Migration d'un réseau multi-protocoles routé vers un réseau commuté

■ Pascal GRIS, Pascal.Gris@crc.u-strasbg.fr
Université Louis Pasteur, Strasbourg

Ce document présente, le contexte global, les objectifs et les contraintes du réseau métropolitain strasbourgeois, ainsi que les choix retenus qui auront permis la migration d'un réseau multi-protocoles routé vers un réseau commuté en utilisant, en particulier, les facilités offertes par les technologies de réseaux virtuels.

■ Contexte du projet

Le réseau métropolitain strasbourgeois, commun aux trois universités strasbourgeoises (université Marc Bloch, université Louis Pasteur et université Robert Schuman), aux six écoles d'ingénieurs et aux grands organismes de recherche comme le CNRS et l'INSERM, porte le nom d'Osiris.

Le réseau Osiris s'étend sur 10 campus répartis sur l'ensemble de la communauté urbaine de Strasbourg. Ceux-ci sont raccordés par des fibres optiques, 5 liaisons spécialisées France Télécom et 3 faisceaux hertziens. Les 10 campus représentent 80 bâtiments et l'on dénombre au 1er octobre 1999 plus de 9 500 machines connectées par plus de 100 réseaux Ethernet.

■ Les objectifs du réseau métropolitain strasbourgeois

Le projet comporte plusieurs objectifs :

- La construction d'un réseau fédérateur entre les principaux campus du réseau Osiris dans le but d'offrir à l'ensemble des utilisateurs un accès homogène au réseau en terme de débit et de qualité de service, quelle que soit la localisation géographique de l'utilisateur. Ce réseau fédérateur pourra être étendu localement sur les différents campus dans l'ensemble des bâtiments.
- L'intégration et la connexion des réseaux locaux actuels des différentes entités du réseau Osiris sur ce réseau fédérateur avec le souci de résoudre le problème de la bande passante qui devient un élément critique en certains points du réseau. A cette occasion, certains réseaux locaux sont segmentés ou agrégés par la mise en œuvre de réseaux virtuels.
- La mise en œuvre d'un réseau fédérateur à haut débit dans le but de supporter de nouvelles applications multimédias nécessitant un débit élevé et une qualité de service garantie, comme par exemple la diffusion vidéo de cours pour l'enseignement ; ou encore la fédération de l'ensemble des PABX pour le transport de la voix dont l'intérêt principal serait une économie substantielle des coûts de communication téléphonique intercampus.

■ Les contraintes du projet

Les contraintes globales

- Les partenaires du projet sont multiples : le ministère de l'Enseignement Supérieur, de la Recherche et de la Technologie, le Centre National de la Recherche Scientifique, la Délégation à l'Aménagement du Territoire et à l'Action Régionale, le Conseil Régional, le Conseil Général, la ville de Strasbourg et enfin les partenaires du réseau Osiris qui sont l'université Louis Pasteur, l'université Marc Bloch, l'université Robert Schuman, l'Ecole Nationale Supérieure des Arts et Industries de Strasbourg et l'Institut National de la Santé et de la Recherche Médicale. Un groupe de pilotage du projet est constitué sous l'autorité du Préfet de la Région Alsace.
- Les partenaires financiers du projet favorisent un projet à budget d'investissement plutôt qu'un projet à budget de fonctionnement. Ceci a des implications sur l'architecture du réseau métropolitain. L'aspect redondance de l'architecture du réseau est un élément important du projet. Cette architecture devra

s'appuyer sur des équipements réseaux fiables et redondants et sur une infrastructure de liens réseaux fortement maillés de manière à assurer un fonctionnement du réseau 24h/24h sans intervention.

Les contraintes techniques

- Toutes les entités du réseau Osiris doivent pouvoir accéder au travers de ce réseau fédérateur au réseau national de la recherche RENATER et aux différents services de base du réseau Internet.
- L'aspect multi-protocoles du réseau Osiris doit être conservé en supportant les protocoles IP, IPX, Appletalk ainsi que certains protocoles non routables.
- Tous les aspects de sécurité mis en œuvre sur le réseau Osiris doivent être maintenus.
- Le réseau fédérateur doit être capable de supporter les différentes qualités de services nécessaires aux nouvelles applications comme le transport de la voix et de la vidéo.
- Le réseau haut débit doit s'intégrer au projet haut débit régional ALSATER et au réseau haut débit national RENATER. Il doit également intégrer le projet de raccordement à haut débit par faisceau hertzien au réseau allemand EUCOR. Le respect des standards est donc un impératif pour les équipements qui seront installés sur le réseau haut débit.

