Réseaux locaux virtuels : VLAN

Introduction

Problématique

Les commutateurs assurent une segmentation des domaines de collision, mais ils n'empêchent pas les échanges entre sous-ensembles, ni n'arrêtent le passage des broadcasts. En cela, ils sont moins performants que les routeurs. En outre, les machines sont repérées géographiquement selon leur position sur les ports du commutateur (association Adresse MAC/Port).

C'est pourquoi l'on demande à ces matériels de réaliser une virtualisation du réseau physique, en procédant à une organisation gérant les segments indépendamment de la position des machines dans l'entreprise. On parle de VLAN (Virtual LAN ou RV – Réseau Virtuel).

Virtuel

L'organisation de sous-ensembles incapables de communiquer pourrait être mise en place grâce à une séparation sur des matériels indépendants (des switches différents pour les différents réseaux physiques). Mais cela demande la constitution d'une interconnexion propre à chaque sous-ensemble et une intervention physique (brassage) sur les matériels pour déplacer un poste d'un sous-ensemble à l'autre. La virtualisation permet au contraire :

- De réaliser des économies en ne multipliant pas les matériels
- De diminuer les équipements à administrer
- De remplacer les manipulations physiques par des configurations logiques : un réseau virtuel peut donc être modifié sans un déplacement sur le lieu de présence des équipements.
- De réaliser un filtrage souple des échanges, grâce à l'inscription des matériels sur un ou plusieurs VLAN

Quatre techniques se complètent pour réaliser cette segmentation :

- appartenance par le port
- appartenance par l'adresse MAC
- les réseaux virtuels de niveau 3
- appartenance par mot de passe

Cependant, seule la première correspond à une normalisation. Les autres techniques reviennent, après identification (du poste par son adresse MAC ou IP, ou de l'utilisateur), à configurer le port dans un VLAN.

I Normalisation des VLAN : 802.1Q

Définition

Un VLAN est un espace:

- logique : indépendant des connexions physiques (dans le principe)
- constitué au niveau 2 du modèle OSI : les hubs ne participent pas à la formation des VLAN, il n'est pas possible d'empêcher les échanges entre matériels connectés à un hub
- isolé du reste du réseau : il ne peut être mis en relation avec d'autres VLAN par des fonctions de niveau 2, il ne véhicule les broadcasts que dans son VLAN
- connu par les seuls matériels d'interconnexion de niveau 2 : les serveurs ne connaissent leur VLAN que s'ils disposent de cartes VLAN aware. Les postes ne connaissent pas les VLAN. Les routeurs peuvent reconnaître les VLAN.
- fonctionnant par une association par port : toute autre technique revient à associer le port à un VLAN. Seuls les ports sont associés aux VLAN.

VLAN et Normalisation

Pour que plusieurs matériels d'interconnexion puissent partager leurs informations relatives aux VLAN, il faut qu'ils puissent spécifier à quel VLAN appartient une trame qui circule entre plusieurs switches. De la contrainte liée au niveau 2, cette spécification du numéro de VLAN doit apparaître dans les entêtes de niveau 2. Or, rien dans la trame Ethernet ou 802.3 ne permet d'ajouter un tel numéro.

Deux techniques offrent une réponse à ce problème.

- Les switches communiquent entre eux pour définir à quel RV appartient le paquet qui circule (Cabletron System). Complexe et lourde, cette technique n'a pas été normalisée.
- Les switches ajoutent une étiquette (tag) identifiant le RV au paquet. Cette dernière technique s'appuie sur la norme IEEE 802.1Q, datant de 1998, l'étiquette ayant une forme et une position définies dans l'entête. La technologie propriétaire ISL de Cisco System, réalise l'équivalent.

La norme 802.1Q définit donc un entête spécifique, ajouté entre la partie Ethernet et le paquet de niveau 3. Pour qu'un matériel puisse lire cette information et qu'il ne reconnaisse pas une trame mal formée, il faut qu'il intègre la norme 802.1Q et que le port d'interconnexion soit indiqué comme participant à un échange 802.1Q. On parle d'un port ***VLAN Aware*** ou ***VLAN Tagged***, ou encore ***VLAN Capable***. Cisco utilise la terminologie ***mode trunk***.

