Segmentation des réseaux locaux

Philippe Latu
philippe.latu(at)linux-france.org

http://www.linux-france.org/prj/inetdoc/

Historique des versions		
$Revision: 1387 $	$Date: 2009-05-10 18:03:03 +0200 (dim 10 mai 2009) $	$Author: latu $
Année universitaire 2008-2009		

Résumé

Depuis quelques années, les commutateurs sont les outils de base de la conception d'architecture réseau. La garantie sur la bande passante délivrée par port a fortement contribué au développement des réseaux locaux. Pour autant, la commutation de trames Ethernet associée aux réseaux virtuels (VLANs) peut-elle supplanter le routage dans la gestion des réseaux ? Aujourd'hui, pour concevoir correctement une architecture, il faut considérer : les besoins en application, les schémas de trafic et la composition des groupes de travail. Cet article donne des éléments de choix entre routage et commutation.

Table des matières

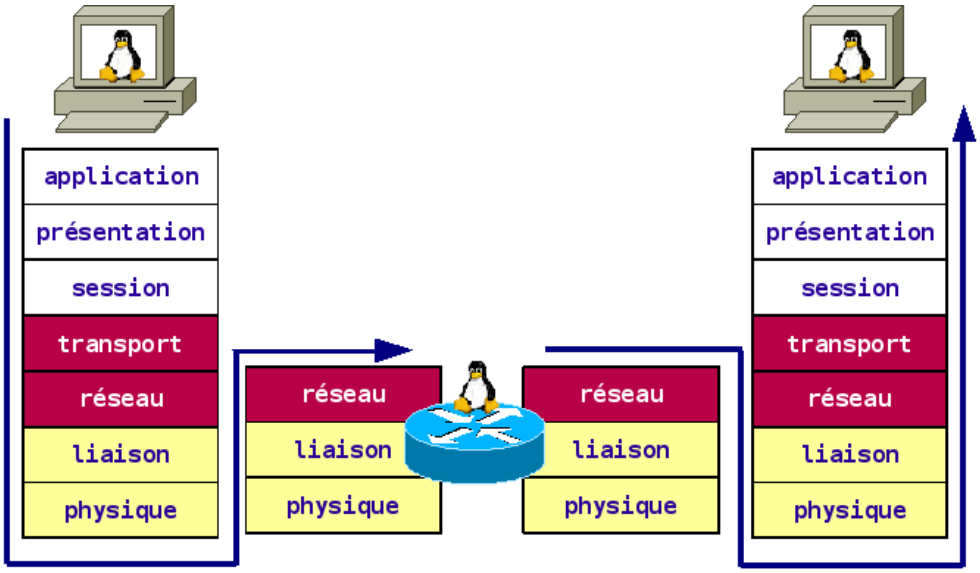
1. Copyright et Licence

1.1. Meta-information

Cet article est écrit avec *DocBook*[1] XML sur un système *Debian*[2]. Il est disponible en version imprimable aux formats PDF et Postscript : `segmentation_lan.pdf`[3]| `segmentation_lan.ps.gz`[4].

2. Introduction

D'après la modélisation OSI, c'est la couche réseau (niveau 3) qui assure l'interconnexion entre les réseaux. La couche réseau gère donc le trafic entre réseaux.



Les 7 couches du modèle OSI - vue complète[5]

La conception des réseaux locaux a toujours été l'art de trouver le bon équilibre entre rapidité et qualité. Les commutateurs répondent parfaitement au critère rapidité tandis que les routeurs répondent parfaitement au critère qualité.

Voici donc une présentation des deux techniques : commutation et routage, suivie d'une synthèse sur la segmentation des réseaux locaux.

3. La commutation

La technologie de commutation opère au niveau 2 du modèle de référence OSI. La nouvelle popularité des commutateurs peut être vue comme la résurgence de la technologie des ponts.

- Tout comme un pont, le commutateur décide de la redirection à partir de l'adresse MAC contenue dans chaque trame.
- A la différence d'un pont, le commutateur redirige les données avec des temps d'attente très courts et des algorithmes intégrés directement dans ses composants.

