Déploiement de VLAN 802.1Q/ISL dans un environnement hétérogène

Christophe WOLFHUGEL, wolf@oleane.net
Direction technique, Responsable Serveurs, France Telecom Oléane

Les VLAN (Virtual LAN ou réseaux locaux virtuels) sont apparus voilà quelques années pour une raison que j'ai encore à ce jour du mal à appréhender. Ces VLAN dont on parle tant ne seraient-ils tout simplement qu'une invention du marketing destinée aux entreprises dont le personnel change sans arrêt de bureau (on pourrait qualifier ces entreprises de « modernes ») ou bien s'agit-il réellement d'une technologie utile et qui tombe à pic ? Après quelques informations sur la technologie utilisée et les standards en la matière nous aborderons des points plus pragmatiques basés sur deux expériences de terrain :

- *le déploiement quasi contraint des VLAN sur un réseau de campus (plus de 2 000 prises) d'un centre de recherche ;*
- *la mise en place voulue des VLAN sur les réseaux « serveurs » chez Oléane, mise en place démarrée début 1999 et maintenant quasi finalisée.*

Ces deux expériences de terrain devraient permettre au lecteur d'appréhender un peu mieux ces nouvelles technologies et le guider dans ses choix futurs.

Introduction aux VLAN

L'idée de base des VLAN est de découper un seul réseau local (c'est à dire un ensemble cohérent d'infrastructures de niveau 2) en des réseaux logiques totalement disjoints : c'est comme si on avait plusieurs réseaux physiques totalement disjoints, un par VLAN. Ces réseaux partagent une même infrastructure, par exemple une épine dorsale d'un réseau de campus en Ethernet 100 Mbits/s et un ensemble de commutateurs. Nous nous situons bien ici au niveau de la couche liaison du modèle ISO, c'est à dire au niveau des trames (ethernet, token-ring, FDDI pour citer quelques technologies). Pour utiliser des termes plus proches de la technologie ethernet on peut dire que chaque VLAN correspond à un domaine de diffusion (et de *multicast*) indépendant des autres.

Les routeurs sont à considérer comme des équipements standards (au même titre qu'un serveur ou qu'une station de travail) et ils peuvent être branchés derrière un port d'un commutateur, et donc participer au VLAN, et à l'interconnexion de VLAN si tel est le souhait de l'administrateur du réseau.

Les équipements modernes permettent à l'administrateur du réseau de construire des VLAN selon des critères techniques différents. Nous allons expliquer en quelques paragraphes à quoi correspondent les trois types de VLAN que l'on rencontre le plus fréquemment.

Le « VLAN par port »

Chaque port physique du commutateur est configuré par l'administrateur du réseau pour appartenir à un (plusieurs ?) VLAN, et toute machine (ou ensemble de machines) qui se trouve branchée sur ce port fera partie de ce VLAN. C'est le mode de fonctionnement le plus simple et le plus déterministe, c'est à dire celui où potentiellement les défauts de logiciel sont le moins probable.

Ce type de réseaux virtuels n'a rien de bien innovant. Au bon vieux temps, lorsque les équipements réseau étaient simples et fiables, on faisait déjà des VLAN par port tout simplement en construisant des réseaux physiquement séparés, chacun ayant son câblage et ses propres équipements actifs. C'est bien le branchement physique sur un port d'un concentrateur plutôt qu'un port d'un autre concentrateur qui déterminait l'appartenance à un réseau.

On peut se risquer à comparer les VLAN par port à la construction de réseaux séparés :

- l'usage de VLAN doit permettre de mutualiser les équipements actifs ainsi qu'une partie de câblage informatique (notamment les épines dorsales), mais d'un autre côté cela impose l'usage de commutateurs ; on peut

dire à juste titre que de moins en moins de gens utilisent des concentrateurs pour le déploiement de leurs réseaux ;

- sur un réseau d'une certaine taille, comme un réseau de campus, il faudra construire autant d'épines dorsales qu'il y a de réseaux à construite, cela peut coûter fort cher non seulement en câblage, mais aussi en équipement actif car les équipements de collecte adaptés à la fibre optique sont dans une gamme de prix bien plus élevée que les équipements de collecte de réseaux en cuivre ;
- lorsqu'une prise informatique doit être affectée à un autre réseau, une intervention est nécessaire sur site, dans la baie de concentration, afin de brasser la prise concernée dans le nouveau réseau et sur l'équipement actif adéquat.

C'est donc probablement plus un critère de paranoïa qu'un critère technique qui l'emportera sur la décision finale lorsque l'une ou l'autre des solutions est envisagée.

