Interconnexion réseau & Logiciel Libre

Serveur d'accès - Routeur d'agence

Philippe Latu
Chargé de mission Systèmes & Réseaux
IUT 'A' Paul Sabatier

philippe.latu@iut-tlse3.fr

Laurent Foucher
Administrateur Système
IUT 'A' Paul Sabatier

foucher@gch.iut-tlse3.fr

Interconnexion réseau & Logiciel Libre: Serveur d’accès - Routeur d’agence
par Philippe Latu et Laurent Foucher

Ce programme est destiné aux étudiants d’IUP *Systèmes de Télécommunication et Réseaux Informatiques* (STRI). Il a pour but de mettre en oeuvre deux scénarii d’interconnexion types : *Serveur d’accès* (NAS) et *Routeur d’agence* (SOHO).

Copyright et Licence

Historique des versions
Version $Revision: 1.4 $ $Date: 2001/11/05 22:43:12 $ Revu par : PL
Edition 2001

Table des matières

Liste des tableaux

Liste des exemples

Introduction au programme

1. Meta-information sur ce support

Cet article est écrit en *DocBook* (http://www.dodcbook.org) SGML sur un système *Debian* (http://www.debian.org). Il est téléchargeable à partir du site *GNU/Linux inetdoc* (http://www.linux-france.org/prj/inetdoc/download) aux formats PDF (http://www.linux-france.org/prj/inetdoc/download/inet1.pdf) et Postscript compressé (http://www.linux-france.org/prj/inetdoc/download/inet1.ps.gz).

2. Les prérequis

Ce programme est une introduction à l'interconnexion réseau. Il suit le cours *Configuration et dépannage d'une connexion réseau* (http://www.linux-france.org/prj/inetdoc/courses/minidep/) et suppose que l'on sache effectuer les opérations de base sur la configuration d'une interface réseau individuelle. De plus, il faut connaître un minimum de commandes Unix pour accéder aux outils du système GNU/Linux. Il est conseillé de suivre le programme *Exploration GNU/Linux* (http://www.linux-france.org/prj/inetdoc/courses/explore/) pour acquérir les bases système avant d'aborder l'interconnexion.

3. Les objectifs

Les objectifs de ce programme sont de deux ordres : techniques et méthodologiques.

3.1. Technique

Le premier objectif technique est de mettre en oeuvre deux scénarii types : « Serveur d'accès » (NAS : *Network Access server*) et « Routeur d'agence » (SOHO : *Small Office Home Office*). Dans les deux cas, il s'agit d'interconnecter un réseau grande distance téléphonique (WAN/RNIS) et un réseau local (LAN/Ethernet). De cette façon on illustre les deux grands modes d'exploitation des réseaux : le mode connecté en téléphonie et le mode diffusion d'Ethernet.

Le second objectif est l'introduction au contrôle d'accès. Dans ce but, on introduit la classification par périmètre puis les outils de contrôle de services et d'accès.

3.2. Méthode

L'exploitation de documentation en ligne est un objectif largement aussi important que les précédents. Compte tenu de la quantité de notions à appréhender et du volume de documents disponibles, il est indispensable de savoir rechercher, trier et analyser des documents en ligne. La capacité d'un individu à concevoir et exploiter une infrastructure réseau est conditionnée par son aptitude à utiliser tous les types de supports documentaires en ligne.

3.3. Logiciel libre

Le choix du système libre GNU/Linux pour les applications de ce programme n'est pas gratuit. GNU/Linux comprend à la fois un système d'interconnexion très performant et le code original des services Internet. Les fonctions réseau du noyau Linux permettent d'illustrer des techniques difficiles d'accès avec les systèmes propriétaires. Les logiciels des services qui fonctionnent avec GNU/Linux dominent l'Internet sans contestation possible. Enfin, les mécanismes de filtrage, de contrôle d'accès et de qualités de services réseau sont à la pointe de l'innovation.

L'argumentation à caractère « marketing » ci-dessus est nécessaire puisque le Logiciel Libre ne bénéficie pas de la même promotion que les systèmes propriétaires. Pour aller au delà, il faut rappeler que le Logiciel Libre est avant tout une solution alternative. Dans le cadre d'un cursus de formation initiale, il est important d'étudier des solutions alternatives. Dans un domaine où on ne fait souvent référence qu'au « leader mondial », le Logiciel Libre est un excellent moyen pour développer une analyse critique entre plusieurs solutions.

4. Le déroulement

Comme indiqué ci-avant, le programme comprend des cours et des travaux pratiques. Les cours introduisent à la fois les concepts et les outils à utiliser lors des travaux pratiques.

4.1. Support de Cours Réseau

Conception d'une interconnexion réseau.

Architecture réseau

: Classification, périmètres et modes de connexion.

Interconnexion réseau

: Techniques de transmission entre réseaux et contrôle d'accès.

Technologie RNIS

: Avantages des connexions RNIS dans l'interconnexion des réseaux et référence au *Guide RNIS Linux* (http://www.linux-france.org/prj/inetdoc/guides/rnis/).

4.2. Support de Cours linux

Configuration des fonctions réseau du système GNU/Linux.

Présentation du noyau Linux

: Qu'est-ce qu'un noyau, ses fonctions, la répartition *kernelspace*, *userspace*, rôle et avantages des modules.

Les technologies réseau du noyau Linux

: Les types d'interfaces, les fonctions des niveaux réseau et liaison, le filtrage, le sous-système RNIS et la compilation du noyau.