La commutation permet de répartir la bande passante à la fois sur des segments partagés et des segments dédiés.

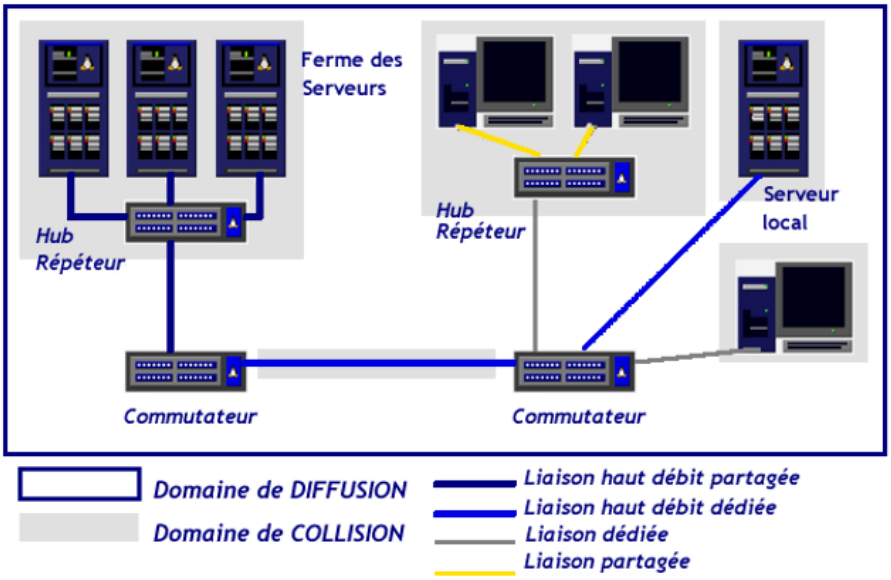
3.1. Modèles de propagation

Commutation *cut-through*
: Elle démarre le processus propagation à partir de l'adresse MAC du destinataire avant que la totalité de la trame soit reçue. Avec ce modèle, les temps d'attente sont aussi courts quelle que soit la longueur des trames. Cependant, les trames erronées sont transmises sans aucun contrôle.

[1] http://www.dodcbook.org
[2] http://www.debian.org
[3] http://www.linux-france.org/prj/inetdoc/telechargement/segmentation.lan.pdf
[4] http://www.linux-france.org/prj/inetdoc/telechargement/segmentation.lan.ps.gz
[5] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/images/osi.png

Commutation *store and forward*
: La totalité de la trame est lue et validée avant sa retransmission. Ceci permet de supprimer les trames corrompues et de définir des filtres pour contrôler le trafic à travers le commutateur. Les temps d'attente augmentent avec la longueur des trames.

3.2. Où utiliser des commutateurs ?



Où utiliser la commutation ? - vue complète[6]

Les commutateurs doivent être considérés comme fournisseurs de bande passante et non comme une amélioration de la sécurité et du contrôle du réseau. Les besoins en bande passante proviennent :

- du nombre toujours croissant du nombre de postes connectés,
- du développement de la puissance des postes,
- de l'émergence d'applications client/serveur de type Internet (courrier, serveurs Web, etc.),
- du regroupement des serveurs au sein de «fermes de serveurs».

4. Le routage

Les routeurs opèrent au niveau 3 du modèle de référence OSI. Ils ont beaucoup plus de fonctions logicielles qu'un commutateur. En fonctionnant à un niveau plus élevé qu'un commutateur, un routeur distingue les différents protocoles de la couche réseau : IP, IPX, AppleTalk, etc. Cette connaissance permet au routeur de prendre des décisions plus sophistiquées de propagation.

- Comme un commutateur, un routeur fournit aux utilisateurs une communication transparente entre des segments individuels.
- A la différence d'un commutateur, un routeur détermine les limites logiques entre des groupes de segments de réseaux.

Un routeur fournit un service de *contrôle d'accès* parce qu'il ne transmet que le trafic destiné à le traverser. Pour accomplir ces tâches, un routeur doit réaliser 2 fonctions de base :

1. Créer et maintenir une table de routage pour chaque protocole de routage. Ces tables sont mises à jour dynamiquement grâce aux protocoles de routage.