Les choix retenus

ATM pour le réseau fédérateur

L'analyse technique des technologies réseaux à haut débit et l'étude du réseau existant nous ont permis de retenir le choix de la technologie ATM pour le déploiement du réseau métropolitain strasbourgeois. ATM répond aux principaux objectifs du projet et possède des atouts majeurs qui sont :

- Une offre haut débit actuelle allant jusqu'à 622 Mbits/s ;
- La gestion et l'optimisation de la bande passante avec la possibilité d'adaptation du débit. Cet aspect prend toute son importance dans un contexte de réseau métropolitain où la bande passante intercampus est chère et limitée ;
- Le support de la qualité de service à travers différentes classes de services ATM ;
- Le support du trafic isochrone (sensible au délai) permettant le développement et l'intégration des applications multimédias comme la voix et la vidéo sur une même architecture de réseau ;
- Une architecture adaptée aux domaines des réseaux locaux (LAN), métropolitains (MAN) et distants (WAN) ;
- La redondance de chemins sur des liens physiques grâce à un routage dynamique PNNI ;
- Le support des réseaux virtuels qui permet une gestion souple et efficace du réseau en s'affranchissant des contraintes de topologie physique du réseau ;
- Une grande perspective d'évolutivité en terme de services et de débit.

LAN Emulation

LAN Emulation (LANE) est une spécification de l'ATM Forum, dont l'objectif est de permettre aux réseaux classiques (Ethernet, Token Ring) de fonctionner avec la technologie ATM. Il s'agit, d'une part, de faire dialoguer des entités Ethernet et Token Ring avec des entités ATM, et d'autre part, d'assurer la migration vers ATM sans remettre en cause les protocoles de niveau supérieur (« Réseau », « Transport ») des réseaux actuels.

Principe

Le dénominateur commun des architectures actuelles de réseaux locaux est la couche MAC au-dessus de la couche physique. Le but est d'offrir, sur une infrastructure ATM, un support transparent pour tous les protocoles de communication actuels, d'où la création d'une couche offrant les mêmes services que la couche MAC traditionnelle. C'est cette couche que l'on appelle LAN Emulation.

Architecture

LAN Emulation définit quatre éléments fonctionnels distincts :

- LAN Emulation Client - LEC

  Le LEC est une entité du réseau. Cette entité peut être une station, un serveur ou tout élément disposant d'une adresse ATM et de n adresse(s) MAC. Dans le cas où n=1, le LEC peut être assimilé à une simple station ATM du réseau. Dans le cas où n>1, le LEC est un "Edge Device" tel qu'un commutateur Ethernet/ATM. Les n adresses MAC étant celles des entités Ethernet dont le commutateur a connaissance. On appelle ces entités "proxy-LEC".

- LAN Emulation Serveur - LES

  Le LES est un service logiciel permettant d'effectuer la résolution d'adresse ATM. Lorsqu'un LEC tente d'initialiser une connexion vers un autre LEC, la communication ne peut s'établir que lorsqu'un circuit virtuel est établi entre ces entités (inhérent au mode de fonctionnement d'ATM). Le LES a pour rôle de trouver l'adresse ATM du LEC demandé, et de la fournir au LEC appelant.

- Broadcast Unknown Server – BUS

  ATM fonctionne sur un principe de mode connecté, c'est-à-dire qu'une connexion virtuelle doit avoir été établie entre les entités avant qu'un échange de données ne puisse commencer. Or les protocoles de réseaux classiques reposent fréquemment sur la diffusion d'informations point à multipoint. Le BUS permet de diffuser ces informations à de multiples destinataires en maintenant des connexions permanentes avec l'ensemble des LEC.

- LAN Emulation Configuration Server - LECS

  Le LECS est un service logiciel permettant aux LEC de connaître l'adresse du LES sur lequel ils doivent se connecter.

