interconnexion de périmètres réseaux

philippe.latu(at)linux-france.org

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

Historique des versions		
$Revision: 1619 $	$Date: 2011-04-05 00:08:00 +0200 (mar. 05 avril 2011) $	$Author: latu $
(draft) En cours de rédaction.		

La conception d'une architecture réseau est un problème très vaste. L'objectif de ce document est de donner les éléments de conception nécessaires aux deux scénarios : Serveur d'accès et Routeur d'agence utilisés pour illustrer l'interconnexion d'un réseau local avec un réseau étendu. Pour répondre à cet objectif, on présente une autre approche de la classification des réseaux basée sur la notion de périmètre. On introduit ensuite les 3 principaux types d'interconnexion suivant cette classification.

Table des matières

Chapitre 1. Copyright et Licence

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

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.linux-france.org/prj/inetdoc/telechargement/interconnexion.perimetres.pdf
[4] http://www.linux-france.org/prj/inetdoc/telechargement/interconnexion.perimetres.ps.gz

Chapitre 2. Classification des réseaux

La méthode «traditionnelle» de classification des réseaux est basée sur les distances. Elle est fondée sur le principe qui veut que les techniques de transmission changent suivant les distances à parcourir. En première approximation, les travaux pratiques présentés ici constituent une bonne illustration.

1. Transmission en mode non connecté par diffusion côté réseau local (LAN).
2. Transmission en mode connecté point à point côté réseau étendu (WAN).

Avec l'évolution des technologies et surtout l'augmentation du nombre et de la taille des réseaux, la distance n'est plus le critère unique de classification. On trouve aujourd'hui des réseaux de diffusion dits locaux de taille très supérieure à certains réseaux étendus.

Consécutivement au développement des types d'interconnexions liés à l'Internet, la notion de *périmètre* tend à supplanter le découpage classique : LAN, MAN, WAN. Cette dénomination recouvre plusieurs sens. Voici une classification suivant le *niveau de contrôle*.

2.1. Périmètre d'intervention

C'est la définition la plus générale. A ce niveau on distingue le réseau privatif, celui sur lequel on peut intervenir, du réseau de connexion. Le réseau de connexion correspondant à une prestation d'un opérateur de télécommunication, on ne peut intervenir sur ses équipements. La frontière entre les 2 domaines est matérialisée par le *Point Of Presence* (POP), le local où l'opérateur installe et maintient ses équipements.

2.2. Périmètre de diffusion

C'est la définition «historique» de l'interconnexion de réseaux. Dès qu'il y a routage, on crée deux périmètres ou domaines de diffusion. Pour plus d'information, lire l'article *Segmentation des réseaux locaux*[1].

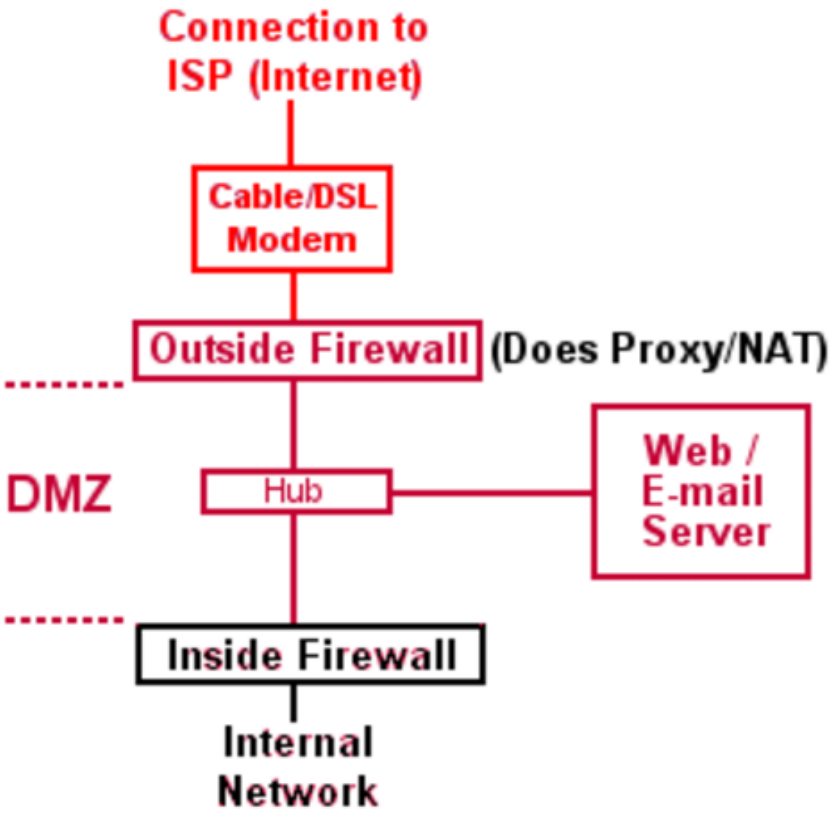
2.3. Périmètre de contrôle d'accès

C'est ce dernier type qui a propulsé la notion de périmètre au devant de la scène. Dans une interconnexion mixte entre réseaux privés et réseaux publics partagés on ne peut plus se permettre de ne contrôler que la diffusion.

Aujourd'hui, un périmètre de contrôle doit répondre à 2 objectifs : la qualité de service réseau et la sécurisation des accès. En règle générale, on définit plusieurs périmètres à l'intérieur d'une infrastructure privée suivant les niveaux de contrôle que l'on veut instaurer.

Le découpage en vogue consiste à constituer une «zone démilitarisée» (DMZ) ou «réseau écran» entre le réseau public partagé (l'Internet) et le réseau privé. Dans tous les cas, on cherche à faire coïncider les périmètres de sécurité et de qualité de service.