Les deux autres catégories de VLAN présentées n'existaient pas par le passé car la séparation physique des réseaux ne permet pas d'obtenir le résultat escompté : l'affectation dynamique d'une machine dans un ou plusieurs réseaux virtuels.

Le « VLAN par protocole »

Le critère d'appartenance à un VLAN n'est plus lié au port sur lequel la machine est connectée, mais à un ou plusieurs critères liés à la nature de trafic généré par cette machine. On va par exemple définir l'appartenance à un VLAN à un protocole particulier : un VLAN pour IP, un autre VLAN pour le trafic Appletalk. Si l'intérêt du VLAN par protocole n'est pas évident lorsque son réseau à été bien conçu dès le départ et qu'il n'utilise pas des protocoles bizarres, on peut imaginer quelques situations dans lesquelles le VLAN par protocole peut aider à faire progresser le fonctionnement du réseau.

Imaginons un réseau de campus qui est fortement maillé et routé (plutôt que commuté). Ce réseau utilise les protocoles IP et Appletalk. Pour eux tout se passe bien, parce que par conception ces deux protocoles sont adaptés aux réseaux routés. Ajoutons maintenant sur ce réseau d'entreprise un protocole réseau de mauvaise qualité qui n'a pas été conçu pour être routé (le lecteur mettra ici le nom du protocole non routé qu'il déteste le plus). Que peut-on faire ? Construire un deuxième réseau physique pour ce protocole ? Trop coûteux. C'est ici que le VLAN par protocole a son intérêt : l'administrateur du réseau va définir un VLAN qui recueillera le trafic correspondant au protocole choisi. Le commutateur va analyser et trier chaque trame qu'il reçoit afin de la placer dans le VLAN qui lui correspond.

La gestion et l'administration de ce type de VLAN peuvent être compliquées et ne répondent pas aux mêmes besoins de sécurité que le VLAN par port (en fait je dirais que cela ne répond pas vraiment à des besoins de sécurité).

Le « VLAN par adresse »

Le critère d'appartenance à un VLAN n'est plus lié à un protocole où à une localisation sur le réseau, mais à un identifiant de la machine et plus particulièrement de sa carte réseau. Avec de l'ethernet c'est l'adresse MAC de la carte qui peut être l'identifiant, et c'est justement ce que de nombreux produits du marché permettent de faire.

L'intérêt de cette configuration est la banalisation de chaque prise informatique du réseau. Aussitôt un poste de travail branché sur un port d'un commutateur, celui-ci pourra l'affecter au VLAN adéquat. On peut aussi imaginer que toute adresse MAC inconnue se voit refuser l'accès au réseau ou se retrouve dans un VLAN « visiteurs ».

Cette méthode de travail a cependant quelques inconvénients. Lorsqu'un utilisateur change la carte ethernet de son ordinateur, il faut une intervention de l'administrateur du réseau afin de réactualiser la configuration des commutateurs. Chaque nouvelle machine doit également être déclarée afin d'être configurée. Toutes les entreprises ne sont pas prêtes à accepter le surcoût lié à une telle architecture.

Dans un environnement hétérogène

Si les produits du marché s'en sortent pas trop mal dans un environnement hétérogène, gérer des VLAN par protocole ou par adresse est bien plus difficile dès que l'on souhaite utiliser des produits provenant de différents constructeurs. Le concepteur du réseau devra tester et valider longuement ses choix afin de limiter les risques et les mauvaises surprises.

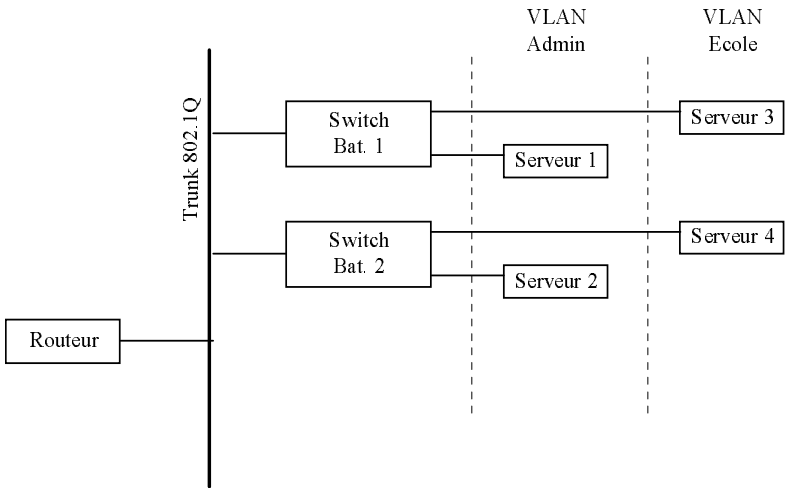
Comment les commutateurs gèrent-ils les VLAN ?

