDNS a constitué le début du système d'information, car nous avons dû intégrer deux types d'informations qui n'ont à priori rien à voir avec la gestion de zones DNS : les réseaux (avec établissement de rattachement, communauté d'usage, localisation, etc.) et les droits nécessaires pour effectuer la délégation. Ces informations représentent une documentation des aspects organisationnels (qui est responsable de quelle machine ou de quel domaine, à quel établissement est rattaché quelle plage d'adresses IP, etc.) dont l'utilisation s'étend bien au delà de la stricte application WebDNS.

La figure 1 inclut également un domaine fonctionnel regroupant les informations relatives à l'infrastructure physique (fibres optiques, câbles, etc.). Nous verrons dans la section 7 que ces informations ne sont pas encore présentes dans la base, mais sont actuellement en cours de collecte.

Le dernier grand domaine fonctionnel est celui de la gestion de la topologie du réseau, aux niveaux 2 et 3 du modèle OSI (réseaux, vlans, etc.). Cette notion de topologie est un constituant essentiel de notre système d'information.

Une des originalités de notre démarche est d'alimenter la base de données du système d'information à partir d'informations déduites de là où elles sont toujours à jour : les configurations des équipements réseau. Actuellement, toutes les heures, la topologie entière du réseau Osiris est recalculée à partir des configurations des équipements, et un fichier représentant cette topologie est généré. Pour le moment, pour des raisons que nous verrons dans la section 6, les données ne sont pas encore injectées dans la base.

Ce transfert automatisé vers la base de données n'est toutefois pas un pré-requis pour l'utilisation de notre système d'information. Toujours dans la perspective de distribuer nos outils, l'utilisation de l'injection automatisée d'information à partir des configurations des équipements peut s'avérer trop lourde à mettre en place si la topologie est simple et très statique.

5 WebDNS : le cœur du système

Comme nous l'avons vu, WebDNS représente le cœur du système d'information. De ce point de vue, le nom (WebDNS) est réducteur mais il correspond au besoin immédiat que nous avons cherché à satisfaire. Il faudra envisager de renommer cette application dans un futur proche.

Cette section décrit brièvement la genèse de cette application, ainsi que ses extensions, puis décrit en quoi les informations placées dans la base servent de support pour d'autres applications présentes et à venir.

5.1 Historique

Comme nous l'avons signalé, le besoin de WebDNS a surgi lorsque, en 2001, le disque hébergeant la base de données des déclarations DNS est tombé en panne. En l'absence du rédacteur de l'ancienne application, du mainteneur, de documentation... et de sauvegardes (heureusement, les zones DNS étaient conservées), nous avons entrepris la rédaction d'un nouvel outil plus moderne et surtout conservant une centralisation de la gestion tout en autorisant une délégation de la gestion des données, via un mécanisme de droits fins.

Après la récupération des données à partir de divers fichiers épars (feuille de calcul des sous-réseaux, liste des correspondants, fichiers de zones, etc.), nous avons ouvert l'application aux correspondants en juin 2002. Aujourd'hui, après 3 années d'exploitation, 23 000 noms sont enregistrés dans la base, dont 50% ont été saisis ou modifiés depuis le chargement initial, soit environ 15 modifications par jour ouvrable.

L'application a été présentée et démontrée aux JRES en novembre 2003. Devant l'intérêt suscité, un effort de documentation et de rédaction de scripts pour l'installation et l'importation initiale de données a été fait. Cet effort a été concrétisé par une annonce dans la liste de diffusion `webdns@u-strasbg.fr` en avril 2004. Une nouvelle version a vu le jour, annoncée plus largement en avril 2005 sur d'autres listes plus générales. Cette application est aujourd'hui disponible sur :

```
ftp://ftp.u-strasbg.fr/pub/crc/webdns/
```

WebDNS a été installée sur des sites très divers, depuis un laboratoire individuel jusqu'à un grand campus parisien avec ses 240 zones DNS, validant ainsi les principes initiaux de conception.