[1] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/



2.3.1. Qualité de service

Face à la croissance constante du trafic sur tous les types de réseaux, l'augmentation de la bande passante ne peut résoudre tous les problèmes. C'est ce constat qui a conduit au développement de la qualité de service réseau.

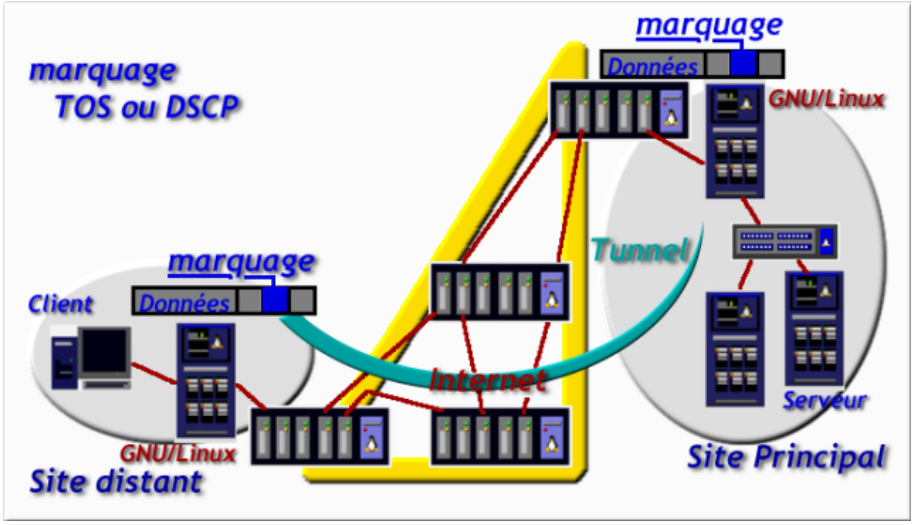
La qualité de service (QoS ou *Quality of Service*) se définit au moins à deux niveaux d'après le standard RFC3198 *Terminology for Policy-Based Management*[2] :

Niveau d'abstraction
: Aptitude à délivrer des services réseau suivant les paramètres spécifiés par une convention de service (*Service Level Agreement*).

Niveau réseau
: Ensemble de fonctions qui permet à un fournisseur de services de contrôler les priorités, la bande passante et les temps d'attente. Il existe deux approches de mise en oeuvre de qualité de services sur les réseaux IP : services intégrés [RFC1633 *Integrated Services in the Internet Architecture: an Overview*[3]] et services différenciés *Differentiated Services*. La signalisation est assurée par le protocole RSVP [RFC2205 *Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification*[4]] pour les services intégrés et par le protocole DiffServ [RFC2475 *An Architecture for Differentiated Service*[5]] pour les services différenciés. RSVP alloue les ressources du réseau par flux en se basant sur les besoins quantitatifs des applications. DiffServ assure le marquage des en-têtes de paquets IP pour affecter une priorité sur plusieurs flux.

Une fois le mécanisme de priorité disponible, la mise en place d'une qualité de service suppose la définition des règles pour utiliser ce mécanisme. Pour garantir le respect de ces règles, on emploie une «police» (*policy*) qui les impose aux limites d'un périmètre. On parle de *routing policies*.

[2] http://www.faqs.org/rfcs/rfc3198.html
[3] http://www.faqs.org/rfcs/rfc1633.html
[4] http://www.faqs.org/rfcs/rfc2205.html
[5] http://www.faqs.org/rfcs/rfc2475.html



2.3.2. La sécurisation des accès

La «règle d'or» de la sécurité réseau veut que le contrôle d'accès soit appliqué sur les équipements réseau. Les équipements d'interconnexion les plus importants sont placés aux frontières des périmètres. Une politique de routage (*routing policiy*) s'applique à chaque paquet IP traversant le routeur d'extrémité du périmètre tandis que l'authentification ne s'applique qu'à la première utilisation d'une application.

Le respect de cette règle impose une hiérarchie dans le contrôle d'accès.

1. Routage filtrant : sélection des réseaux (autres périmètres) pouvant accéder au périmètre à contrôler.
2. Sélection des services ouverts : fermeture de tous les ports/services inutiles à l'intérieur du périmètre à contrôler.
3. Administration des services ouverts : restriction des accès par services. En général chaque application/service (bind, sendmail, apache, etc.) possède ses propres mécanismes de sécurité.

2.3.3. La sécurisation des échanges

Avec le développement des échanges commerciaux ou des échanges entre les différents sites géographiques d'une même société, il est nécessaire d'envisager la sécurisation des échanges entre périmètres. La mise en place de tunnels de communication chiffrés entre périmètres permet de sécuriser le transport de l'information sur les réseaux publics partagés. On parle alors de Réseaux Privés Virtuels (VPN : *Virtual Private Network*).

Les différents types de Réseaux Privés Virtuels sont présentés dans l'article *Logiciel Libre & Technologies Réseaux*[6].