Les VLAN existent sur les commutateurs depuis fort longtemps, notamment les VLAN par port. Tant que le réseau n'est constitué que d'un seul commutateur tout ceci est fort simple. Le fonctionnement des VLAN se complique lorsqu'il s'agit de faire discuter plusieurs commutateurs et notamment lorsque ceux-ci viennent de fabricants

concurrents. Afin de transporter le trafic des VLAN entre différents commutateurs il est nécessaire de trouver un protocole de transport entre les équipements qui permettent de conserver les informations d'appartenance aux VLAN. Le terme anglais *trunk* est utilisé pour caractériser les liaisons entre commutateurs et permettant le transport des VLAN. Il existe de nombreux protocoles propriétaires (par exemple ISL chez Cisco, 3Com) depuis déjà quelques temps et un protocole standardisé : 802.1Q. Ce dernier protocole n'est disponible et opérationnel sur les produits que depuis quelques mois, même si les brochures du marketing vendaient cette fonction bien avant qu'elle n'existe et surtout qu'elle fonctionne correctement.

On peut dire, très sommairement que 802.1Q est un protocole de multiplexage (sur ethernet c'est un type particulier de trames) qui permet le transport des trames des différents VLAN du réseau. C'est l'administrateur du réseau qui décide si un port est destiné à accueillir des machines ou bien si c'est un *trunk* destiné à l'interconnexion des différentes parties d'un VLAN.

Terminons cette partie par un petit schéma qui présente un réseau très simple qui fait utilisation de VLAN :



Nous avons dans cet exemple un petit réseau qui s'étend sur deux bâtiments. Chaque bâtiment dispose d'une baie de concentration qui est équipée d'un commutateur. Un routeur assure d'une part le routage du trafic entre les réseaux Administration et Ecole (selon autorisations définies par la politique de sécurité appliquée au routeur), et on peut d'autre part imaginer qu'il assure également la connexion du réseau à l'Internet. Dans cet exemple le routeur est connecté directement au *trunk* car il sait utiliser le protocole 802.1Q, et on peut ainsi configurer plusieurs interfaces logiques au-dessus d'une interface physique. Si le routeur ne savait pas faire de VLAN il faudrait 2 pattes ethernet et les brancher sur 2 ports ethernet d'un des commutateurs, chacun de ces ports appartenant à l'un des VLAN.

802.1Q & ISL en quelques lignes

Les protocoles 802.1Q et ISL sont deux protocoles permettant de transporter des VLAN sur des infrastructures partagées. Le premier est un protocole normalisé, disponible depuis peu : annoncé par les vendeurs voilà plus d'un an, figurant dans les documentations des produits depuis à peu près la même période, mais dans la pratique cela fait tout au plus une petite année que 802.1Q est disponible et utilisable sur les produits. Le protocole ISL est l'un des protocoles propriétaires qui existaient (et existent toujours) avant que les constructeurs ne se mettent d'accord et commencent à adopter 802.1Q.

Aujourd'hui les produits bas de gamme en sont bien souvent restés au seul protocole propriétaire de leur constructeur alors que les commutateurs haut de gamme permettent de choisir entre 802.1Q et le protocole propriétaire, et en général d'effectuer la conversion entre l'un et l'autre. Certains (Lucent, gamme Prominet entre autres) ont fait le choix de proposer outre 802.1Q un nombre plus important de protocoles propriétaires (Cisco, 3Com) et permettent de convertir les trames d'un format à l'autre. Il est évident que ces produits visent un marché de fédérateur d'un existant hétérogène ne sachant pas faire du 802.1Q.

Il existe des protocoles de transport de VLAN sur différents supports physiques (Ethernet, ATM par exemple). Lors de mon étude et de mes expériences je me suis volontairement limité à la technologie ethernet. Je ne décrirais pas l'encapsulation ISL de Cisco, et me contenterais de faire une très brève présentation de l'encapsulation 802.1Q.

Grossièrement, les trames 802.1Q sont des trames ethernet de type 0x8100. L'entête 802.1Q contient divers identifiants, dont le numéro du VLAN sur 12 bits (ce qui permet un maximum de 4096 VLAN, même si beaucoup

de produits ne savent pas aller au-delà de 1024). On trouve également 3 bits donnant à la trame l'un des 8 niveaux de priorité disponible. S'en suivent d'autres informations, et bien sûr la trame originale. Le travail des équipements consiste donc entre autres à assurer l'encapsulation et l'opération inverse des trames circulant sur un VLAN avant de pouvoir les véhiculer sur le *trunk*. Le lecteur souhaitant se pencher dans les détails de 802.1Q pourra consulter la documentation sur ce standard sur le site Web de l'IEEE (http://grouper.ieee.org/groups/802/1/vlan.html).