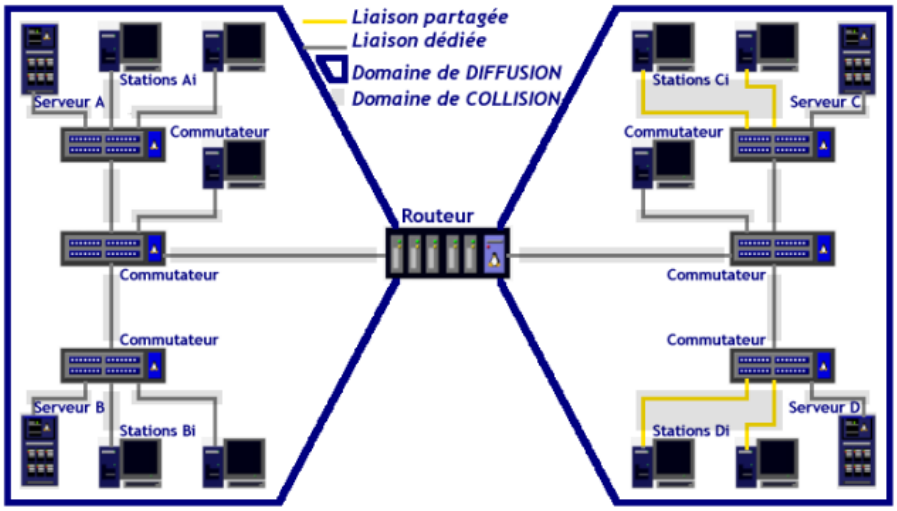
2. Identifier le protocole contenu dans chaque paquet, extraire l'adresse de destination réseau et prendre la décision de propagation en fonction des données de la table de routage.

[6] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/images/utiliser_commutation.png

Les fonctionnalités étendues d'un routeur lui permettent de choisir le meilleur chemin à partir de plus d'éléments qu'une simple adresse MAC : comptage des « sauts », vitesse de transmission, coût, délais et conditions de trafic.

Ces améliorations conduisent à une meilleure sécurité, une meilleure utilisation de la bande passante et plus de contrôle sur les opérations réseau. Cependant, les temps de traitement supplémentaires peuvent réduire les performances comparativement à un simple commutateur.

4.1. Où utiliser des routeurs ?



Où utiliser un routeur ? - vue complète[7]

Les routeurs sont conçus pour gérer les architectures réseau en assurant les besoins suivants :

1. Segmenter les réseaux en domaines de diffusion isolés. La hiérarchie résultante permet de déléguer l'autorité et la gestion des réseaux.

2. Filtrer intelligemment les paquets et supporter les chemins redondants en assurant une «balance de charge».

Dans l'exemple ci-dessus :

- Les stations Ai et Bi bénéficient de liaisons dédiées. Chacune dispose de la totalité de la bande passante du réseau.
- Les stations Ci et Di utilisent des liaisons partagées. La bande passante totale est répartie entre les stations actives.
- Le trafic de diffusion des serveurs A et B ne traverse pas le routeur. La bande passante est préservée entre les réseaux.