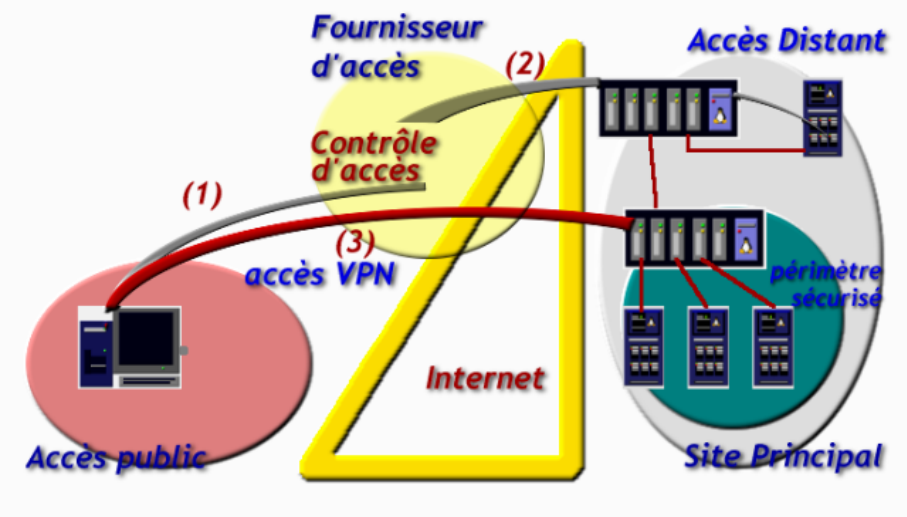
[6] http://www.linux-france.org/prj/inetdoc/articles/reseau.libre/

Chapitre 3. Types d'interconnexion

Pour concevoir une architecture d'interconnexion, on peut distinguer 3 types d'interconnexion.

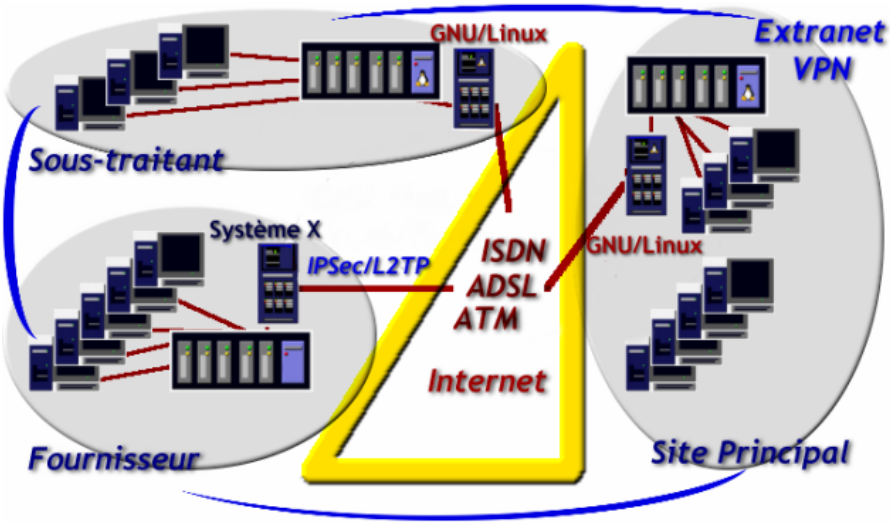
Connexion individuelle

On désigne par connexion individuelle, nomade ou distante (*remote access*) tous les accès extérieurs aux périmètres sous contrôle à partir d'un poste isolé.



Interconnexion d'agences

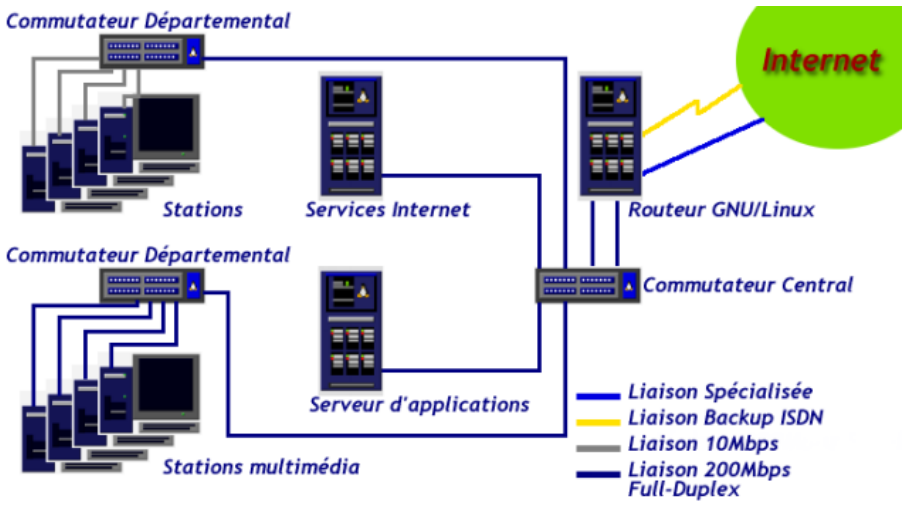
Ce type correspond à l'interconnexion de plusieurs périmètres (*extranet*) à travers l'Internet.



