CROUS de Strasbourg : Problématique de raccordement d'une cité universitaire

■ Yannick OTTINGER, Yannick.Ottinger@crous.u-strasbg.fr
Crous de Strasbourg, Service informatique

Cet exposé présente le contexte global, les objectifs et les contraintes du raccordement des sites du CROUS de Strasbourg (logements des étudiants et salles libre-service dans les Cités Universitaires, services administratifs) au réseau métropolitain strasbourgeois OSIRIS ainsi que la solution retenue basée essentiellement sur les réseaux virtuels par authentification.

■ Contexte

Le CROUS (Centre Régional des Œuvres Universitaires et Scolaires) de STRASBOURG gère les services de la vie étudiante de l'Académie de Strasbourg : logement, restauration, bourses, culture, emploi, social, voyages. A Strasbourg, près de 50 000 étudiants sont gérés par le CROUS dont environ 5 000 hébergés dans les Cités Universitaires représentant 9 sites et 22 bâtiments.

Le projet du CROUS consiste à raccorder les 5 000 étudiants logés et 100 agents administratifs à OSIRIS (Réseau métropolitain), à RENATER (Réseau National de Télécommunications pour l'Enseignement et la Recherche) et à INTERNET.

OSIRIS irrigue l'ensemble des campus situés dans la Communauté Urbaine de Strasbourg. Plus de 20 sites, soit 120 bâtiments sont reliés au réseau Osiris, et à travers lui à Internet. Les liaisons font appel à des technologies très différentes : faisceaux hertziens et infrarouges, fibre optique, liaisons Transfix France Télécom.

La structure originale du réseau Osiris en deux sous-réseaux sécurisés (Enseignement/Recherche et Administration), la première mise en service en France, permet de garantir la confidentialité des informations (gestion financière et comptable, notes d'examen…). Un troisième sous-réseau, réservé aux étudiants, sera progressivement mis en place afin d'éviter la saturation due au trafic généré par une communauté forte de plus de 50 000 étudiants à Strasbourg, et suite au raccordement à Osiris des cités universitaires gérées par le CROUS.

Une Convention CROUS/OSIRIS a été rédigée pour préciser les modalités de la mise à disposition du réseau OSIRIS et des services qui lui sont associés : objet, participation financière, développement du réseau, maîtrise d'œuvre, utilisation du réseau, gestion technique du réseau, renouvellement de la Convention.

Dans le cadre de la diffusion des Nouvelles Technologies de l'Information et fortement encouragé par le Ministère de l'Education Nationale, de la Recherche et de la Technologie, le projet du CROUS est subventionné par le CNOUS et par les collectivités territoriales. Ce projet doit permettre à l'étudiant aux revenus modestes d'avoir accès à OSIRIS et à INTERNET à moindre coût tout en valorisant le parc immobilier du CROUS. Le CROUS de Strasbourg fait figure de pionnier dans ce domaine. Financièrement, il s'agit de privilégier les coûts d'investissement par rapport aux coûts de fonctionnement. Pédagogiquement, la chambre d'étudiant est vue comme le prolongement de la salle de cours pour améliorer les conditions de travail de l'étudiant.

■ Besoins

La mise en réseau des Cités Universitaires à travers le réseau métropolitain OSIRIS comporte 3 volets :

- câblage interne des bâtiments dans le respect des normes de câblage de catégorie 5 (câble 4 paires torsadées à 120 Ohms – 100 MHz – connectique RJ45 ou fibre optique multimode 62,5/125 pour des distances supérieures à 90 m),
- mise en place d'une infrastructure de transport via fibre optique monomode 9/125, multimode 62,5/125 (génie civil pour la pose de fourreaux souterrains) ou faisceau hertzien (34 Mbits/s dans la bande des 26GHz selon autorisation de l'ART) si les distances sont trop importantes ou si non autorisation d'occuper le domaine de la voirie publique,
- installation d'équipements actifs réseaux tels que hubs, commutateurs ATM/Ethernet, routeurs, serveurs.

Compte tenu du contexte éducatif, les critères suivants sont primordiaux pour le choix des équipements réseaux :

- Sécurité par authentification.
- Simplicité de connexion à OSIRIS.
- Robustesse du réseau.
- Possibilité d'avoir deux fournisseurs d'accès Internet.