Les réseaux virtuels

Généralités

Evolutivité, commutation et sécurité sont les trois critères qui fondent le concept du réseau local virtuel, ou VLAN (Virtual Local Area Network). Un réseau virtuel peut être défini comme un ensemble de ressources interconnectées et regroupées logiquement, indépendamment de leur localisation géographique. Il s'agit de s'affranchir des contraintes physiques du réseau, notamment du câblage, et de permettre la création dynamique de domaines de diffusion (broadcast).

Le principe des réseaux virtuels met en jeu des technologies complexes. On peut aujourd'hui considérer que l'on peut construire des réseaux virtuels selon trois critères : à partir des ports d'interconnexion, à partir des adresses MAC, c'est-à-dire des niveaux 1 et 2 du modèle OSI et, d'une manière dynamique à partir des protocoles ou adresses réseaux du niveau 3 du modèle OSI, ce dernier type de réseau virtuel étant implémenté dans des équipements hybrides se situant entre un routeur et un commutateur.

- **Réseaux** virtuels de niveau 1 : il s'agit d'assigner des ports de connexion physique d'un commutateur ou d'un routeur à des groupes logiques, chaque groupe représentant un réseau local virtuel. Cette approche suppose que le réseau physique soit reconfiguré chaque fois qu'une station change de groupe logique ou de segment. Pour communiquer de segment de réseau à segment, il faut nécessairement passer par un routeur.
- Réseaux virtuels de niveau 2 : l'appartenance à un réseau virtuel s'effectue par identification de l'adresse MAC, qui définit la connexion et l'accès d'une station au réseau local (Ethernet ou Token Ring en général). Un degré dans la mobilité est franchi par rapport au niveau 1, dans la mesure où la station se déplace avec son adresse MAC. Les commutateurs de réseaux locaux agissent au niveau 2. Toutefois, l'administrateur doit assigner manuellement chaque station à chaque groupe logique lors de la création de chaque réseau virtuel. Dans ce cas également, un routeur est nécessaire pour assurer la communication entre réseaux virtuels.
- Réseaux virtuels de niveau 3 : un réseau local de niveau 3 est défini par les champs d'adresses réseaux contenus dans les paquets. Une manière simple de constituer des réseaux virtuels consiste à s'appuyer sur le protocole comme facteur discriminant : IP pour un réseau virtuel, Appletalk pour un autre réseau virtuel, etc. Il est aussi possible d'utiliser l'adresse réseau comme discriminant : typiquement l'adresse IP. Ce mode de définition des réseaux virtuels présente l'avantage d'être paramétré depuis un poste de gestion de réseau.

Choix du constructeur Xylan - Alcatel

Les réseaux virtuels propriétaires

Les règles physiques

- **Règle par port** : elle définit un réseau virtuel en groupant des ports répartis sur un ou plusieurs commutateurs.

Les règles logiques

Une règle logique analyse le contenu et non pas la provenance (port) de la trame. De ce fait, l'avantage principal est que l'affectation d'un poste de travail à un VLAN est indépendante des processus de commutation et du média concerné.

Les commutateurs Xylan - Alcatel possèdent de nombreuses possibilités de réseaux virtuels :