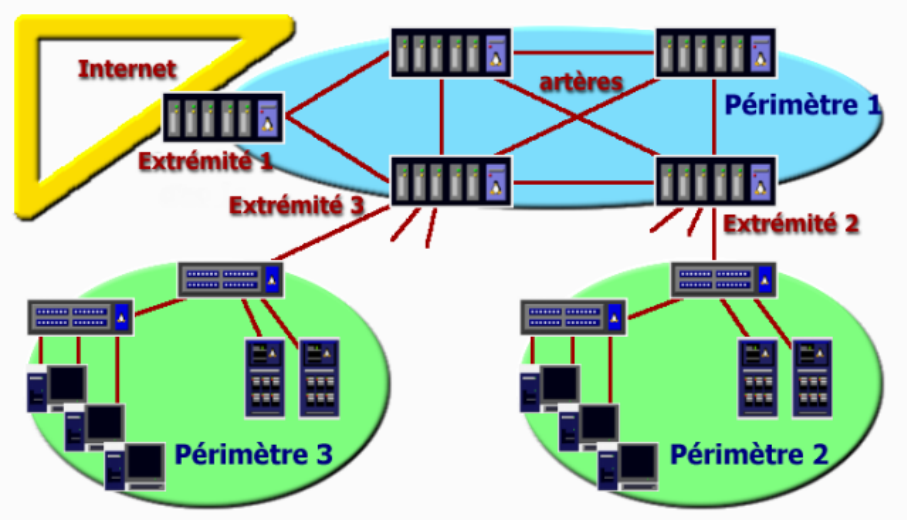
Interconnexion de campus

Un réseau de campus correspond à une interconnexion de réseaux locaux de taille importante (200 hôtes ou plus). La principale différence par rapport aux deux types précédents tient à l'utilisation de la commutation. Les commutateurs sont des éléments importants de qualité de service. Ils fournissent un débit garanti par port. Pour plus d'information, lire l'article *Segmentation des réseaux locaux*[1].

[1] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/


Commutateur Départemental
Internet
Stations
Services Internet
Routeur GNU/Linux
Commutateur Départemental
Commutateur Central
Serveur d'applications
Liaison Spécialisée
Liaison Backup ISDN
Liaison 10Mbps
Liaison 200Mbps Full-Duplex
Stations multimédia

Chapitre 4. Technologies d'interconnexion réseau



On peut distinguer 2 modes de fonctionnement :

Interconnexion de réseaux sans contrôle d'accès, Interconnexion intra-périmètre
: Dans un environnement ouvert, ou plus exactement à l'intérieur d'un périmètre sous contrôle, c'est ce premier mode d'interconnexion qui domine. On ne se préoccupe ici que de la transmission de l'information. Les principales fonctions traitées sont le transport sur des réseaux hétérogènes et l'équilibre de charge de trafic entre réseaux.

Interconnexion de réseaux avec contrôle d'accès, Interconnexion inter-périmètre
: Avec le développement des flux réseaux malveillants sur l'Internet, on cherche à contrôler la nature de l'information transmise à travers les réseaux publics partagés. Il existe deux mode d'exploitation génériques du contrôle d'accès :

- Application de règles de filtrage et de qualités de services aux frontières des périmètres sur les routeurs d'extrémités.

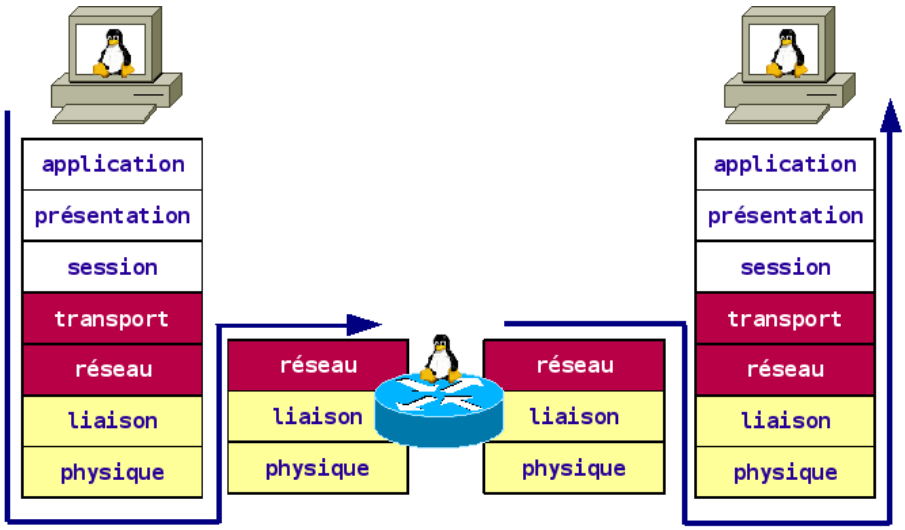
- Mise en œuvre de tunnels de transmission chiffrés sur les réseaux publics partagés entre les périmètres sous contrôle. L'article *Logiciel Libre & Technologies Réseaux*[1] donne quelques exemples.

4.1. Interconnexion de réseaux sans contrôle d'accès

Ce mode d'interconnexion remonte aux origines des liaisons entre systèmes informatiques. Au départ, les difficultés de transmission étaient liées à l'hétérogénéité matérielle et logicielle des réseaux. Les premières techniques d'interconnexion dépendaient soit des constructeurs de systèmes informatiques, soit des compagnies de télécommunication.

Il a fallu attendre 1984 pour que l'on aboutisse à une modélisation ouverte publiée par un organisme de normalisation indépendant : le modèle OSI. Lire l'article *Modélisations réseau*[2] pour plus d'informations sur les principales modélisations réseau. Ce sont les couches liaison (2) et réseau (3) qui couvrent tous les problèmes d'interconnexion.

[1] http://www.linux-france.org/prj/inetdoc/articles/reseau.libre/
[2] http://www.linux-france.org/prj/inetdoc/articles/modelisation/



4.1.1. Interconnexion de niveau 2

4.1.1.1. Les types d'équipement

Il existe 2 types d'équipement réseau pour l'interconnexion au niveau liaison de la modélisation OSI.

Pont
: Les ponts sont apparus au début des années 1980. Un pont sert à interconnecter deux réseaux locaux ou plus pour constituer un réseau local unique de plus grande taille. La transmission des trames d'un réseau à l'autre est basée sur les adresses MAC. Suivant les types de réseaux, on trouve différents types de ponts :
  - Dans le cas d'une connexion entre deux réseaux Ethernet, on parle de *transparent bridging*.
  - Dans le cas d'une connexion entre deux réseaux Token Ring, on parle de *source-route bridging*.
  - Dans le cas d'une connexion entre un réseau Ethernet et un réseau Token Ring, on parle de *translational bridging*.
  - Il est aussi possible de relier deux réseaux locaux à l'aide d'une ligne téléphonique. On parle alors de *remote bridging*.