Sécurité par authentification

Compte tenu de la location à durée déterminée des chambres de CU, il est particulièrement vital de mettre en œuvre une politique d'authentification de l'usager. Chaque utilisateur doit être identifié avant de pouvoir accéder à des services extérieurs. Cette identification doit être simple et corrélée avec les services de boîtes aux lettres électroniques mises en place par les universités pour les étudiants. Cette authentification repose sur un concept de deux zones : une zone accessible sans authentification avec des services réseaux minimum comme par exemple des serveurs d'information (cf. point suivant) et une zone dite OSIRIS qui est accessible après authentification. Un suivi des connexions doit être possible. Un avis sera demandé à la CNIL.

Simplicité de connexion à OSIRIS

A terme, le projet devra permettre la connexion de 5 000 chambres avec une durée moyenne d'occupation d'un an, soit un raccordement de 5 000 machines chaque année entre septembre et octobre. Par conséquent, il est impératif de prévoir une infrastructure de réseau qui nécessite le minimum d'installation et d'intervention sur les machines. En particulier, il n'est pas souhaitable d'avoir à paramétrer un logiciel spécifique. De la même manière, il est supposé que l'étudiant a une compétence suffisante pour se connecter par lui-même. Le personnel du CROUS ne doit pas intervenir pour une installation. Il est nécessaire de prévoir l'information et la communication sur le mode de connexion. Il semble plus que probable qu'une gestion dynamique des adresses IP avec une translation d'adresse vers une classe officielle soit retenue.

Robustesse du réseau

Ce critère est aussi très important. En cas de problème de connexion soit par inadvertance, soit par malveillance, les équipements réseaux doivent pouvoir isoler le port RJ45 concerné. Pour la liaison de raccordement au backbone, le choix stratégique se porte sur la technologie ATM pour plusieurs raisons : une bande passante très large, des débits importants de 155 à 622 Mbits/s et la possibilité d'affecter des portions du trafic à des applications particulières, telles que la voix et le multimédia.

Possibilité d'avoir deux Fournisseurs d'Accès Internet (FAI)

Une extension des services offerts pourrait être l'accès à un autre fournisseur Internet que RENATER/OSIRIS. Ce dernier étant à vocation éducative, il est fortement envisagé que les étudiants puissent accéder à un autre fournisseur avec des conditions spécifiques (facturation par exemple).

Il s'agit de séparer les flux dits « professionnels » (accès via RENATER pour ce qui est formation, éducation) de ceux considérés comme « personnels » (via un autre fournisseur d'accès). La problématique réside dans la mise en œuvre de cette politique. RENATER n'ayant pas de monopole sur l'ensemble des flux qui peuvent être générés par les étudiants, il faut laisser le secteur économique jouer son rôle.

Au moins 2 solutions existent pour aiguiller le trafic sortant vers le FAI concerné : filtrer les adresses IP destinataires présente des risques importants et n'est pas le rôle de RENATER ; identifier les adresses IP des sites RENATER en les laissant passer et en redirigeant les adresses IP non concernées par RENATER vers l'autre FAI semble être la meilleure solution techniquement possible. Concernant l'adressage IP, la double connexion (RENATER et FAI) crée une complexité de routage plus ardue (trafic devant emprunter les mêmes routes à l'aller et au retour). Un groupe de travail est chargé de préconiser une approche consolidée.

■ Cahier des charges[1]

Le cahier des charges a été rédigé pour exprimer nos besoins. Les points suivants sont les principes de base pour réaliser une maquette simulant le futur réseau étudiant du CROUS :

- Equiper l'ensemble des sites avec des commutateurs ATM/ETHERNET permettant d'authentifier les utilisateurs. Les commutateurs actuellement en place sur le réseau universitaire OSIRIS étant de marque

[1] Pour réaliser une maquette de test du réseau étudiant.

ALCATEL-XYLAN et les routeurs de marque CISCO, les matériels proposés devront être parfaitement compatibles avec tests d'interopérabilité à l'appui.