■ Rappels sur la commutation

Les commutateurs ne sont rien d'autre que des ponts filtrants, certes équipés de fonctions plus nombreuses et de performances qui n'ont rien de comparable aux bons vieux ponts que nous utilisions voilà une petite dizaine d'années. Les commutateurs de niveau 3 ou 4 ne sont autre que des inventions du marketing pour remplacer respectivement les mots routeurs et passerelles et rajouter des nouvelles fonctions applicatives (et non pas de commutation). On nous justifie l'usage de ce nouveau nom en raison des performances supposées meilleures de ces nouveaux produits. Nous ne nous intéressons qu'aux vrais commutateurs dans cet exposé.

Le travail de base d'un commutateur est de gérer des tables d'adressage : savoir sur quel port se trouve une adresse MAC afin d'éviter de diffuser le trafic inutile sur les segments des autres machines. Le nombre d'adresses MAC par port et pour l'ensemble du commutateur font partie des caractéristiques du produit auxquelles l'administrateur du réseau doit s'intéresser avant tout achat.

Lorsque le réseau n'est pas bouclé (c'est à dire que pour aller d'un point à un autre du réseau il y a un et un seul chemin), cette gestion de tables d'adresses MAC est suffisante. Lorsqu'il peut y avoir plusieurs chemins pour aller d'un point à un autre du réseau il est nécessaire d'utiliser en plus des arbres de recouvrement (*spanning-tree* en anglais). L'arbre de recouvrement a pour but d'éviter les cycles (et donc des trames qui se baladent) et doit être recalculé à chaque modification de la topologie d'un réseau. Un effet visible de l'utilisation de cette technologie est les blocages de quelques secondes voire dizaines de secondes que les utilisateurs peuvent observer lorsqu'une machine est insérée dans un réseau sur lequel il y a un arbre de recouvrement (débranchez une machine d'un commutateur, rebranchez-la et observez : si votre réseau se bloque quelques temps c'est peut-être que votre commutateur recalcule son arbre de recouvrement). On ne saurait donc que conseiller à l'administrateur du réseau de désactiver totalement l'utilisation des arbres de recouvrement s'il est sûr que son réseau ne permet pas l'établissement de boucles.

Dès lors que l'on utilise des VLAN il n'y a plus une table d'adresses MAC et un arbre de recouvrement, mais il y en a autant que de VLAN gérés dans le système. Les équipements participant au réseau à base de VLAN doivent donc être en mesure de gérer cette multitude de tables et d'arbres de recouvrement.

Les autres fonctions des commutateurs modernes telles la limitation de la quantité de paquets en diffusion ou la gestion du flux sont certes utiles, mais n'ont aucun intérêt dans le sujet qui nous intéresse.

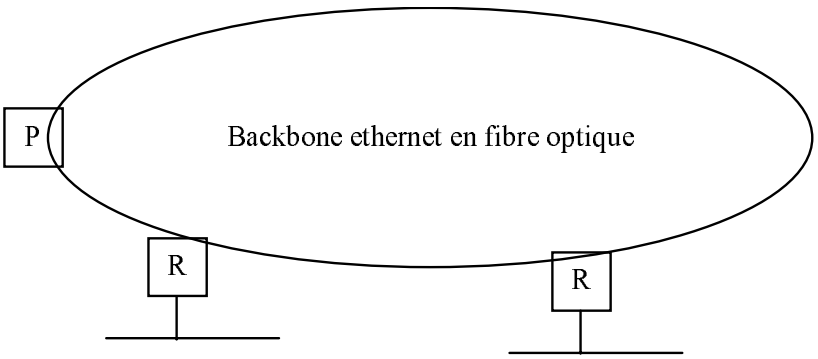
Les ports de type *trunk* sont-ils des ports comme les autres ? La littérature des fabricants est moins bavarde sur ce point, mais il semble que du point de vue des tables d'adresses le comportement est similaire aux autres ports : seul le trafic utile (diffusion, multicast ou trame à destination d'une machine qui se trouve de l'autre côté) emprunte ces liaisons. Si deux machines appartenant au même VLAN et étant sur le même commutateur s'échangent des trames, celles-ci ne passeront pas par les *trunk*. Les paquets diffusés (broadcast) ou multicast vont par contre emprunter tous les liens *trunk* sur lesquels leur VLAN d'appartenance est diffusé. Avec certains protocoles réseau cela peut représenter une quantité non négligeable de trafic.