5.2 Fonctionnalités de base

La fonctionnalité de base de l'application est de permettre à un correspondant réseau, via un navigateur Web standard, de déclarer ses machines dans le DNS, c'est à dire d'associer à un nom une ou plusieurs adresses IPv4 ou IPv6.

Périodiquement (toutes les 10 minutes sur Osiris), les fichiers de zones sont générés sur le serveur DNS à partir des données qui se trouvent sur le serveur hébergeant la base. Par construction, les zones générées sont syntaxiquement valides, et il n'y a plus d'incohérence comme celles que ZoneCheck[1] ou DNSReport [2] signalent encore trop souvent.

Les fonctionnalités ajoutées par la suite concernent deux domaines : DHCP et les rôles de messagerie.

La gestion de l'allocation des adresses IPv4 via DHCP est concrétisée, pour les correspondants réseau, par la possibilité de saisir une adresse MAC pour chaque machine (pour effectuer un adressage statique) ou de définir un intervalle d'adresses IP pour l'allocation dynamique. Comme pour la gestion des zones DNS, le fichier de configuration du serveur DHCP est généré périodiquement. Ceci permet, notamment à l'aide de la fonction de relais DHCP offerte par la plupart des routeurs, d'organiser et de fiabiliser un service DHCP centralisé à l'échelle d'un campus. Après seulement 5 mois de mise en service sur Osiris, 1025 adresses MAC ont été ajoutées par les correspondants dans 42 sous-réseaux pour l'adressage statique, et 17 intervalles couvrant 1111 adresses dynamiques ont été déclarés.

La dernière fonctionnalité ajoutée à WebDNS est la gestion des « rôles de messagerie » : elle permet à un correspondant réseau dûment autorisé de définir quelles sont les adresses possibles pouvant figurer dans une adresse électronique (en partie droite du symbole `@`), et vers quelle machine il faut rediriger les messages. Concrètement, cela signifie qu'un MX

[1] www.afnic.fr/outils/zonecheck
[2] www.dnsreport.com

à ce nom doit être publié dans le DNS, et qu'une entrée doit être ajoutée dans la table de routage du MTA (`sendmail`, `postfix` ou équivalent).

5.3 Les réseaux et les droits

L'application WebDNS intègre une notion de « réseau ». Défini formellement comme un « domaine de *broadcast* », un réseau est représenté par une plage d'adresses IPv4 et IPv6, un établissement, une communauté d'usage, une localisation géographique, et un ou plusieurs correspondants réseau responsables. Cette notion est très peu utilisée dans l'application (essentiellement pour la sélection des réseaux à consulter), mais nous a semblé essentielle :

– pour documenter les réseaux et abandonner enfin la vieille feuille de calcul que tout le monde utilise ;
– pour gérer l'espace d'adressage, repérer les réseaux occupés, énumérer les réseaux libres, etc. ;

Par la suite, nous avons trouvé de nouvelles applications à cette notion, comme par exemple la génération de fichiers de configuration pour le serveur DHCP, pour l'outil netMET de métrologie (pour associer des plages d'adresses IP à des établissements), etc.

La deuxième notion fondamentale pour le système d'information est la notion de droit, qui permet de formaliser et documenter qui est responsable de quoi sur le plan organisationnel. Plusieurs types de droits coexistent, en fonction des objets manipulés :

– des droits sur les réseaux, comme vu précédemment, qui permettent de savoir si un correspondant peut déclarer des intervalles dynamiques DHCP sur ce réseau, ou encore y déclarer des ACL ;
– des droits sur des plages d'adresses (IPv4 ou IPv6). Ainsi, par exemple :
  ```
  <allow,192.168.1/24>
  <deny, 192.168.1.252/30>
  <deny, 192.168.0.0/32>
  ```
  Ces lignes définissent un droit sur toute la plage de 256 adresses, sauf les 4 dernières (l'adresse de diffusion, et sur Osiris, l'adresse VRRP de la passerelle et les deux adresses réelles des routeurs) et l'adresse 0 qui ne correspond à aucune machine. On voit donc que la granularité des droits est très fine, et permet de gérer toutes les situations ;
– des droits sur des domaines ;
– d'autres types de droits suivant des applications plus particulières, comme par exemple l'accès à des profils DHCP (qui permettent de configurer le démarrage de clients légers ou de stations sans disque).