- Utiliser le principe des VLANs par authentification pour vérifier l'identité des utilisateurs par la saisie d'un login et d'un mot de passe. Le port du commutateur est affecté dynamiquement du VLAN par défaut au VLAN paramétré pour l'utilisateur qui s'authentifie : ceci permet une mobilité géographique des utilisateurs (pas de brassage physique sur les équipements) et une optimisation de la sécurité des postes de travail.
- Le serveur d'authentification et son interface graphique seront configurés dans un environnement PC Windows NT 4.0 Server.
- Mettre en œuvre un client d'authentification simple à utiliser autant pour la connexion que pour la déconnexion comme par exemple de type XVSS (protocole Microsoft DLC 32 bits de niveau 2) à privilégier à TELNET (protocole IP de niveau 3). La méthode d'authentification ne devrait pas varier en fonction du client (PC Windows 95 ou 98, PC Linux, MAC). Nous évaluons que 90% du parc concerné par l'authentification est de type PC Windows 95 ou 98.
- Le client d'authentification sera déployé facilement et rapidement sur l'ensemble des postes clients.
- Définir l'architecture logique avec des VLANs par défaut, des VLANs mobiles ou non mobiles, des VLANs authentifiés, un VLAN sécurisé pour le serveur d'authentification.
- Définir les règles d'affectation aux VLANs pour des règles de type « lier une adresse Ethernet à un port et à un protocole ».
- Utiliser des outils d'administration fiables pour la supervision du réseau.
- Tenir au journal des connexions pour identification en cas d'acte de piratage.
- Superviser l'ensemble des ports des commutateurs à partir d'un poste de gestion centralisé (par exemple situé au service informatique du CROUS) permettant de valider ou de dévalider ces ports dans le cadre de la politique globale de sécurité.
- Définir des profils utilisateurs en fonction du VLAN d'authentification.
- Identifier les connexions ou tentatives de connexion et déconnexions à partir du serveur d'authentification (port du commutateur, IP, MAC, protocole, horaire…).
- Utiliser le protocole ATM 155 pour le réseau d'interconnexion (jusqu'au dernier commutateur), Ethernet 10 Mbits/s pour raccorder les postes clients et Ethernet 100 Mbits/s pour les serveurs.
- L'adressage IP sera dynamique via un serveur DHCP (Dynamic Host Configuration Protocol) lors de l'affectation dans un VLAN.
- Translation d'adresses IP via NAT (Network Area Translation) vers un réseau de classe C officielle pour accéder à Internet.
- Définir un plan d'adressage.
- Utiliser le protocole de routage OSPF déjà utilisé sur Osiris.
- La création de la base de données des utilisateurs devra pouvoir se faire de manière automatique par un chargement d'un fichier externe.
- La base de données des utilisateurs devra à terme pouvoir supporter d'autres méthodes d'authentification telles que carte à puce.
- Définir une méthode de sauvegarde des bases de données.
- Sécuriser le réseau administratif par rapport au réseau étudiant (Fire-Wall).

■ Règles de gestion

Les règles suivantes permettent d'exprimer des choix de gestion qui représentent des contraintes techniques du projet :

- Un étudiant devra pouvoir s'authentifier à partir de n'importe quelle chambre de la Cité Universitaire à laquelle il appartient. Il ne pourra pas s'authentifier à partir d'une chambre d'une autre cité universitaire.
- Un étudiant ne pourra avoir qu'une seule connexion simultanée.
- Des salles libre-service sont prévues uniquement pour les étudiants des Cités Universitaires. Un étudiant pourra accéder au réseau Osiris, en s'authentifiant, à partir des salles libre-service de toutes les Cités Universitaires.
- Le personnel administratif ne s'authentifiera pas. Le personnel est supposé utiliser le réseau uniquement pour des besoins professionnels. Cette approche permet de réaliser une économie sur le coût des commutateurs ATM/Ethernet à acquérir puisqu'il faut un port physique de commutateur pour chaque poste de travail à partir duquel l'utilisateur doit s'authentifier.

■ Description et résultats de la maquette

La solution retenue suite à l'appel d'offres concernant les équipements actifs propose une maquette reposant sur le principe des VLANs par authentification et mettant en œuvre les éléments suivants :

- 1 châssis ATM/ETHERNET de type ALCATEL-XYLAN 590,
- 1 commutateur ATM/ETHERNET de type ALCATEL-XYLAN 210-3032,
- 1 serveur d'authentification RADIUS Steel-Belted sous Windows NT4.0 Server,
- 2 serveurs DHCP sous Windows NT4.0 Server,
- 1 client XVSS sous Windows 95,
- 1 client XVSS sous Windows 98,
- 1 client XVSS sous Linux,
- 1 client TELNET (Win 3.11, Mac…).