5. Segmentation

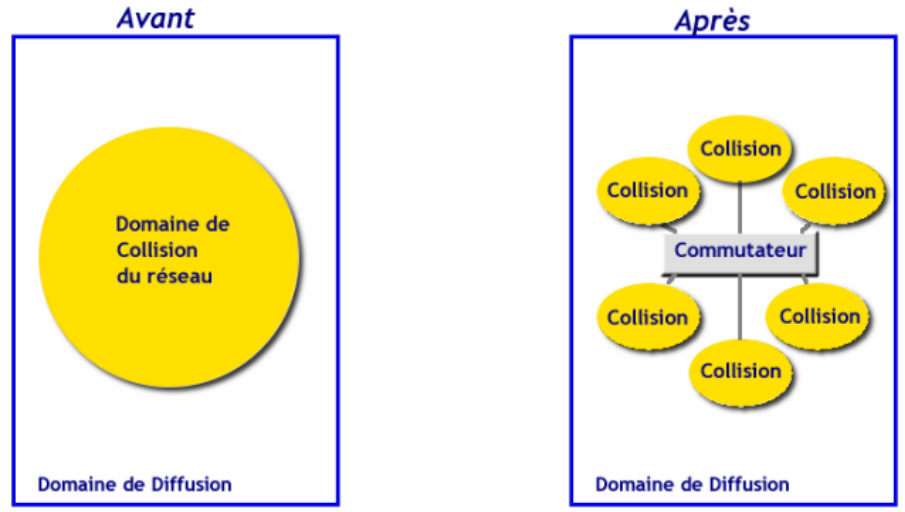
Les facultés des commutateurs et des routeurs à segmenter les réseaux sont une source de confusion. Comme chacun des 2 dispositifs opère à un niveau différent du modèle OSI, chacun réalise un type de segmentation différent.

5.1. Un commutateur segmente des domaines de collision

La segmentation au niveau 2 réduit le nombre de stations en compétition sur le même réseau local. Chaque domaine de collision possède la bande passante délivrée par le port du commutateur.

Les domaines de collisions appartiennent au même domaine de diffusion.

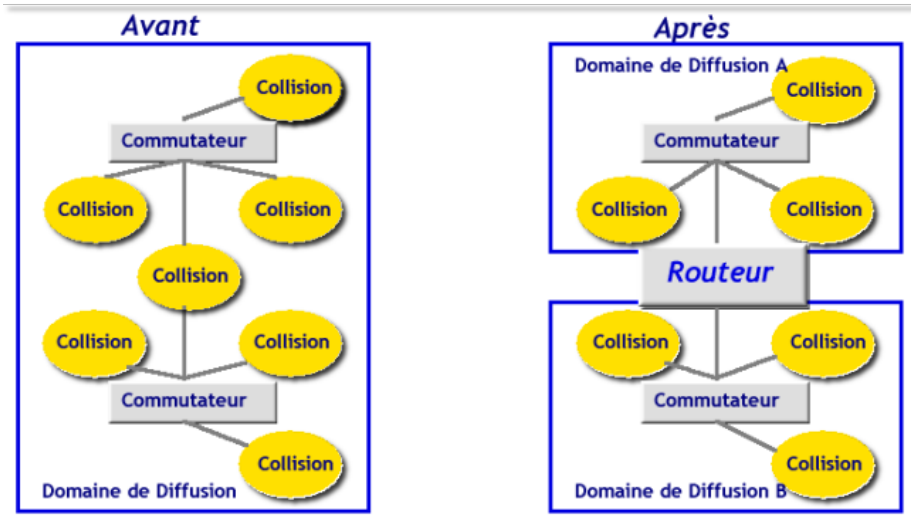
[7] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/images/utiliser_routage.png



Segmenter avec un commutateur - vue complète[8]

5.2. Un routeur segmente des domaines de diffusion

La segmentation au niveau 3 réduit le trafic de diffusion en divisant le réseau en sous-réseaux indépendants.



Segmenter avec un routeur - vue complète[9]

5.3. Synthèse

C'est grâce aux progrès de l'électronique qui ont permis d'augmenter les densités d'intégration et les fréquences, que les commutateurs ont pu se développer.

Dans le même temps, les fonctions réalisées par les routeurs n'ont cessé d'augmenter en quantité et en qualité. Il ne faut pas oublier que toute la sécurité d'un système d'information se «joue» sur les équipements d'interconnexion. Une règle de sécurité sur une équipement réseau est évaluée à chaque nouveau paquet tandis qu'une règle de sécurité applicative n'est évaluée qu'à l'authentification.

Il était donc inévitable que l'on aboutisse à des équipements «hybrides». Aujourd'hui, les routeurs les plus performants associent une électronique rapide (celle du commutateur) au niveau 2 et un logiciel complet (les fonctions du routeur) au niveau 3.