- **Règle par adresse MAC** : l'administrateur dresse une liste d'adresses MAC définissant un réseau virtuel. Cette règle assure un degré de contrôle et de sécurité important.
- **Règle par protocole** : toutes les stations utilisant un même protocole réseau (IP, IPX, Decnet ou Appletalk) sont affectées dynamiquement au même réseau virtuel. Cette règle permet de segmenter le réseau par domaines de broadcast de même nature.
- **Règle par sous-réseau IP ou réseau IPX** : tous les utilisateurs appartenant au même sous-réseau IP ou réseau IPX sont affectés au même réseau virtuel.
- **Règle configurable** : la majorité des besoins des utilisateurs est adressée par les règles prédéfinies. Néanmoins, s'il existe sur le réseau un protocole exotique nécessitant d'être isolé, il est possible de créer sa propre règle. La seule contrainte est de pouvoir identifier un invariant dans chaque trame qui définit ce protocole particulier. Il suffit de définir l'offset, le masque et la valeur pour isoler ce protocole spécifique.
- **Règle complexe** : il est possible de combiner plusieurs types de règles dans la définition d'un seul réseau virtuel (par exemple, adresse MAC ou sous-réseau IP).
- **Réseaux virtuels pour applications multicast** : certaines applications multicast occupent de manière significative la bande passante et perturbent le fonctionnement de stations non concernées. Le principe des réseaux virtuels pour applications multicast est d'envoyer les trames sur les ports où il existe au moins une station participant à cette application, au lieu de les envoyer systématiquement sur tous les ports. Il existe, pour les applications utilisant des multicast IP, un protocole IGMP permettant aux stations d'avertir leur routeur de leurs volontés de participer à un domaine de multicast. L'analyse de ces requêtes IGMP permettra au commutateur de construire dynamiquement la liste des stations appartenant à un réseau virtuel multicast IP donné.
- **Réseaux virtuels par authentification** : le principe est de se connecter premièrement sur le serveur de sécurité et de s'authentifier par l'intermédiaire d'un compte utilisateur et d'un mot de passe. En fonction du compte utilisateur et de la réponse positive du serveur de sécurité la station sera affectée aux réseaux virtuels qui lui sont autorisés.

Les réseaux virtuels normalisés

Le standard IEEE 802.1q défini par le comité IEEE permet de résoudre les problèmes d'interopérabilité des réseaux virtuels entre différents constructeurs. Ce standard utilise des mécanismes de "tagging", pour transporter l'information « réseau virtuel » à travers des médias du type Ethernet.

■ Etude de l'existant

Nous avons effectué une campagne de statistiques sur l'ensemble du réseau. Ces statistiques sont basées sur des données brutes provenant des fichiers d'audit des routeurs CISCO. Une station de travail Unix collecte quotidiennement l'ensemble des fichiers d'audit de tous les routeurs du réseau. Le traitement des données est effectué par des scripts PERL que nous avons développés spécifiquement.

Résultats de cette campagne de mesure :

Trafic entrant/sortant du réseau backbone en Mega-octets par interface de routeur et par protocole

Routeur	Interface	IP	IPX	AT
adit1-cisco	Eth0	165/833	0/0	0/0
api-cisco	Eth1	2665/6158	361/1623	505/1448
api-cisco	Eth0	50381/72756	315/555	816/632
…	…	…	…	…

Grâce à ces informations, nous avons pu estimer le nombre d'équipements du backbone et de définir leurs caractéristiques. Ces résultats nous renseignent également sur la répartition des différents protocoles sur le réseau, ce qui nous a permis de dégager une stratégie pour diminuer la part de routage, afin de favoriser la commutation, dans le but d'augmenter les performances du réseau en terme de délais d'acheminement.

Nombre de machines par protocole, IP, IPX et Appletalk par routeur et par interface

Routeur	Interface	machines IP	machines IPX	machines AT
adit1_cisco	Eth0	26	0	0
api_cisco	Eth0	102	0	7
api_cisco	Eth4	29	0	9
…	…	…	…	…

Matrice de flux intra Osiris pour le protocole IP

Nous obtenons, après traitement des fichiers d'audit, une matrice de flux de dimension 130 par 130, qui correspond aux 130 sous-réseaux IP du réseau *Osiris*. Cette matrice nous renseigne sur les flux IP entre les différents sous-réseaux IP. Ces informations sont particulièrement intéressantes pour la définition et la mise au point des réseaux virtuels. A cette occasion, nous avons pu constater (à quelques exceptions près) qu'il ne se dégageait aucune réelle communauté d'usagers répartis sur l'ensemble du réseau *Osiris*.

■ Les réseaux virtuels mis en œuvre sur *Osiris*

Réseaux virtuels par port

La règle de réseau virtuel par port a été mis en œuvre pour les réseaux administratifs et les réseaux étudiants. Ces deux communautés sont parfaitement identifiées et doivent être isolées pour des raisons de contrôle des communications et de sécurité. Des ports du commutateur sont affectés statiquement à un réseau virtuel « administratif » ou « étudiant ». La communication entre ces communautés est assurée par des routeurs CISCO sur lesquels sont mis en œuvre des filtres de communication (ACL). Le filtrage va progressivement être supprimé des routeurs pour être mise en œuvre sur des équipements spécialisés de type "Fire Wall", ce qui n'entraînera aucune modification de l'architecture.