Principe des VLANs par authentification

Le VLAN (réseau virtuel) doit être considéré comme un domaine de broadcast. Il présente surtout l'avantage de rendre l'utilisateur indépendant de sa localisation géographique.Les VLANs par authentification viennent s'ajouter aux VLANs par port, par MAC adresse, par protocole… Techniquement, dans un VLAN, la limite est fixée à 1 000 utilisateurs connectés simultanément. Le découpage pour le CROUS se fait en fonction de la Cité Universitaire à laquelle l'étudiant a été affecté.

Initialement, avant le démarrage du poste de travail de l'étudiant, le port du commutateur qui correspond au poste de l'utilisateur qui doit s'authentifier est positionné dans un VLAN par défaut à partir duquel l'utilisateur n'a pas accès au réseau OSIRIS.

Lors de l'authentification, une phrase de bienvenue sur le réseau CROUS/OSIRIS apparaît. L'utilisateur doit saisir son login et son mot de passe pour s'authentifier. Cette procédure nécessite un dialogue entre le commutateur (agent d'authentification) et le serveur d'authentification RADIUS chargé de vérifier la conformité du login et du mot de passe et de spécifier le VLAN auquel est affecté le port de l'utilisateur authentifié.

Une adresse IP et un VLAN sont affectés à l'étudiant authentifié pour lui permettre d'accéder au réseau CROUS/OSIRIS. Au moment où l'étudiant se déconnecte (logoff), le port du commutateur est replacé dans le VLAN par défaut, l'adresse IP est réinitialisée et libérée.

Le client XVSS

Principe de fonctionnement : l'utilisateur active le processus de logon, renseigne son user id et password pour se connecter ; il active le processus de logoff pour se déconnecter. L'adresse IP est attribuée après authentification par le serveur DHCP du VLAN authentifié.

- Avantages : associé à l'utilisation du protocole DHCP, il permet une plus grande mobilité sur le campus.
- Inconvénient : il nécessite l'installation d'un soft ALCATEL-XYLAN et du protocole Microsoft DLC 32 bits.

Le client Telnet

Principe de fonctionnement : l'utilisateur fait un telnet sur une adresse IP et un port TCP spécifique, renseigne son user id et password pour se connecter et se déconnecter d'un groupe authentifié. L'adresse IP est attribuée au démarrage du poste de travail par le serveur DHCP du VLAN par défaut.

- Avantages : l'application telnet fait partie de la couche TCP/IP de Windows.
- Inconvénients : L'utilisation du client telnet induit une mobilité restreinte puisque son adresse IP reste identique après authentification (et quel que soit le groupe authentifié).

Le serveur RADIUS

Le serveur RADIUS dialogue avec l'agent d'authentification du commutateur. Il gère les profils utilisateurs, les comptes utilisateurs, les VLANs, le journal qui recense l'historique des tentatives de connexion, des connexions et des déconnexions. Le serveur RADIUS se trouve dans un VLAN sécurisé.

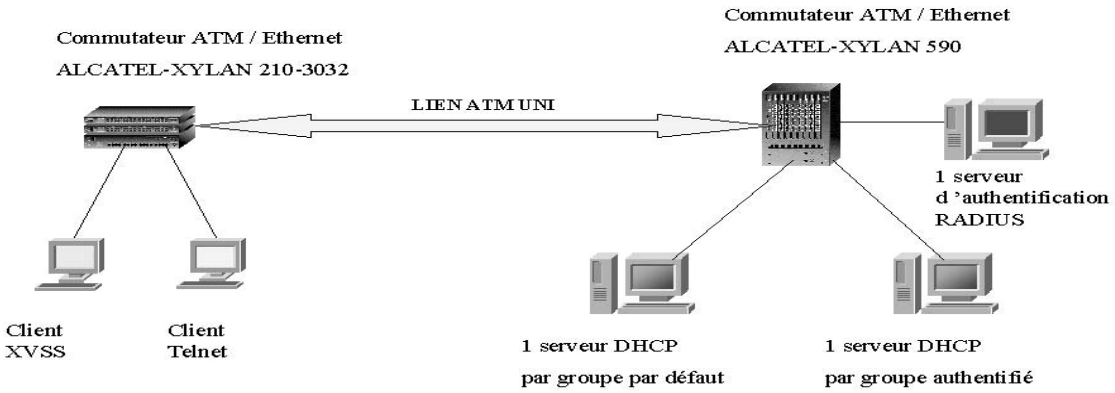
L'utilisateur a soit un login de profil XVSS, soit un login de profil TELNET. Un login XVSS ne peut s'authentifier qu'avec le client XVSS ; un login TELNET peut s'authentifier avec le client TELNET et avec le client XVSS (à cause de l'instant de l'affectation de l'adresse IP via DHCP).