Les commutateurs peuvent offrir cette possibilité, mais certaines cartes réseau (et le système d'exploitation) l'autorisent aussi. Les routeurs peuvent aussi supporter l'étiquetage de trames 802.1Q. La trame étiquetée aura alors la forme :

- Les deux premiers octets de ce nouveau champ auront la valeur 0x8100, qui remplace le protocole de niveau supérieur censé se trouver à cet endroit (0x0800 pour IP), et indique une étiquette VLAN. Un système ne supportant pas 802.1Q ne reconnaîtra pas cette trame (numéro de protocole supérieur inconnu) et la détruira.
- La partie priorité servira pour des acheminements hiérarchisés, grâce au protocole 802.1p.
- Le champ *CFI (Canonical Format Indicator)* sert aux techniques de routage à la source (une option de niveau 2 qui permet de définir en entête la liste des routeurs à traverser pour l'acheminement d'un paquet → commutation par les routeurs).

- Le numéro de VLAN est précisé sur 12 bits (valeurs entre 0 et 2047).

II Mise en œuvre

La mise en œuvre des VLAN consiste à paramétrer la façon dont chaque port d'un commutateur va appartenir à un VLAN, soit de manière permanente (configuration par port) soit en fonction de l'équipement ou de l'utilisateur qui utilise la machine derrière le port.

2.1 VLAN par ports

C’est la technique la plus basique, et la seule qui est effective au final.

- Un port pour machine ne peut être associé qu'à un VLAN.
- Un port appartient au moins à 1 VLAN (il y a donc un VLAN par défaut sur un commutateur gérant les VLAN).
- Plusieurs ports peuvent être affectés à un même VLAN.
- Un port d'interconnexion VLAN aware ou VLAN Tagged (il est interconnecté à un autre commutateur VLAN) véhicule l'étiquette du numéro de VLAN de la trame en circulation. Il peut être associé à plusieurs VLAN ou à tous les VLAN (technique de port trunk chez CISCO). Les ports untagged ôtent l'étiquette du VLAN.
- Un port VLAN Tagged doit communiquer vers une carte VLAN Tagged : un autre commutateur, un routeur, un serveur
- Le commutateur conserve une table associant chaque port à un VLAN (ou plusieurs)

Principe d'étiquetage et d'échange

- (1) Une trame arrive depuis un poste sur un port de commutateur.
- (2) Le commutateur étudie le numéro de VLAN associé au port.
- (3) Il consulte sa table de commutation (MAC/Port) pour déterminer si le port destination est sur le même VLAN
- (3.a) Si ce n'est pas le cas, la trame est détruite
- (3.b) Sinon, la trame est transmise vers le port destinataire.
- (4) Si le port destinataire est VLAN tagged, la trame est transmise avec étiquette, sinon sans l'étiquette.
- (5) Si le commutateur récepteur n'est pas associé au VLAN véhiculé dans l'étiquette, le paquet est détruit, sinon les étapes (3) à (5) sont reproduites.

Évaluation

On peut constater que cette technique ne répond pas entièrement au besoin d’indépendance géographique. C'est toujours le port qui est associé au VLAN, indépendamment de la machine présente derrière. Le déplacement d’un matériel le change de VLAN.

L’organisation ainsi produite colle donc étroitement à l’organisation géographique. De plus, la réalisation de ce type de VLAN devient complexe lorsque l’organisation attendue est très hiérarchisée.

Pour améliorer la situation, les fabricants ont défini des moyens de configuration dynamique de l'appartenance du port à un VLAN en s'appuyant sur des informations plus significatives telles que l'adresse MAC, les adresses IP ou l'authentification de l'utilisateur.

2.2 Appartenance par l’adresse MAC

Chaque commutateur devra disposer d’une table comportant la correspondance entre les adresses MAC des machines et le numéro de RV auquel elles sont associées.

La table MAC/Port peut être complétée par une colonne VLAN.

Principe d'étiquetage et d'échange

C'est lors de l'arrivée de la première trame que le commutateur étudie l'adresse MAC émetteur pour connaître quel VLAN sera associé au port.

Une fois ce travail effectué, le fonctionnement reste identique à la version présentée précédemment.

Évaluation

Cette technique est plus souple que la précédente. Si l'on déplace un poste sur un autre port, le port se positionnera par rapport à l'adresse MAC émetteur. Les ports sont donc auto-configurables et la gestion devient dynamique.

Toutefois, le paramétrage des associations MAC/VLAN doit être effectuée sur chaque équipement ou ceux-ci doivent disposer des protocoles d'échange de tables d'association. Il n'y a pas de système d'apprentissage automatique pour un commutateur.

Cette gestion présente l’inconvénient d’une lourdeur dans l’administration lorsque le nombre de machines croît, puisque c'est l'adresse MAC de chaque carte qui doit être renseignée. On monte donc au niveau 3 pour gagner en souplesse.