L'administrateur du réseau dispose également de quelques éléments de contrôle. Il peut par exemple limiter certains *trunks* à certains VLAN et donc interdire le transport de trafic, même diffusé sur ces segments pour certains VLAN. D'autres équipements disposent d'une fonction permettant aux commutateurs de s'échanger la liste des VLAN qu'ils transportent ou pour lesquels il assurent du transit et de les éliminer automatiquement du transit. Il semble que ces extensions soient principalement propriétaires : leur fonctionnement doit être testé lorsque des équipements d'origine différente sont utilisés sur un réseau.

■ Cas numéro 1 : déploiement de VLAN ISL sur un réseau de campus

Certains réseaux ont été conçus au début des années 90 selon une architecture dont la robustesse et la simplicité sont exemplaires. Nous sommes ici sur un réseau de campus d'un centre de recherches qui est constitué d'une épine dorsale en fibre optique qui assure la diffusion dans les différents bâtiments du campus. Cette fibre optique forme un anneau qui est ouvert à l'une de ses extrémités par un pont filtrant. En utilisant ce pont et la technologie ethernet, on est ainsi résistant à une coupure dans cette boucle optique. La diffusion vers les réseaux capillaires se fait par l'utilisation de produits très simples : des routeurs deux ethernet de type Cisco IGS. Un port ethernet est connecté à l'épine dorsale, l'autre vers le concentrateur qui assure la diffusion capillaire vers les

utilisateurs. L'utilisation de matériel en châssis (en l'occurrence des châssis Chipcom, une excellente gamme avant que la société Chipcom ne soit rachetée par 3Com) avait l'avantage de réduire significativement la quantité de fils qui traînent et les problèmes de connectique. Le produit coûte plus cher à l'achat, mais l'absence de tous ces câbles supplémentaires contribue significativement à la qualité globale du réseau en réduisant le nombre de sources d'incidents. Le schéma ci-dessous présente sommairement ce réseau très fortement maillé (protocoles IP et Ethertalk principalement) :



Réseaux ethernet capillaires de distribution dans les bâtiments

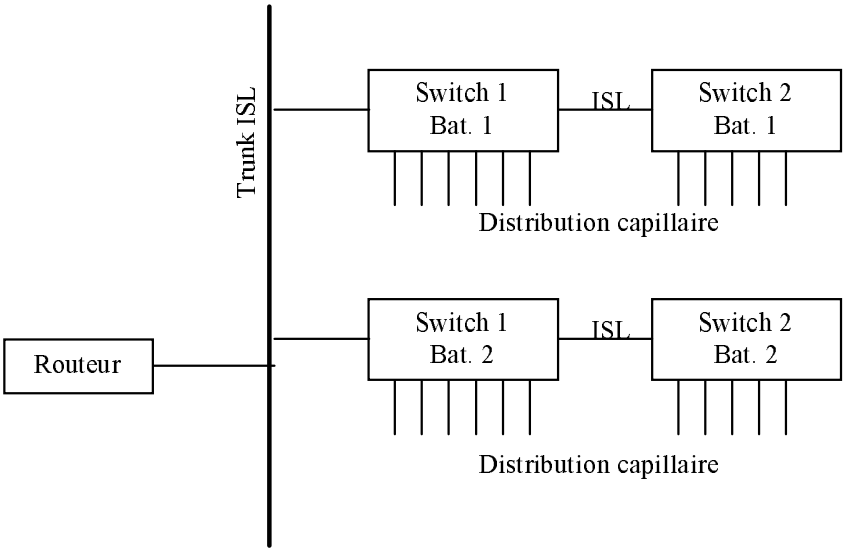
Ce réseau d'entreprise d'environ 2 000 prises et dont l'épine dorsale est constituée d'une cinquantaine de répartiteurs et d'autant de routeurs double ethernet aurait très bien pu continuer d'évoluer encore de longues années, si les génies du marketing n'avaient pas décidé d'arrêter la fabrication et la vente des produits utiles pour les remplacer par des produits modernes, à très haut débit et qui coûtent cher, dont le client n'avait que faire. Il fallait donc trouver un moyen de continuer à croître alors que les routeurs double ethernet pour châssis Chipcom n'étaient plus disponibles. Quelques solutions de remplacement ont été étudiées :