Une action nécessite parfois plusieurs droits : par exemple, pour supprimer une machine, il faut que le correspondant ait accès à la zone et à l'ensemble des adresses de la machine. Ce modèle s'adapte aussi bien à une grande zone de 23 000 machines qu'à un grand campus réparti sur 240 zones.

Les droits sont gérés au niveau d'un groupe, et les personnes (les correspondants) sont affectés à des groupes. Une évolution envisagée est l'héritage de droits, qui permettrait de définir les droits d'un groupe par rapport à un autre groupe. Ainsi, un correspondant pourrait à son tour déléguer une partie de ses droits. Les administrateurs (i.e. les membres du groupe contenant les ingénieurs du CRC) n'ont pas de droits particuliers dans WebDNS. Seul un attribut du groupe (l'attribut « admin ») permet à ses membres de définir les droits des autres groupes.

5.4 Extensions

Certaines extensions ont vocation à être intégrées dans WebDNS. Ainsi, la gestion des ACL (*access-lists*) permettra à chaque correspondant ayant les droits sur le réseau concerné de définir des filtres. Ces filtres seront ensuite installés sur les routeurs de cœur.

D'autres extensions n'ont pas vocation à être intégrées, car trop dépendantes du mode de fonctionnement du CRC. Ainsi, le traitement automatisé des incidents de sécurité nécessite la localisation du réseau concerné et du ou des correspondants responsables, ainsi qu'un filtrage sur le routeur. Pour ce faire, les scripts utilisent les données du système d'information.

6 Topologie

Une des caractéristiques de notre démarche est l'intégration des informations mémorisées dans les équipements dans le système d'information, et la construction d'un graphe modélisant la topologie du réseau. Dans cette section, nous décrivons le contexte qui nous amené à cette intégration, puis les outils utilisés, les outils réalisés et les applications actuelles ou à venir de cette intégration.

6.1 Contexte

La mise en place du nouveau cœur de réseau Osiris 2 a permis d'assainir une situation où avaient été accumulées des strates historiques de cas particuliers. De plus, nous avons pu organiser une gestion rationalisée de l'infrastructure : équipements placés dans un Vlan d'administration distinct, filtrage et authentification centralisée grâce à Radius.

Les équipements embarquant des fichiers de configuration, la question de la duplication de données avec le système d'information s'est posée avant même le début du déploiement du nouveau cœur de réseau. Deux options ont été envisagées :

1. centraliser les données dans le système d'information, et générer automatiquement les configurations des équipements ;
2. conserver les données dans les équipements (qui font alors partie du système d'information), et les récupérer pour les injecter dans la base de données.

La première option avait l'avantage de permettre une confi-

guration rapide, au moins pour les premières phases du déploiement. Nous ne l'avons toutefois pas retenue, car par la suite, il aurait été très difficile de traiter rapidement des cas particuliers qui n'étaient pas prévus dans le système d'information.

Nous avons dès lors reconnu la primauté de la configuration des équipements par un être humain, et opté pour la seconde solution, qui consiste à « suivre » les configurations. Pour ce faire, nous avons rapidement adopté les outils Rancid[3] et CVSWeb[4], sans lesquels nous n'imaginerions plus aujourd'hui de travailler...

Par la suite, lors des réflexions sur WebDNS et en particulier sur la gestion des ACL, nous avons déterminé qu'il fallait ajouter les deux points de routage de chacun des 208 sous-réseaux d'Osiris. Ces informations sont très fastidieuses à saisir manuellement, et de plus très dynamiques.