Réseaux virtuels par sous-réseau IP

La règle de réseau virtuel par sous-réseau IP est la plus utilisée pour fédérer l'ensemble des sous-réseaux existants qui n'ont pas de contraintes particulières en terme de sécurité et de filtrage. Le routage sera distribué sur les différents équipements réseaux (routeurs, commutateurs de backbone ou commutateurs d'extrémité pour réseaux locaux) en fonction des besoins et des ressources disponibles.

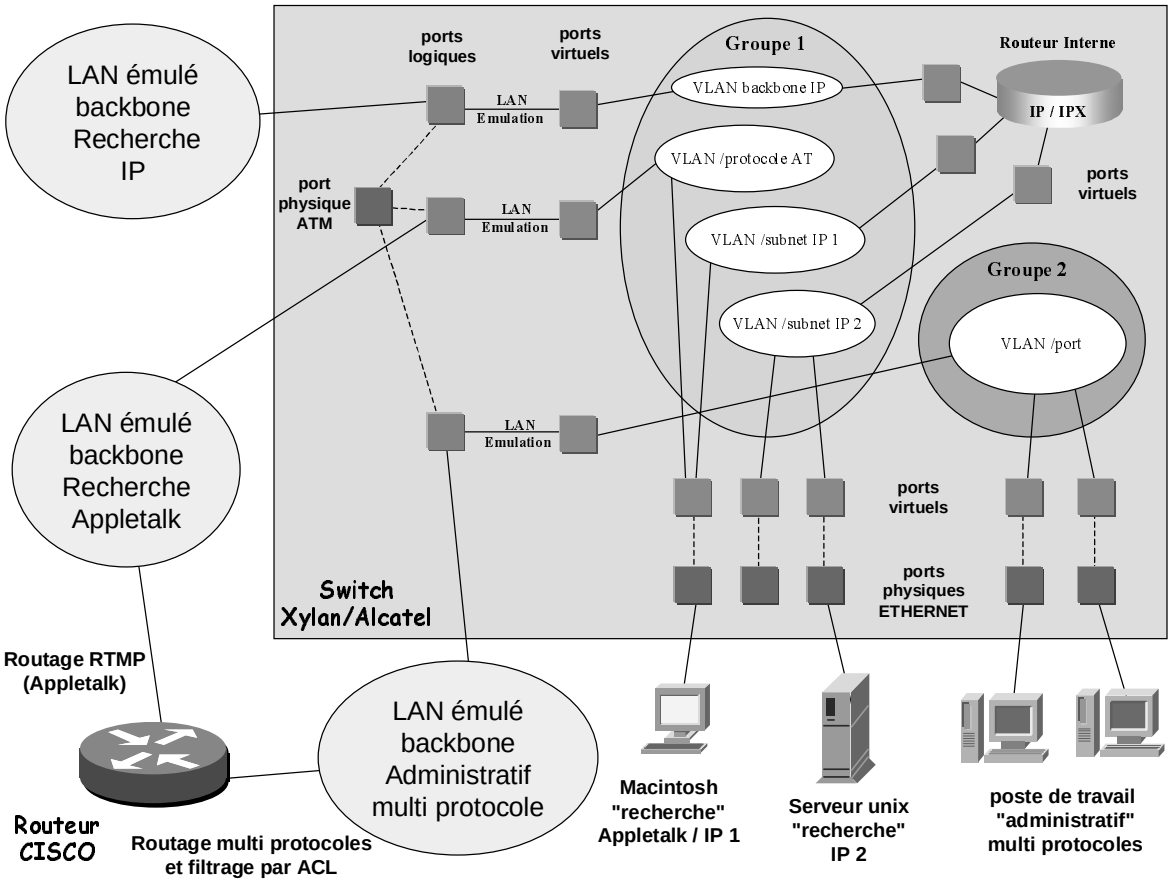
Réseaux virtuels par protocole Appletalk et IPX

Osiris est un réseau multi-protocoles routé. Les protocoles Appletalk et IPX sont routés sur l'ensemble du réseau. Le routage de ces protocoles engendre de nombreux problèmes de dysfonctionnement qui sont liés en particulier à une saturation de la bande passante sur le réseau et à la limite physique du nombre de nœuds pour le protocole Appletalk. Ces dysfonctionnements constatés sont dus à la spécificité de ces deux protocoles qui génèrent un trafic important de type broadcast. Le routage de ces deux protocoles va progressivement être supprimé, néanmoins le protocole Appletalk reste largement utilisé sur de nombreux sites et sera maintenu en utilisant la technique de réseau virtuel par protocole. Les réseaux virtuels par protocole Appletalk et IPX seront routés par les routeurs CISCO.