- Les solutions à base de routeur non Cisco ont eu du mal à être appréciées à leur juste valeur : de façon générale on leur reprochait d'une part d'être difficiles à appréhender en raison d'interfaces utilisateur textuelles fort différentes, et d'autre part pour certains produits de n'avoir qu'une interface graphique qui ne faciliterait pas la gestion d'un parc de routeurs.
- Les petits routeurs Cisco avec deux cartes ethernet n'existaient pas encore à l'époque, et il se posait clairement le problème de la conversion 10 base T vers 10 base FB qui était le standard utilisé sur la dorsale en fibre optique. De plus ces produits n'étaient pas à vraiment rackables.
- Les routeurs de la série Cisco 2500 étaient rackables et proposaient une configuration avec 2 cartes ethernet, mais pourquoi alors payer deux ports série dont on a que faire ? De plus sur ce modèle « rackable » la connectique se situe en face arrière ce qui n'est pas bien malin pour un produit destiné à être mis dans des gaines techniques.
- Les routeurs de la série 4000 permettaient de créer 2 réseaux, voire plus, mais outre leur coût ils avaient le même inconvénient que le 2500 : la connectique est en face arrière. Ce routeur est également plus volumineux que son petit frère, et les gaines techniques ne sont que rarement très vastes.

Clairement, aucun produit simple et économique ne répondait au besoin et il fallait se rendre à l'évidence : les fabricants avaient prématurément mis fin au marché des réseaux locaux routés, afin de contraindre leurs clients à remplacer le plus d'équipements possibles.

L'évolution forcée vers des plus hauts débits était donc nécessaire, et le choix d'une topologie robuste en double anneau FDDI était tentant. Tentant mais trop coûteux, puisque là encore le marché à tué FDDI au profit de l'ethernet 100 Mbits/s et maintenant du Gigabit ethernet (ceux qui préfèrent des choses coûteuses et peu fiables pourront se tourner vers ATM).

L'objectif était d'avoir un coût le plus faible possible par patte ethernet routée, car il était hors de question de casser le réseau en le mettant à plat (comme c'est hélas de plus en plus souvent le cas). C'est dans cette configuration que les VLAN avaient un intérêt : un routeur haut de gamme capable de gérer un *trunk* de VLAN pourrait faire l'affaire, l'objectif étant de ramener le routage d'un nombre important de VLAN sur chaque routeur et de limiter le nombre de points de routage dans le campus. On se retrouverait ainsi avec une nouvelle architecture, bien moins robuste, du réseau de campus que l'on peut schématiser ainsi :



L'économie de routeurs et visible. La contrepartie est un trafic bien plus important sur le segment fédérateur en ethernet 100 Mbits/s. En effet lorsqu'une station d'un réseau du Switch 2, bâtiment 1 veut discuter (en IP par exemple) à une machine d'un autre sous-réseau qui se trouve également sur ce commutateur, le trame ethernet va être envoyée au routeur qui va la renvoyer là d'où elle vient. Certains fabricants disposent d'extensions fort coûteuses qui permettent au routeur et au commutateur de s'échanger des informations de ce type afin que seul le premier paquet fasse le grand chemin. Mais vu la fragilité rencontrée avec une topologie aussi simple, je ne suis pas pressé d'essayer ces produits « encore meilleurs », pour reprendre les paroles des vendeurs.

Les équipements choisis

Le réseau qui vous est ici présenté tourne aujourd'hui dans un environnement homogène. Les commutateurs et routeurs sont tous d'origine Cisco. Le routeur n'est pas un boîtier séparé, mais c'est la carte de routage RSM pour commutateur Catalyst 5000 qui a été choisie : elle permet de bénéficier d'un débit plus important puisque directement connectée au fond de panier de l'un des commutateurs du cœur du réseau. Les gros commutateurs installés sont des Catalyst 5000 et les plus petits sont des modèles de type Catalyst 1924 équipés du logiciel Enterprise qui permet de gérer les VLAN. Le protocole de communication ISL, propriétaire Cisco, a été choisi, non pas par conviction, mais tout simplement parce que la plupart des produits ne connaissaient pas ou mal 802.1Q.