  Avant l'émergeance de la commutation, les ponts tendaient à disparaître au profit des routeurs. Aujourd'hui, les équipements de commutation possèdent de nombreuses fonctions plus intéressantes : coût, nombre de ports, bande passante par port et réseaux virtuels de type VLAN.

Commutateur
: Les commutateurs, comme les ponts, relient plusieurs segments de réseaux locaux pour constituer un réseau unique. La transmission des trames est aussi basée sur les adresses MAC. La dénomination *commutation de trame* provient de l'intégration dans des composants spécifiques (ASICs) des algorithmes de transmission. C'est grâce aux performances de ces composants que la bande passante par port est garantie. Pour plus d'informations, lire l'article *Segmentation des réseaux locaux*[3].

  La commutation de trame (ou de cellules) s'applique aussi bien aux réseaux locaux Ethernet (de 10Mbps à 10Gbps) qu'aux réseaux étendus de type ATM.

4.1.1.2. Les réseaux locaux virtuels

Les réseaux locaux virtuels (VLANs *Virtual Local Area Networks*) sont apparus consécutivement aux commutateurs. La norme IEEE 802.1Q a été publiée en Décembre 1998.

La première génération de réseau virtuel était basée sur la commutation par port (*port switching*). Le principe de base consiste à associer les ports du commutateur en un réseau unique. Cette méthode est très simple mais elle engendre de grosses difficultés d'administration lorsque le nombre de ports augmente. C'est à partir de ce constat que l'on a aboutit aux VLANs.

[3] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/

Le principe du VLAN consiste à associer des adresses MACs en un réseau unique. De cette façon, si un poste (une adresse MAC) se déplace à l'intérieur de l'infrastructure réseau, il appartiendra toujours au même VLAN. L'argument principal d'adoption des VLANs provient de la vitesse de commutation. En effet, les composants spécialisés d'un commutateur effectuent les opérations d'aiguillage beaucoup plus vite que le logiciel d'un routeur traditionnel. Même si une base de données d'adresses MAC (VLAN) est plus facile à gérer qu'une base de câblage (*port switching*), on retombe sur les mêmes difficultés d'administration à l'échelle d'un campus. On a donc redécouvert les vertus des fonctions du niveau réseau (3).

4.1.1.3. Le Spanning Tree Protocol

Ce protocole standard appelé *Spanning Tree Protocol* normalisé IEEE 802.1d a pour rôle principal d'éviter les boucles de transmission. Après une phase de découverte de la topologie physique du réseau, l'algorithme de *Spanning Tree Protocol* établit une arborescence logique sans boucle. Cet algorithme est ancien. Il était présent sur les réseaux maillés par ponts.

L'arbre réseau logique est basé sur une table d'adresses MAC maintenue dynamiquement. La norme IEEE 802.1d spécifie le format des paquets que les équipements de niveau 2 doivent échanger pour construire l'arbre et déterminer quel est l'équipement racine. Cette norme fixe aussi la durée de vie des entrées de table. Lorsqu'il n'y a plus aucune activité sur le réseau, la table se vide progressivement. Au redémarrage du trafic, on assiste à des «orages de diffusions» (*broadcast storms*).

Il existe deux cas de figure dans lesquels on rencontre des boucles de transmission.

Redondance d'artère
: Pour garantir la continuité de service d'une artère de réseau, on a souvent recours à la redondance. L'algorithme STP sert alors à désactiver tous les chemins redondants sauf un et à choisir un nouveau chemin actif si le précédent est en défaut. Comme le trafic n'est jamais nul sur une artère, l'arbre logique est toujours maintenu en état.

Boucle involontaire
: Ce cas ne devrait tout simplement *jamais* se produire.

Utilisation avec GNU/Linux

Il est possible de mettre en œuvre l'algorithme *Spanning Tree Protocol* en utilisant plusieurs interfaces Ethernet en pont avec GNU/Linux. Cette configuration est décrite dans le document *Linux BRIDGE-STP-HOWTO*[4]. Pour les noyaux Linux de la série 2.4.xx, voir <FIXME: support Laurent>. Les outils de l'espace utilisateur sont fournis dans le paquet bridge-utils.

4.1.1.4. Où utiliser l'interconnexion de niveau 2 ?

Les ponts ne présentent plus d'intérêt.

Les commutateurs sont de plus en plus utilisés. Les commutateurs sont des équipements qui fournissent de la bande passante à moindre coût ce qui les rend très populaires. Il faut cependant prendre garde aux problèmes engendrés par la diffusion. Un équipement de niveau 2 ne contrôle pas la diffusion, il doit obligatoirement être associé à un équipement de niveau 3 (routeur ou commutateur). Les configurations à fort trafic de diffusion sont de plus en plus fréquentes : réseaux de plusieurs dizaines de postes clients Windoze utilisant le service DHCP et se connectant à des annuaires/domaines Windoze.

Les VLANs sont une bonne solution d'organisation logique des réseaux de taille limitée. Dès que les domaines définis pour chaque VLAN augmentent en taille ou commencent à se chevaucher, il faut passer à l'interconnexion de niveau 3.

Il est préférable que la redondance soit pilotée par des équipements de niveau 3. Ainsi, tous les liens participent au transport de l'information et la gestion de la balance de charge est plus souple.