Les configurations des équipements contenant déjà tous les éléments nécessaires, nous nous sommes logiquement dirigés vers une analyse syntaxique des fichiers de configuration pour extraire ces éléments, comme indiqué sur la figure 2.

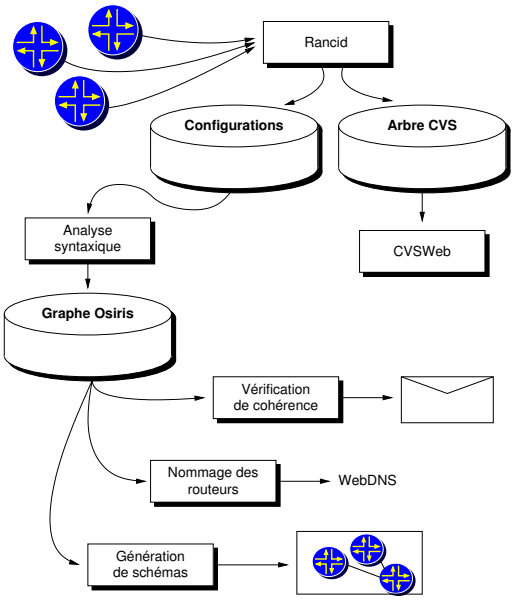

Figure 2 – *Chaîne d'outils « Topologie »*

Comme nous le verrons plus loin, le potentiel de cette analyse est considérable pour les tâches d'exploitation.

6.2 Rancid et CVSWeb

Comme nous l'avons mentionné précédemment, nous utilisons le logiciel Rancid pour récupérer périodiquement, par ssh, toutes les configurations des équipements. Rancid sait reconnaître un grand nombre de modèles, ce qui lui permet d'opérer dans un environnement hétérogène comme Osiris.

[3] www.shrubbery.net/rancid
[4] www.freebsd.org/projects/cvsweb.html

Chaque configuration est comparée à la précédente version, puis les différences s'il y en a sont mémorisées dans un arbre CVS et envoyées par courrier électronique à toute l'équipe du CRC. Ce dernier point est d'un grand intérêt car toute l'équipe est attentive aux modifications effectuées sur les configurations des équipements.

L'intérêt du stockage des configurations dans un arbre CVS est que nous avons dorénavant accès à tout l'historique des configurations depuis la mise en place du nouveau cœur de réseau. De plus, l'installation de CVSWeb rend la consultation des configurations aisée, la comparaison entre deux versions se fait de manière très visuelle, et la possibilité de « remonter dans le temps » s'est avérée quelques fois utile.

Le seul défaut de cette chaîne est qu'il n'est pas facile de savoir qui a fait une modification, il faut pour cela croiser les dates de modification avec les journaux de Radius.

Sur le plan de l'exploitation, la solution mise en place est très légère en temps et en ressources, elle ne bride pas les ingénieurs et, avec le recul, s'est révélée être très utile.

6.3 Analyse des fichiers de configuration

L'analyse syntaxique des fichiers de configuration pour en extraire des informations est une technique peu répandue. Les administrateurs vont spontanément vers l'interrogation d'équipements via SNMP. Nous n'avons pas retenu cette méthode car les informations sont difficiles à extraire avec un protocole de trop bas niveau, elles ont une logique de structuration très différente d'un objet à l'autre, les MIB standards s'avèrent très limitées, et enfin les MIB propriétaires sont souvent peu documentées et fournissent un niveau inégal d'information, insuffisant pour la plupart de nos besoins. Par exemple, peu de MIB fournissent des informations sur la configuration VRRP d'un routeur, les Vlans autorisés sur un lien, ou encore la présence d'instances de routage distinctes[5].