Les problèmes rencontrés

Ce déploiement simple sur le papier a été l'occasion de nombreuses surprises, qui confirment la baisse générale de la qualité des équipements actifs des réseaux. La configuration des VLAN est assez simple et source de peu d'erreurs. La franche rigolade commence lorsqu'on arrive dans des défauts du logiciel : l'IOS de Cisco est devenu tellement lourd que trouver une version stable et adaptée relève de l'exploit. On peut facilement se retrouver avec deux équipements qui vont faire n'importe quoi parce qu'ils ne tournent pas avec la même version du logiciel. Une petite erreur et c'est tout le réseau qui est en panne. D'autres défauts très graves ont également retardé le déploiement du réseau pendant plusieurs mois : en raison d'un défaut de fabrication (ou de conception ?) les récentes cartes fibres optiques du Catalyst 5000 refusaient de causer ISL avec les Catalyst 1924. Il aura fallu plusieurs semaines au vendeur pour prêter des cartes d'un ancien modèle, et plusieurs mois au fabricant pour corriger le défaut et livrer des nouvelles cartes. A chaque fois changer le matériel signifie des interruptions de service pour l'utilisateur et une baisse de disponibilité du réseau.

Autre plaisanterie similaire : la mise en cascade de Catalyst 1924 ne peut se faire qu'à un très faible niveau de profondeur. Il est hors de question de chaîner 4 ou 5 commutateurs les uns derrière les autres sans avoir de mauvaises surprises. Là aussi cela oblige souvent l'utilisateur à se diriger vers des produits haut de gamme et coûteux dont il n'a pas forcément besoin.

Conclusion

La mise en service quasi forcée des VLAN sur ce réseau a permis d'une part de continuer l'extension de celui-ci et d'autre part le passage vers des plus hauts débits. Ce dernier point n'était cependant pas un élément moteur du choix. L'architecture a été significativement compliquée et fragilisée et, parce que les équipements actuels sont plus adaptés aux réseaux en étoile qu'en anneau il aura été nécessaire de faire poser des fibres optiques supplémentaires. La fragilité bien réelle de ces nouvelles technologies ne peut qu'inciter le responsable du réseau à une très grande prudence : l'époque où les équipements réseau étaient fiables et robustes est belle et bien passée.

■ Cas numéro 2 : déploiement de VLAN 802.1Q et ISL sur un réseau d'un centre serveur

Tout prestataire qui fournit des services de connexion à l'Internet doit disposer d'un certain nombre de serveurs afin de rendre à ses clients au moins les services de base tels l'hébergement de boîtes aux lettres, la résolution de noms et l'accès aux news, pour ne prendre que quelques exemples. Les centres serveurs des prestataires, lorsqu'il y en a plusieurs comme cela est notre cas ne sont en fait rien d'autre que des réseaux locaux qui sont connectés de diverses manières à l'Internet. Nous ne nous intéresserons pas à la façon dont ceux-ci sont connectés à l'Internet, mais plus aux choix qui ont été fait lors de la mise en service des salles machine, des équipements actifs et des serveurs. Lors de la conception du réseau différentes philosophies s'opposent : le tout à plat et utilisation au maximum des avantages de la commutation, ou bien la création de nombreux réseaux routés de petite taille correspondant à des grappes de serveurs. Si la première solution a l'avantage de la simplicité conceptuelle elle peut réserver des surprises en matière de sécurité. La rédaction de filtres adéquats peut s'avérer compliquée et on arrive rapidement à des listes de contrôle d'accès de plusieurs centaines de lignes. La seconde solution est séduisante mais afin de pouvoir être envisagée et acceptée, il est nécessaire qu'elle soit d'un coût raisonnable. L'utilisation de VLAN est un moyen d'arriver à un coût quasi identique qu'il y ait un sous-réseau IP sur le centre serveur ou bien qu'il y en ait vingt : avec les équipements de commutation et de routage haut de gamme les extensions VLAN sont comprises dans le prix, on les paye que l'on utilise ces fonctions ou pas. Alors autant les utiliser.

Un réseau de serveurs d'un prestataire de services Internet (et même d'un hébergeur) a des caractéristiques que l'on retrouve presque partout en matière de trafic : les machines communiquent peu entre elles et beaucoup avec le monde extérieur, c'est à dire les clients et les visiteurs qui utilisent les services tels la consultation de serveurs Web. Dans le cas numéro 1 présenté précédemment, on notait qu'il y avait un trafic entre réseaux voisins, et que donc dans le choix d'architecture retenu un paquet IP pouvait circuler deux fois sur le même *trunk* et contribuer ainsi à sa saturation. Dans le cas du fournisseur de services Internet le trafic étant presque toujours dirigé vers l'extérieur, cette contrainte est moins forte : la plupart des paquets sont échangés entre les serveurs et le ou les routeurs, et le trafic résiduel entre machines est très faible. Il s'agit réellement d'un trafic en étoile, et c'est aux routeurs d'avoir les capacités adéquates pour assurer en même temps le travail de gestion d'un *trunk* de VLAN, le routage des paquets IP et un minimum de sécurité par l'utilisation de filtres. Un autre avantage de la segmentation en petits réseaux est également la facilité offerte pour déménager par morceaux des parties du

centre serveur : on peut faire simplement le déménagement réseau par réseau jusqu'à par exemple un déménagement complet.