Les serveurs DHCP

Il y a un serveur DHCP par VLAN. L'adresse IP est affectée dynamiquement à la machine cliente en fonction du VLAN dans lequel elle se trouve. Des plages d'adresses sont réservées pour chaque VLAN. Le serveur DHCP indique systématiquement les informations sur les adresses IP utilisées (taux d'utilisation, identification des postes de travail…).

En conclusion, la maquette réalisée pour simuler le futur réseau étudiant du CROUS a donné des résultats et des garanties satisfaisantes au niveau de l'authentification même si certains points du cahier des charges et certaines règles de gestion ne peuvent pas être respectées. Après cette étape, l'objectif est maintenant de valider un site pilote.

Architecture physique du CROUS de Strasbourg



■ Bilan du site pilote GALLIA

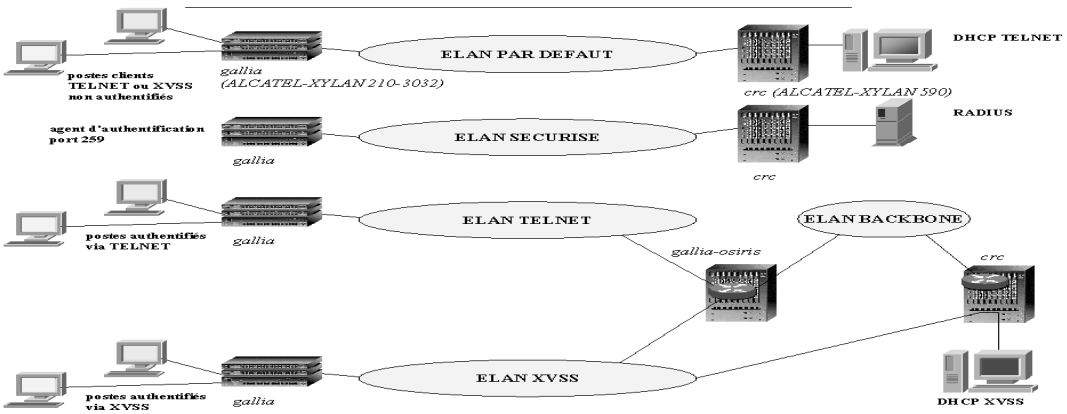
Le site pilote choisi correspond à la Cité Universitaire GALLIA avec 280 prises « étudiants » pour les étudiants résidant dans les chambres, les salles libre-service et 70 prises « administratifs » pour le personnel administratif du CROUS.

Au 01/10/1999, la mise en œuvre sur le site pilote GALLIA correspond exactement à la maquette qui a été réalisée. Chaque étudiant devra s'authentifier pour accéder au réseau.

De plus, un Fire-Wall (FW) à deux interfaces a été mis en place pour :

- protéger et interdire les intrusions sur le réseau administratif du CROUS,
- donner accès à OSIRIS (Internet et messagerie) aux agents administratifs du CROUS avec translation d'adresses IP gérée par le FW vers une adresse IP OSIRIS.

Architecture logique du CROUS de Strasbourg



Au 01/10/1999, le site pilote GALLIA a permis principalement de valider les points suivants :

- le câblage interne du bâtiment GALLIA du CROUS dans le respect des normes de câblage de catégorie 5 (280 prises) ,
- l'interconnexion du CROUS au réseau OSIRIS via 500 m de fibre optique (backbone ATM à 155 Mbits/s),
- le principe des VLANs par authentification sur des commutateurs ATM/ETHERNET ALCATEL-XYLAN avec les clients d'authentification XVSS et TELNET.