À l'inverse, les fichiers de configuration, même avec une syntaxe peu structurée comme sur IOS, sont relativement faciles à analyser automatiquement. Ainsi, toutes les heures, ils sont parcourus et le graphe complet du réseau et des équipements est généré. Il est placé pour le moment dans un fichier, afin de le manipuler plus aisément pendant les phases de développement qu'on ne pourrait le faire avec une base de données relationnelle. Le format de ce fichier permet d'étendre le graphe généré pour y intégrer davantage d'informations. Même si le projet est d'intégrer les informations du graphe à terme dans la base de données, il est très probable que le fichier restera un support complémentaire pour des raisons de performances.

Représenter un réseau et des équipements au niveau de détail nécessaire n'est pas chose aisée, et nous sommes parvenus à une modélisation des fonctions de commutation et de routage capable de représenter des équipements aussi différents

[5] Notion spécifique aux équipements Juniper.

que des commutateurs-routeurs (bien que nous n'en ayons pas), des garde-barrières bridgés ou routés, des liaisons spécialisées et même des équipements ATM ! Pour le moment, nous avons développé des analyseurs pour des routeurs Juniper (JunOS) et des commutateurs Cisco (IOS), et il est bien évidemment possible d'en ajouter d'autres au fur et à mesure des besoins.

Le graphe de l'ensemble des 145 équipements de la dorsale du réseau Osiris représente 20154 nœuds, et est généré en moins de 30 secondes.

6.4 Applications aujourd'hui opérationnelles

Au fur et à mesure de notre avancée, nous avons mesuré le potentiel important que recèle cette analyse. Pour le moment, nous avons implémenté les outils suivants :

- vérification de la cohérence des informations : tous les liens sont-ils identifiés et documentés ? tous les réseaux sont-ils routés ? y a-t'il des configurations VRRP pour des réseaux routés à un seul endroit ?
- vérification du nommage des interfaces des routeurs par rapport au DNS, et envoi par mail d'un script pour actualiser la base WebDNS (pour le moment, ces modifications sont supervisées par un humain) ;
- génération automatique de schémas de niveau 2 (par Vlan) et de niveau 3 (pour un sous-réseau IPv4 ou IPv6, voire plusieurs sous-réseaux).

La génération de schémas (voir exemples en figure 3) était au départ un exercice de style, une sorte de gadget pour nous aider à visualiser le graphe produit pendant les phases de développement. Avec l'expérience, elle s'est révélée être une avancée majeure pour le CRC. Dorénavant, l'équipe est déchargée de la lourde tâche de production de schémas réseau. De plus, ces schémas sont générés toutes les heures, ce qui signifie qu'ils sont virtuellement toujours à jour. Enfin, du fait de la représentation graphique, des erreurs de configuration qui sont longtemps restées cachées dans des fichiers de configuration apparaissent enfin immédiatement !