Dans les salles serveurs, qu'elles accueillent du matériel appartenant aux clients ou bien au prestataire, plus qu'ailleurs banaliser chaque prise informatique est un impératif : il y a en effet des mouvements réguliers de machines et une prise doit pouvoir être affectée rapidement à un réseau particulier. Il faut aussi être en mesure de créer un nouveau réseau IP et de préférence sans avoir à se déplacer pour effectuer des manipulations de câbles.

La technologie choisie dans les salles machine et d'hébergement est un câblage classique en cuivre permettant de délivrer sur chaque prise de l'ethernet 10 Mbits/s ou de l'ethernet 100 Mbits/s. Le câblage est classique et deux baies de distribution assurent chacune la distribution des prises vers les équipements terminaux. Chaque baie de distribution est à côté d'une baie d'équipements actifs, les deux ensembles étant séparés à peine d'une vingtaine de mètres et de quelques murs.

Les équipements choisis

Le trafic est relativement modeste au départ de chaque point d'accès au réseau (tout au plus quelques Mbits/s) et est plutôt important sur les points de sortie. Le routage est assuré par des routeurs Cisco 7200 équipés de deux cartes Ethernet 100 Mbits/s : l'une vers le backbone, l'autre utilise un *trunk* 802.1Q et va vers l'un des commutateurs *backbone* issu de la gamme Prominet de Lucent. Les autres ports du commutateur sont affectés par l'administrateur du réseau à des VLAN particuliers qui correspondent à des réseaux définis. D'autres commutateurs de plus faible capacité sont connectés aux Lucent également en *trunk* mais cette fois-ci avec le protocole ISL.

La liaison routeur Cisco vers commutateur Lucent aurait au choix pu également être en ISL, mais le protocole ouvert étant disponible sur les deux équipements, c'est celui-ci que nous avons préféré choisir. La configuration côté routeur est élémentaire : chaque VLAN se présente comme une sous-interface sur le routeur. Voici un petit exemple de configuration d'un *trunk* 802.1Q sur un routeur Cisco, avec deux VLAN :

```
interface FastEthernet0/0
 description Trunk 802.1Q
 no ip address
!
interface FastEthernet0/0.1
 description VLAN 802.1Q numéro 1
 encapsulation dot1Q 1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/0.2
 description VLAN 802.1Q numéro 2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
```

Le lecteur peut constater que la configuration est un jeu d'enfant sur le routeur et qu'il n'est pas nécessaire de consacrer beaucoup d'énergie à la création de nouveaux VLAN. Un problème particulier a cependant été rencontré : dans certaines circonstances bien précises que nous n'avons pas pris le soin de préciser totalement (car cela concernant surtout une liaison ISL entre un routeur Cisco et un commutateur Catalyst) il fallait activer le protocole CDP de Cisco afin de faire fonctionner les VLAN. Problème que nous n'avons pas rencontré entre le routeur Cisco et le commutateur Lucent.

Les performances obtenues sont bonnes, et nous n'avons en fait pas vu d'impact sur la charge du routeur quant à l'utilisation des VLAN.

Les problèmes rencontrés

Les problèmes rencontrés ont été fort peu nombreux : la configuration du commutateur fût moins aisée que celle du routeur, car nous étions habitués au vocabulaire d'un seul fabricant, et forcément il fallait retrouver les mots et expressions équivalentes dans le vocabulaire Lucent. Ce commutateur assez déroutant au début pour sa configuration des VLAN devient vite un outil plaisant car d'une part il permet de faire beaucoup de choses, et d'autre part le constructeur a livré à la fois une interface texte et une interface Web (certes c'est à la mode), et bien qu'étant par principe opposé aux interfaces de configuration par le Web, j'avoue que celle-ci m'a bien plu, au point que je l'utilise régulièrement et même que je le préfère à l'interface *telnet*.

Conclusion

Après plusieurs mois d'exploitation, la satisfaction est au rendez-vous : l'usage de VLAN a été un moyen simple de banaliser un ensemble de prises dans nos locaux et surtout un outil qui nous a permis de simuler pour un coût moindre de créer de nombreux réseaux routés, répondant ainsi à nos besoins de séparation du trafic. La solution choisie est extensible aisément, puisque aussi bien commutateur que routeur peuvent évoluer vers du Gigabit Ethernet, média sur lequel l'encapsulation 802.1Q est également disponible.