Réseaux virtuels par authentification

L'ensemble des chambres des cités universitaires du CROUS (Centre Régional des Œuvres Universitaires de Strasbourg), soit plus de 4 500 chambres, va être connecté au réseau *Osiris*. Pour des raisons de sécurité et de contrôle des communications, nous avons mis en œuvre la technique de réseau virtuel par authentification. Ainsi, un étudiant voulant accéder au réseau *Osiris* devra, au préalable, s'authentifier avec un compte utilisateur et un mot de passe. Au démarrage du poste de travail client, ce dernier sera connecté à un réseau virtuel par défaut non routé. Après authentification sur un serveur de sécurité, celui-ci informera le client d'authentification résident sur le commutateur qui aura à sa charge d'affecter le port à un réseau virtuel authentifié en fonction du profil de l'utilisateur. Cette technique sera également utilisée dans les salles de ressources étudiant en libre service.

Architecture de réseaux virtuels sur les commutateurs



■ Conclusion

Difficultés rencontrées

Compte tenu des contraintes de disponibilité du réseau qui deviennent de plus en plus fortes, la migration d'un réseau routé vers un réseau commuté engendre de nombreuses perturbations dans l'exploitation du réseau qui nécessitent une bonne organisation ainsi qu'une planification rigoureuse des interventions.

L'introduction de la commutation et des réseaux virtuels dans les réseaux locaux constitue souvent un prétexte pour les utilisateurs pour dénoncer des dysfonctionnements déjà existants sur les différents sous-réseaux. Il s'agit alors de résoudre l'ensemble de ces dysfonctionnements en collaboration avec les responsables informatiques des différents sites.

Dans le but d'augmenter les performances dans les réseaux locaux, nous devons diminuer globalement le routage et introduire ou augmenter la commutation. Pour atteindre cet objectif nous sommes contraints de réviser globalement le plan d'adressage IP du réseau. En effet, certains sous-réseaux doivent être agrégés et d'autres segmentés pour bénéficier au maximum de la commutation. Ceci implique une re-numérotation IP partielle voire totale pour certains sous-réseaux. La re-numérotation constitue bien souvent une contrainte forte pour les

utilisateurs et un casse tête complexe pour trouver des plages d'adresses IP disponibles et contiguës dans l'espace d'adressage du réseau existant.

La définition et la stratégie de réseau virtuel à déployer sur les différents sites nécessitent une étude approfondie au cas par cas.

La couche réseau LANE introduit un niveau de complexité supplémentaire tant au niveau de la configuration du réseau qu'au niveau diagnostique de panne et de l'exploitation du réseau. Ce point est particulièrement vrai dans un contexte de redondance des services LECS, LES et BUS.

Bilan

La migration vers un réseau commuté nous a permis de résoudre le problème de la saturation de la bande passante, d'augmenter le niveau de sécurité dans les réseaux locaux et de s'affranchir des contraintes géographiques.

Le backbone ATM offre un réseau de transport à haut débit supportant les applications sensibles aux délais d'acheminement comme la voix et la vidéo et fiable, grâce aux liens redondants et à un protocole de routage (PNNI) performant, capable de prendre en considération les paramètres de qualité de service.

L'objectif d'offrir un accès homogène au réseau en terme de débit et de qualité de service quelle que soit la localisation de l'utilisateur a été atteint.

Grâce aux technologies des réseaux virtuels, nous sommes en mesure de satisfaire des demandes particulières émanant des utilisateurs en terme de réseau.

La commutation offre une grande souplesse dans la configuration du réseau. En effet, l'interconnexion des différentes ressources du réseau est entièrement logique. Elle est réalisée par configuration logiciel des équipements connectés au backbone ATM.