Les points suivants constituent un bilan par rapport au cahier des charges initial et font état des remarques qui concernent principalement l'administration du réseau :

- serveur d'authentification AMC (Authentication Management Console) non retenu (pas de remontée des déconnexions, soft propriétaire) au profit de RADIUS Steel-Belted (visualisation des logoff, fichier d'accounting au format CSV),
- logiciel d'authentification dépendant du système d'exploitation utilisé (XVSS utilisable seulement pour Win95 et Win98, TELNET dans tous les autres cas…),
- logiciel d'authentification installé sur chaque poste de travail (déploiement, diffusion…),
- plages d'adresses utilisées sur le domaine u-strasbg.fr temporairement en attendant de définir la solution du routage CROUS avec deux fournisseurs d'accès,
- étudiants répartis géographiquement par VLAN en fonction de la CU à laquelle ils ont été affectés,
- gestion des logins et des mots de passe dans un système où le mot de passe est choisi par l'étudiant, créé par le DBA et ne peut pas être modifié par l'étudiant, suivi du journal, sauvegardes (administration d'un nombre important d'utilisateurs mobiles et turn-over rapide),
- serveurs d'informations non accessibles à partir du VLAN par défaut. Les serveurs d'information doivent se trouver dans un VLAN authentifié,
- possibilité de mettre en place ponctuellement des opérations avec un compte utilisateur générique dans un VLAN réservé pour accéder à des services particuliers (exemple : diffusion du logiciel d'authentification, accès à une demande de dossier au CROUS, vérification de résultats d'affectation ou d'examens…),
- mise en place d'un système de logoff automatique au bout de 4 heures pour éviter les oublis de logoff (problématique dans les salles libre-service où l'étudiant est responsable s'il ne se déconnecte pas et libération des adresses IP),
- éviter que les utilisateurs modifient la configuration de leurs postes de travail,
- définition du minimum de protocoles réseaux (TCP/IP, Microsoft DLC 32 bits) pour optimiser la gestion de la CAM (Table d'adressage sur le commutateur).

Les principaux points restant à régler concernent :

- Adressage IP à optimiser en fonction du routage CROUS préconisé par le groupe de travail sur le routage CROUS.
- Simplification et assouplissement des tâches administratives (diffusion du client d'authentification, gestion des logins B mots de passe B fichiers logs - sauvegardes).
- Optimisation de la politique de sécurité pour protéger administratifs et étudiants sans nuire aux performances.
- Offrir un service de messagerie propre aux administratifs du CROUS (remplacer crous.u-strasbg.fr par crous-strasbourg.fr ou strasbourg.crous.fr au niveau des adresses e-mail en fonction du nom de domaine attribué).
- Attribuer des adresses e-mail aux étudiants.
- Gérer une adresse e-mail unique pour tout étudiant strasbourgeois quel que soit son point de connexion (CROUS, Universités, salles libre-service…) en accord avec tous les partenaires concernés pour simplifier la gestion et le suivi des utilisateurs.
- Développer des serveurs d'information et un site Internet pour le CROUS.
- Analyser les performances en fonction de l'évolution du trafic (montée en charge).
- Accélérer le déploiement sur les autres sites. Au 01/10/1999, 3 autres sites du CROUS de STRASBOURG sont en cours de câblage (1 000 prises).
- L'installation des 3 Faisceaux Hertziens du CROUS. Concernant l'ART, le porteur du réseau universitaire existant, Osiris, a fait la demande et l'ensemble des infrastructures est considéré comme un seul réseau indépendant (communauté universitaire = 1 GFU).

■ Conclusion

Les VLANs par authentification représentent exactement une solution adaptée à nos besoins de sécurité et doivent à présent faire leurs preuves à grande échelle pour plusieurs milliers d'utilisateurs. Le CROUS de Strasbourg a pris le risque d'être un pionnier dans la mise en place de cette architecture réseau devant permettre d'identifier les utilisateurs tout en ayant pour objectifs de responsabiliser et d'éviter l'apparition de cybercafés dans les Cités Universitaires !