[4] http://tldp.org/HOWTO/BRIDGE-STP-HOWTO/

4.1.2. Interconnexion de niveau 3

4.1.2.1. Les types d'équipement

Il existe 2 types d'équipement réseau pour l'interconnexion au niveau 3 de la modélisation OSI.

Routeur traditionnel
: Le routeur traditionnel utilise des composants matériels pour les niveaux physique et liaison puis des composants logiciels pour le niveau réseau. Cette solution a été adoptée pour gérer plus facilement les évolutions des fonctions de routage.

Commutateur de niveau 3
: Un commutateur de niveau 3 reprend l'utilisation de composants spécifiques (ASICs) du commutateur de niveau 2 en y ajoutant des fonctions supplémentaires au niveau 3. Ces fonctions réseau effectuent des traitements sur les en-têtes de paquets standards (IP, IPX, etc.). On utilise alors l'appellation *packet-by-packet Layer 3 switches*.

4.1.2.2. Le rôle du niveau réseau

Le rôle et les fonctions du niveau réseau sont présentés dans les articles *Modélisations réseau*[5] et *Segmentation des réseaux locaux*[6].

Il existe 2 catégories de protocoles de routage. Ils se distinguent par la méthode de maintenance des tables de routage.

Distance-Vector
: Les protocoles tels que RIP I & II et IGRP procèdent par échange périodique des informations contenues dans les tables de routage. Sur des liens de faible débits, ces échanges peuvent consommer une partie non négligeable de la bande passante. Dans le cas de connexions téléphoniques, ils peuvent générer des appels inutiles lorsqu'il n'y a pas d'activité sur le réseau.

Link-State
: Les protocoles tels que EGP, BGP, EIGRP et OSPF ne transmettent leurs informations de routage que lors d'un changement d'état du réseau. On limite ainsi la consommation de bande passante utile. Relativement aux protocoles *Distance-Vector*, ils nécessitent une plus grande puissance de calcul. Chaque processus de routage doit recomposer une image complète de la topologie du réseau à chaque changement d'état.

Utilisation avec GNU/Linux

Tous les protocoles de routage essentiels sont disponibles sur les systèmes GNU/Linux. Le projet *Quagga Routing Suite*[7] fournit un logiciel de routage fiable et parfaitement interopérable avec des équipements hétérogènes.

4.1.2.3. Où utiliser l'interconnexion de niveau 3 ?

L'interconnexion de niveau 3 est intrinsèquement la plus complète.

Les 2 critères de choix entre le routeurs et le commutateur de niveau 3 sont :

- *Le coût*. Le routeur traditionnel utilise un matériel standard largement amorti. A l'inverse, le commutateur de niveau 3 utilise une électronique spécifique beaucoup plus onéreuse. Au delà de l'intégration des fonctions dans les composants, la vitesse de commutation des paquets est un élément important dans le coût d'un commutateur.
- *La bande passante entrante*. Si le débit maximum entrant dans le périmètre est limité comme dans le cas d'une connexion d'agence, il est inutile d'employer un commutateur aux capacités très supérieures. A l'inverse une interconnexion de campus bénéficie d'une bande passante entrante élevée compte tenu des besoins d'accès importants générés par un grand nombre d'utilisateurs. Voir Chapitre 3, *Types d'interconnexion* ; exemple Interconnexion de campus.

[5] http://www.linux-france.org/prj/inetdoc/articles/modelisation/
[6] http://www.linux-france.org/prj/inetdoc/articles/segmentation.lan/
[7] http://www.quagga.net/

Enfin, les équipement de niveau 3 sont les seuls à pouvoir gérer efficacement la redondance et la balance de charge entre périmètres.

4.2. Interconnexion de réseaux avec contrôle d'accès

Cette catégorie d'interconnexion est apparue consécutivement au développement de l'Internet. L'Internet a d'abord été perçu comme un fantastique moyen de travail coopératif entre équipes de recherche universitaires et ensuite entre sociétés commerciales. Relativement aux lignes spécialisées, le coût d'interconnexion du réseau des réseaux est toujours très attractif. L'enthousiasme des premiers temps s'est très vite estompé face à la multiplication des comportements malveillants. Les modes d'interconnexion évoluent donc vers des fonctions de contrôle d'accès et de confidentialité dans les échanges.

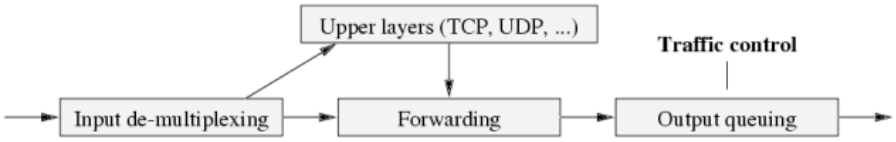
On reprend ici les éléments définis dans la définition du *Périmètre de contrôle d'accès*.

4.2.1. Définition du contrôle d'accès

La notion de contrôle d'accès regroupe plusieurs traitements :

- Le filtrage
- La qualité de service
- La traduction d'adresses

Ces traitements utilisent les mêmes composants du système.



Le document *Kernel Packet Traveling Diagram*[8] aide à distinguer les fonctions de contrôle de trafic des fonctions de filtrage.

Utilisation avec GNU/Linux

Le vocabulaire GNU/Linux parle de contrôle de trafic (*traffic control*) plutôt que de qualité de service. Le noyau Linux intègre un jeu de fonctions génériques utilisables pour tous les traitements. Voir la version française du *LARTC* : *HOWTO du routage avancé et du contrôle de trafic sous Linux*[9]

4.2.2. Contrôle de trafic avec Linux

Pour une introduction complète sur le fonctionnement du contrôle de trafic, consulter le document *Linux Traffic Control - Next Generation*[10].