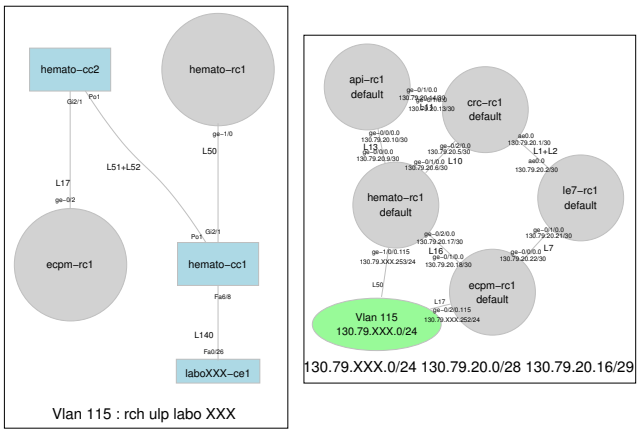

Figure 3 – *Exemples de schémas de niveau 2 et 3*

[6] www.graphviz.org

Les schémas sont produits avec les utilitaires de la remarquable suite Graphviz[6]. Il ne s'agit pas d'une qualité artistique visant à concurrencer la Joconde, mais les graphes sont suffisamment clairs pour détecter immédiatement les problèmes et apporter des informations utiles. Ainsi, sur l'exemple de la figure 3, le schéma de gauche est un schéma de niveau 2 (Ethernet) montrant tous les équipements connectés au Vlan 115 (les rectangles sont les commutateurs, les cercles les routeurs) avec mention des numéros de liens et des interfaces physiques. De même, le schéma de droite est un schéma de niveau 3 (IP) montrant la connexion de ce même Vlan (l'ellipse) à la dorsale Osiris. On voit clairement les 5 routeurs de la dorsale, et les deux liens qui raccordent ce Vlan au routeur VRRP principal et au routeur VRRP secondaire.

6.5 Applications prévues

Les applications présentées ci-dessus ne sont qu'une petite partie du potentiel important que procure l'analyse syntaxique des fichiers de configuration, et que nous n'avons pas fini d'exploiter.

Les évolutions futures sont :

- injection de données concernant les points de filtrage des réseaux pour la mise en place de la gestion des ACL dans WebDNS, ce qui était le but premier de l'analyse syntaxique !
- injection des autres données du graphe dans la base du système d'information, permettant ainsi...
- ... d'étendre les droits sur les réseaux vers les équipements et les ports, permettant ainsi...
- ... de proposer à chaque correspondant réseau de voir les graphes de métrologie qui le concernent.
- construction d'un arbre de dépendances pour l'automatisation du traitement des tickets d'incidents réseau (annonces d'interruptions de service, d'interventions, etc.) ;
- poursuite des travaux sur les schémas pour en faire un système de navigation graphique intégré.

Les applications potentielles sont multiples et variées, et ouvrent des possibilités nouvelles pour le système d'information.

6.6 Distribution

Les outils de topologie sont en cours de développement. Si des participants aux JRES sont intéressés, ils sont invités à se manifester auprès des auteurs pour les inciter à faire l'effort de distribution de ces outils, et pour être tenus informés de l'état d'avancement.

7 L'infrastructure physique

Une des autres caractéristiques du réseau Osiris est l'importance de l'infrastructure (61 km de fourreaux, 2 800 km

de fibres optiques) dont les établissements sont en grand partie propriétaires. Cela représente une une charge lourde d'exploitation pour le CRC : demandes de travaux d'autres gestionnaires de réseaux souterrains, supervision de l'infrastructure, capacité d'intervention tant sur les fibres que sur les fourreaux, etc. Il importe donc d'intégrer l'infrastructure physique dans le système d'information.

Nous décrivons dans cette section la démarche générale vis à vis du système d'information, les deux domaines fonctionnels pour lesquels nous collectons actuellement les données, et enfin nous dressons un point sur ce qu'il reste à développer.

7.1 Démarche

N'ayant pas les ressources pour développer immédiatement l'intégration des données dans le système d'information, et n'ayant pas non plus la possibilité de récupérer automatiquement ces données, nous avons entrepris une démarche en trois temps :

1. élaboration d'un modèle de représentation des données, ainsi que d'une nomenclature pour repérer et étiqueter les objets ;
2. parcours sur le terrain pour collecter les données dans une feuille de calcul, et éventuellement étiqueter les objets : c'est ainsi que toutes les armoires et les tiroirs optiques ont été physiquement étiquetés ;
3. dès que les ressources humaines le permettent, rédaction de l'application et intégration des données en provenance des feuilles de calcul.

La deuxième étape est évidemment la plus fastidieuse. Heureusement, les données sont pérennes, l'infrastructure physique ayant pour caractéristique de ne pas être trop dynamique.

7.2 Fibres optiques

La collecte des informations sur les fibres optiques à partir des cahiers de recette a commencé lorsqu'il devenait clair que le nouveau cœur de réseau Osiris 2 serait en Ethernet Gigabit, beaucoup plus exigeant en terme de budget optique (distance et atténuation) que la technologie ATM. Il a alors fallu repérer les liens qui nécessiteraient des lasers LX ou SX.