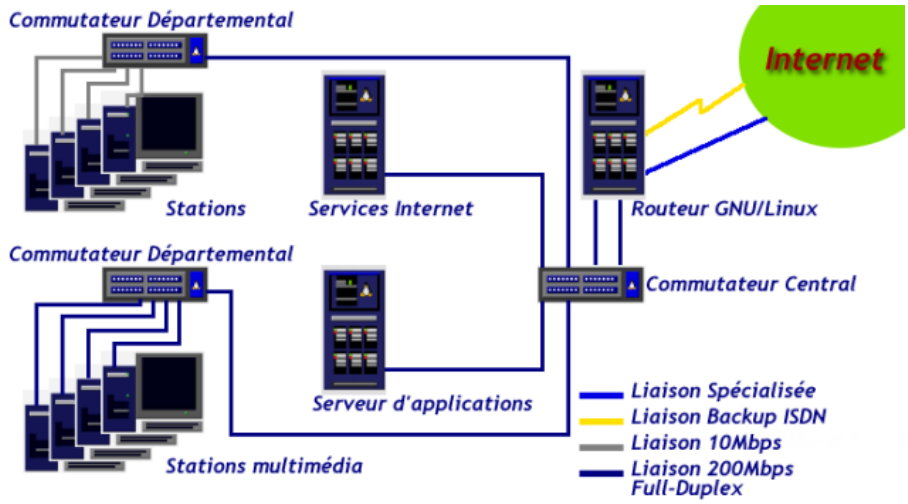
Pour parvenir à ce résultat, on trouve 2 approches :

[8] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/images/domaine_collision.png
[9] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/images/domaine_diffusion.png

- **Les équipements haut de gamme.**
  Les ténors du marché de l'interconnexion réseau proposent des appareils avec une électronique de commutation et de chiffrage spécifique. Les fonctions de routage sont assurées par des systèmes d'exploitation propriétaires. C'est la solution la plus complète et la plus efficace mais elle a un coût très élevé.
- **Les réseaux virtuels ou VLANs.**
  La norme IEEE 802.1Q permet une segmentation dynamique des sous-réseaux. C'est une solution attrayante du point de vue gestion de parc mais incomplète du point de vue contrôle d'accès. Il est possible d'exploiter les informations des trames IEEE 802.1Q en les associant à un adressage réseau de niveau 3. On parle alors de *routage inter-vlan*.

6. Exemple de conception

En tenant compte des notions abordées ci-dessus, voici un exemple d'architecture à faible coût. Il s'agit de concilier la fourniture de bande passante pour le réseau local et le contrôle d'accès pour le réseau étendu.



Exemple de conception - vue complète[10]

Routeur GNU/Linux

Généralement, les liaisons d'accès à Internet ont un débit maximum inférieur à 10Mbps. Un châssis serveur d'entrée de gamme peut très bien accueillir 4 interfaces :

- Une liaison spécialisée à 2Mbps,
- Une liaison Backup RNIS/ISDN à 128Kbps,
- 2 interfaces Ethernet 10/100Mbps supportant le mode Full-Duplex qui permet d'atteindre les 200Mbps. C'est aussi au niveau de ces interfaces que le routage inter-VLAN permet de gérer les domaines de diffusion associés aux groupes de travail.

Une configuration comme celle-ci peut très bien assumer toute la complexité des traitements de contrôle d'accès et déléguer la fourniture de bande passante au commutateur central.

Commutateur central

Toutes les fonctions d'aiguillage au niveau réseau (couche 3 OSI) étant assurées par le routeur, on peut se contenter d'une programmation par port du commutateur central pour délimiter les *périmètres* à l'intérieur du réseau local. Ces périmètres peuvent correspondre à :

- des niveaux d'utilisation : choix d'applications ou de puissance de calcul,
- des niveaux de sécurité : filtrage des services.

Commutateur départemental

Comme ces commutateurs ou hubs sont situés à l'intérieur des *périmètres*, ils ne nécessitent pas de programmation particulière. Ils héritent de la configuration réalisée au niveau supérieur.

[10] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/images/exemple_conception.png