2.3 Les réseaux virtuels de niveau 3

Une première version vise à utiliser un renseignement de niveau 3 (le type de protocole de niveau 3 utilisé (IPX, IP…)) présent dans l’entête de niveau 2. Les réseaux virtuels sont ainsi découpés par protocole. Le port sera configuré en fonction de cette information. Cette approche reste trop anecdotique, les réseaux de niveau 3 autres que IP ont pratiquement disparu.

La vraie technique de niveau 3 consiste à travailler sur les adresses IP à la façon du routage. On s’appuie sur les commutateurs multi-niveaux.

Principe d'étiquetage et d'échange

La table de correspondance associera l’adresse IP (d’une machine ou d’un sous-réseau) à un numéro de RV. L'affectation port/VLAN est fonction de l'adresse IP source de la première trame échangée par le poste présent derrière un port.

Évaluation

Contrairement au routage, les sous-ensembles peuvent être constitués à partir d'un même adressage réseau, ou peuvent regrouper des équipements d'adressage différents.

D'une configuration très simple (sous ensembles IP), elle utilise cependant des matériels plus complexes et plus coûteux (switches de niveau 3 ou 2+).

2.4 Appartenance par mot de passe

Cette dernière technique est la plus souple mais la plus complexe à mettre en œuvre.

L'utilisateur, après s'être identifié (n'importe où dans l'entreprise) auprès d'un serveur d'authentification (TACACS ou le plus souvent RADIUS), se voit rattaché à son réseau virtuel. La correspondance entre l'identifiant/mot de passe et le réseau virtuel est très simple à effectuer et stockée sur un serveur (Windows, Linux, etc).

Principe d'étiquetage et d'échange

Le matériel de commutation joue alors le rôle de relais d'authentification et reçoit en réponse le VLAN d'appartenance du port pour la durée de session.

Évaluation

Ce principe est extrêmement souple puisque c'est l'individu qui est associé à un VLAN et non la machine à laquelle il se connecte. En revanche, il nécessite une infrastructure plus complexe.

Le commutateur doit être le point de passage obligatoire pour la connexion au réseau, ce qui peut compliquer l'infrastructure ou nécessiter beaucoup de matériels coûteux.

III Paramétrage

3.1 Présence sur plusieurs VLANs

Pour qu'un matériel (un routeur ou un serveur) soit présent sur plusieurs VLANs, il faut que la machine possède une connexion sur chacun des réseaux virtuels (donc autant de cartes réseau).

Une autre possibilité est de mettre en place une carte réseau VLAN aware dans le matériel. La demande en provenance du client sera affectée à un VLAN comme vu précédemment, et elle parviendra étiquetée jusqu'au serveur. Celui-ci répondra au client en précisant dès le départ le numéro de VLAN (trame étiquetée) correspondant à celui de la demande qui lui est parvenue.

3.2 Communication Inter-VLAN

L'avantage principal des VLAN est d'interrompre la diffusion des échanges broadcasts (segmentation des domaines de diffusion) et de séparer le réseau en sous-ensembles isolés. L'inconvénient est justement cette impossibilité de connexion entre les réseaux virtuels ainsi constitués.

Solution propriétaire

Certains fabricants ont conçu leurs propres techniques de définition des réseaux virtuels. Les matériels les plus simples ne supportent pas 802.1Q. Ils permettent des associations libres entre un port et plusieurs VLAN, mais qui n'ont d'existence qu'au sein d'un matériel unique.

CISCO a implémenté sa propre solution **ISL**, très proche de 802.1Q mais avec des étiquetages propriétaires.

Passage au niveau 3

Une fonctionnalité ajoutée au commutateur est la possibilité d'assurer la communication entre VLAN en travaillant sur une information de niveau supérieur : le niveau réseau.

Le commutateur se comporte alors comme un routeur filtrant, c'est à dire qu'il détermine les contrôles d'accès (Access Control Lists – ACL) entre sous-réseaux IP. Cela implique que l'organisation des réseaux virtuels s'appuie sur un adressage IP suivant le même découpage (en réseaux ou sous-réseaux IP distincts).

On sort du fonctionnement de la couche liaison et il ne s'agit donc plus d'une fonction de commutation, même si elle est intégrée aux mêmes matériels.

Conclusion

Avec les VLAN, le même mouvement de fusion des fonctions de niveau 2 et 3 connu dans les réseaux étendus atteint les réseaux locaux, avec les difficultés de paramétrage que cela entraîne inévitablement.