Nous avons donc rangé dans une feuille de calcul des informations issues des cahiers de recettes des fibres (type de fibre, connecteurs, distance, atténuations, extrémités, etc.).

Lorsque ces informations seront placées dans le système d'information, les premières applications seront :

– trouver un chemin entre deux points quelconques du réseau, identifier les jarretières intermédiaires nécessaires, et connaître les caractéristiques (atténuation, distance) du chemin obtenu ;
– déterminer le budget optique sur un chemin existant ;
– connaître le nombre de fibres disponibles entre deux points.

7.3 Génie civil et fourreaux

Les personnes ayant suivi de près la construction de l'infrastructure de génie civil partant à la retraite dans quelques petites années, il importe d'identifier rapidement les constituants de l'infrastructure (parcours, localisation des chambres de tirage, pénétration dans les bâtiments, etc.).

La collecte d'information actuellement en cours comprend l'identification des quelques 500 chambres de tirage d'Osiris (avec coordonnées GPS et photographie éventuelle servant à localiser la chambre) et les informations administratives (propriétaire du fourreau et autres).

Les applications attendues de ce repérage sont :

– faciliter les interventions, ce qui nécessitera de fournir l'accès à ces informations au prestataire qui assure l'astreinte sur l'infrastructure ;
– répondre aux demandes de travaux des autres gestionnaires de réseaux ;
– donner une meilleure connaissance pour faciliter la mise en place d'extensions.

7.4 Applications et extensions prévues

Bien que les deux domaines fonctionnels décrits ci-dessus ne soient pas encore complètement implémentés, nous savons d'ores et déjà qu'il reste un travail important de repérage des câbles optiques et d'identification des locaux techniques.

La concrétisation de l'ensemble de ce travail sera la production automatique de schémas, dont la réalité géographique sera plus tangible que celle des schémas logiques construits par l'analyse des configurations des équipements réseau.

8 Conclusion

Mesurant les objectifs politiques fixés par les établissements et les contraintes d'exploitation d'un réseau récemment rénové, le CRC s'est résolument engagé dans une démarche pour la réalisation d'un système d'information.

Une caractéristique du projet est le développement incrémental, au fur et à mesure des besoins et des disponibilités pour le développement. Partant d'une application initialement conçue pour la gestion du DNS, nous bâtissons progressivement un système complet pour la gestion technique du réseau, depuis l'infrastructure physique jusqu'aux services associés.

Avec l'expérience, la mise en place des premières briques du système en a confirmé l'utilité. La délégation de certaines tâches vers les correspondants réseau offre une meilleure qualité de service tout en déchargeant le CRC d'une mission sans valeur ajoutée. L'automatisation qui découle des don-

nées accumulées représente un gain de temps et de fiabilité énorme.

Une autre caractéristique du projet est l'inclusion des configurations des équipements réseau dans le système d'information, permettant d'obtenir des informations très intéressantes. Ainsi, la production de schémas réseau toujours à jour est d'une valeur inestimable.

Enfin, notre approche est résolument tournée vers l'ensemble de la communauté universitaire, à travers la distribution de l'application WebDNS. Nous pourrons faire l'effort de distribuer les autres outils rédigés, si l'intérêt suscité par cet article est suffisamment important.

Références

[1] P. David et J. Benoit. Une application pour décentraliser la gestion du dns. Dans *JRES2003*, Lille, 2003.

[2] Groupe de travail CRU. Les réseaux universitaires : quels coûts ? Dans *JRES2005*, Marseille, 2005.

[3] P. Pegon. Fiabilisation d'une architecture dns. Dans *JRES2003*, Lille, 2003.

[4] I. Ben Said et al. Système d'information pour la gestion d'un réseau d'université. Dans *JRES2001*, Lyon, 2001.

[5] L. Gydé et N. Meneceur. Sirap : Le système d'information du réseau académique parisien. Dans *JRES2003*, Lille, 2003.