Voici une présentation des composants systèmes extraite des documents de référence sur le contrôle de trafic.

Input de-multiplexing
: Les paquets entrants sont examinés pour être :
  - directement transmis au réseau ; sur une autre interface si la machine est un routeur ou un pont,
  - transférés vers les couches supérieures de la pile de protocole ; vers les protocoles UDP ou TCP de la couche transport.

Upper layers
: Les couches hautes peuvent aussi générer leurs propres données et les passer aux couches basses pour des traitements tels que l'encapsulation, le routage et éventuellement la transmission.

[8] http://www.docum.org/docum.org/kptd/
[9] http://www.linux-france.org/prj/inetdoc/guides/lartc/
[10] http://tcng.sourceforge.net/doc/tcng-overview.pdf

Forwarding
Ce composant comprend la sélection de l'interface de sortie, la sélection du prochain saut (pont, routeur ou commutateur), l'encapsulation, etc.

Output queueing
Une fois tous les traitements précédents effectués, c'est à ce niveau que le contrôle de trafic intervient.

Parmi les fonctions du contrôle de trafic, on trouve plusieurs types de décisions :

- Décision de mise en file d'attente (*queueing*) ou d'abandon d'un paquet si une limite de taille ou de débit a été atteinte.
- Décision sur l'ordre d'émission des paquets en fonction des priorités sur les types de flux.
- Décision sur le délai d'attente avant émission dans le cas où le débit de sortie a été limité.

Une fois que le contrôle de trafic a libéré un paquet pour qu'il soit émis, le pilote d'interface réseau le prend et l'envoie sur le réseau.

L'échange d'information sur le contrôle de trafic se fait par l'intermédiaire du marquage des paquets. Dans le cas des Services Différenciés (*Differentiated Services* [*Differentiated Services on Linux*[11]]) on utilise le champ TOS de l'en-tête de paquet IP ou un champ spécifique appelé *DS Field* spéficié par le document RFC2474 *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*[12].

Utilisation avec GNU/Linux

Les options de sélection des composants du contrôle de trafic implantés dans le noyau Linux sont accessibles à partir des options réseau. Le paquet iproute contient les outils utilisateurs de configuration.

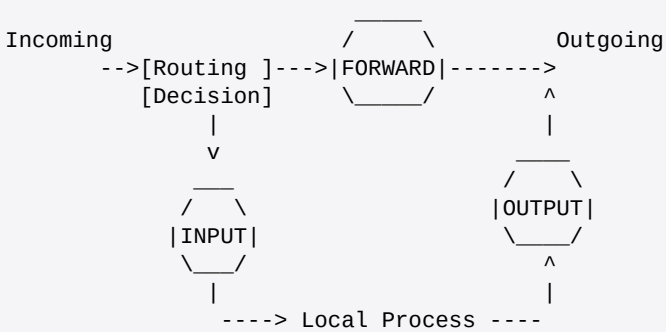
4.2.3. Le filtrage avec Linux

Le filtrage reprend l'utilisation des composants présentés ci-avant. Le rôle du filtrage n'est pas de mettre en forme le trafic réseau entre deux points mais de décider si un paquet doit être transmis ou non. Dans le cas du système GNU/Linux, le filtrage sert aussi à la traduction d'adresses. Il s'agit alors de décider vers quel hôte ou quel réseau un paquet doit être transmis.

Depuis l'origine, le filtrage sur les noyaux Linux est basé sur la notion de *chaîne*. Avant d'aborder les chaînes créées par l'utilisateur, un paquet doit toujours passer par au moins une des trois chaînes qui correspondent aux composants présentés ci-avant.

- INPUT pour les paquets entrant dans le système,
- FORWARD pour les paquets entrant et sortant du système,
- OUTPUT pour les paquets sortant du système.

Voici le synoptique fourni par Rusty Russel dans la section *Comment les paquets traversent les filtres*[13] du *Linux 2.4 Packet Filtering HOWTO*.



[11] http://diffserv.sourceforge.net/
[12] http://www.faqs.org/rfcs/rfc2474.html
[13] http://www.linux-france.org/prj/inetdoc/guides/packet-filtering-HOWTO/packet-filtering-HOWTO-6.html

```
      (c)2000 Rusty Russell
```

4.2.3.1. Les opérations de filtrage

Les traitements effectués sur les paquets à partir des trois chaînes de base sont eux-mêmes implantés sous forme de chaînes :

ACCEPT
: Le paquet est accepté et continue sa traversée du système.

DROP
: Le paquet est abandonné sans aucune notification.

LOG
: La traversée de la chaîne est enregistrée par le système.

REJECT
: Le paquet est rejeté avec notification.

RETURN
: Retour au traitement de la chaîne précédente.

QUEUE
: Le paquet est redirigé vers un traitement défini par l'utilisateur. Il s'agit avant tout de pouvoir ajouter de nouveaux traitements spécifiques.

4.2.3.2. Les spécifications de filtrage

Le filtrage s'applique en spécifiant les éléments suivants :

- Adresses IP source et/ou destination (ex. 192.168.100.2/24).
- Protocoles (ex. TCP, UDP, ICMP).
- Interface (ex. eth0).
- Fragments acceptés ou non.
- Extensions TCP sur les champs de l'en-tête (SYN, ACK, FIN, RST,URG, PSH) ainsi que sur les ports source et destination.
- Extensions UDP sur les ports source et destination.
- Extension ICMP sur le type.
- Adresses MAC source et/ou destination (ex. 00:60:08:91:CC:B7).
- Limite du nombre des demandes enregistrées par seconde (détection des attaques DoS et SYNflood).
- Propriétaire du paquet généré sur le système.

4.2.3.3. Suivi de communication (*stateful inspection*)

Cette fonction est essentielle pour tracer les échanges de de paquets pour chaque «communication» TCP, UDP et ICMP entre 2 hôtes. L'analyse est réalisée à l'aide d'indicateurs d'état (*State Match*).

NEW
: Le paquet crée une nouvelle connexion.

ESTABLISHED
: Le paquet appartient à une connexion existante.

RELATED
: Le paquet est associé à une connexion sans appartenance (ex. Erreur ICMP ou Donnée FTP).

INVALID
: Le paquet ne peut pas être identifié.

4.2.4. Comment utiliser le filtrage ?

Déterminer une politique de sécurité nécessite une réflexion approfondie. Il n'existe pas de solution «clé en main» en matière de sécurité réseau. Autre difficulté, il est extrêmement difficile de mesurer l'efficacité réelle d'une politique de sécurité (système de filtrage). On peut cependant dégager deux principes d'application du filtrage.

4.2.4.1. Deux principes d'application

Principe 1 : Tout ce qui n'est pas autorisé est interdit
: Cette approche est la plus rigoureuse. Seul le trafic réseau explicitement autorisé peut traverser l'équipement d'extrémité filtrant. De cette façon, on limite le trafic à surveiller (celui que l'on a autorisé) et on se protège contre les défauts de sécurité même inconnus.

Principe 2 : Tout ce qui n'est pas interdit est autorisé
: Cette approche interdit le trafic potentiellement dangereux. De cette façon, on ne limite que le trafic identifié comme générateur de problèmes de sécurité.

4.2.4.2. Où appliquer ces Principes ?

De façon pragmatique, on utilise les deux principes de filtrage en fonction de son niveau de «maîtrise» de l'interconnexion réseau. Suivant la distribution des périmètres on peut appliquer une hiérarchie dans la politique sécurité.

Plus le périmètre est petit, plus l'identification du trafic réseau est facile. Il est donc possible d'appliquer le premier principe, le plus rigoureux, sur les réseaux d'agence ou les périmètres départementaux. Ceci revient à dire qu'il faut appliquer le niveau de sécurité le plus élevé au plus près du réseau à protéger

A l'inverse, identifier la totalité des trafics possibles à l'échelle d'un périmètre d'interconnexion de campus est souvent une gageure. Le responsable de la sécurité réseau s'attirera les foudres de la quasi-totalité des utilisateurs s'il cherche à exercer un contrôle trop strict sur un trafic qu'il ne peut pas identifier complètement. En effet, trop de sécurité peut entraver le bon fonctionnement des applications dont les utilisateurs ont légitimement besoin. C'est donc le second principe qui convient le mieux aux réseaux d'interconnexion.

Chapitre 5. Quizz

1. Comment définir la frontière d'un périmètre d'intervention ?

La frontière d'un périmètre d'intervention est délimitée par le *Point Of Presence* (POP) de l'opérateur qui fournit l'accès au réseau public partagé.

2. Sur quels équipements doit-on appliquer les contrôles d'accès ?

Pour une efficacité optimale, les contrôles d'accès doivent être appliqués aux frontières : du réseau public au réseau écran puis du réseau écran au réseau privé.

3. Classer dans l'ordre d'entrée, la hiérarchie des contrôles d'accès : (1) Administration des services, (2) Filtrage de paquets et (3) Sélection des services ouverts.

Du réseau public au réseau privé, il faut traverser : (2) le filtrage de paquets, (3) la sélection des services ouverts et (1) l'administration des services.

4. Parmi les équipements suivants, quels sont ceux qui opèrent au niveau liaison de la modélisation OSI ? pont, hub, commutateur, routeur, répéteur.

pont et commutateur.

5. Parmi les équipements suivants, quels sont ceux qui opèrent au niveau réseau de la modélisation OSI ? pont, hub, commutateur, routeur, répéteur.

routeur.

6. Comment appelle-t-on le protocole d'interconnexion des segments réseau au niveau liaison ? VLAN, IEEE 802.1Q, Spanning Tree Protocol

C'est l'agorithme Spanning Tree Protocol qui permet l'interconnexion des segments de réseau au niveau liaison en construisant un «arbre» qui détermine un chemin unique entre 2 hôtes.

7. Quelles sont les principales limites des équipements d'interconnexion de niveau 2 sur un réseau de campus ?

Les équipements de niveau ne permettent pas d'assurer une balance de charge sur un réseau maillé. Le *Spanning Tree Protocol* impose un chemin unique entre 2 points.

8. Quel est le niveau d'interconnexion qui permet d'assurer une répartition du trafic réseau sur plusieurs liens redondants ?

L'interconnexion au niveau réseau (couche 3) du modèle OSI assure un contrôle de flux et détermine le meilleur chemin entre 2 points à l'aide des protocoles de routage.

9. Quel type d'équipement d'interconnexion de niveau 3 est-il préférable d'utiliser à partir d'une ligne spécialisée longue distance ?

Compte tenu du débit limité (< à 10Mbps) d'une liaison spécialisée, un routeur traditionnel convient parfaitement pour interconnecter un réseau local.

10. Il existe 2 philosophies d'application du contrôle d'accès par filtrage. Quel est le mode le plus approprié aux équipements SOHO (routeurs d'agences) ?

Tout ce qui n'est pas autorisé est interdit. Comme le réseau privé desservi par un routeur d'agence est de taille limitée, il est facile de constituer une liste exhaustive des ports/services ouverts.