Les outils réseau du noyau Linux

Outils de configuration des interfaces et du contrôle d'accès.

4.3. Support de Travaux Pratiques

Mise en oeuvre d'une interconnexion entre un réseau grandes distances (WAN) de type RNIS et un réseau local (LAN) de type Ethernet.

Système d'interconnexion

Avant de lancer la transmission des informations d'un réseau sur l'autre, il faut maîtriser les fonctions et services actifs sur le routeur. On commence par la configuration de la connexion au réseau local pour des raisons pratiques d'accès à la documentation et aux sources du noyau.

On construit ensuite un noyau Linux adapté aux besoins du routeur en étudiant les rubriques: **Networking options+Network device support+ISDN subsystem**.

Enfin, on vérifie le chargement des modules pilotes des interfaces réseau et on sélectionne les services qui seront actifs lors du routage.

Sous-système RNIS

Il s'agit ici de configurer correctement une connexion RNIS. Il faut donc choisir les protocoles et leurs encapsulations pour se connecter en accès direct (*rawip*) puis en utilisant le protocole PPP. La mise au point se fait en analysant les différentes sources de messages : noyau, sous-système RNIS, pilote matériel *HiSax*.

Serveur d'accès (NAS)

Dans ce scénario, le routeur dispose d'un accès haut débit avec son interface Ethernet et doit fournir un accès à Internet par son interface RNIS. On modélise ainsi le fonctionnement des équipements utilisés par les fournisseurs d'accès Internet (FAI/ISP). En plus de la dénomination *Network Access Sever*, on utilise aussi l'appelation « serveur d'appels » (*Dialin Server*).

Routeur d'agence (SOHO)

Dans ce scénario, le routeur accède à Internet par son interface RNIS et redistribue cet accès sur un réseau local. Ce genre de routeur est appelé « routeur d'agence ». Il fait partie de la catégorie d'équipement SOHO, *Small Office Home Office*.

Important : Lors des deux premières séances de travaux pratiques tous les postes utilisent la même configuration. Pour les deux autres séances, une moitié des postes utilise le scénario *Serveur d'accès* et l'autre moitié utilise le scénario *Routeur d'agence*.

5. Les conditions de fonctionnement

5.1. Obtenir les documents

La totalité des documents nécessaires à ce programme de formation sont disponibles sous 3 formats :

- HTML (http://www.linux-france.org/prj/inetdoc/courses/inet1/) pour la consultation en ligne.
- Postscript compressé (http://www.linux-france.org/prj/inetdoc/download/inet1.ps.gz) pour l'impression papier.
- PDF (http://www.linux-france.org/prj/inetdoc/download/inet1.pdf) pour la consultation hors ligne.

Sources de documentation

Projet GNU/Linux inetdoc (http://www.linux-france.org/prj/inetdoc)

- Le présent document est accessible à la rubrique **Cours**⟶**Services réseau & Interconnexion RNIS/Ethernet**.
- Le document sur la configuration et le dépannage d'une interface réseau est accessible à la rubrique **Cours**⟶**Connexion à un réseau local : configuration et dépannage**.
- Les articles de référence sur les technologies réseau sont accessibles à la rubrique **Articles**.

man pages

Les pages de manuel ou *man pages* donnent les options des commandes Unix. Les paquetage `manpages` et `manpages-fr` doivent être installés sur chacun des postes de Travaux Pratiques. Par exemple, on entre à la console **`man ifconfig`** pour connaître les options de la commande **ifconfig**.

HOWTOs

Les *HOWTOs* sont accessibles en ligne à partir du site Linux Documentation Project (http://www.linuxdoc.org) (LDP). Pour obtenir la liste des sujets traités, consulter le HOWTO-INDEX (http://www.linuxdoc.org/HOWTO/HOWTO-INDEX/howtos.html). Ces documents *HOWTOs* sont aussi fournis en paquetages installés sur les postes de travaux pratiques. Ainsi lorsque la connexion Internet est « perdue » on les consulte à partir du répertoire : `/usr/doc/HOWTO/`. Les paquetages `doc-linux-html` et `doc-linux-fr` doivent être installés sur chacun des postes de Travaux Pratiques.

Autres sources

Les autres sources de documentation sont principalement alimentées par les constructeurs d'équipement réseau. 3Com® (http://www.3com.com) et CISCO® (http://www.cisco.com) sont 2 exemples représentatifs.

5.2. Le poste de travaux pratiques

Chaque binôme d'étudiants dispose d'un PC équipé d'une carte RNIS BeWAN/Gazel® R753 et d'une carte Ethernet 3Com® 3C905B-TX. La seule précaution particulière à prendre consiste à ne pas confondre les cordons de brassage RNIS et Ethernet. En effet, les bus S0 sont alimentés avec une tension de 40V par le commutateur téléphonique.

Une distribution Debian (http://www.debian.org) est installée sur chaqueposte de Travaux Pratiques sans configuration réseau.

I. Support de Cours Réseau

Table des matières

Historique des versions

Version $Revision: 1.2 $ $Date: 2001/10/14 19:05:57 $
Edition 2001

Conception d’une interconnexion réseau.

Chapitre 1. Architecture Réseau

La conception d'une architecture réseau est un problème très vaste. L'objectif de ce chapitre est de donner les éléments de conception nécessaires aux deux scénarii : *Serveur d'accès* et *Routeur d'agence* utilisés pour les travaux pratiques. Pour satisfaire 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.

1.1. 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 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.

1.1.1. 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.

1.1.2. Périmètre de diffusion

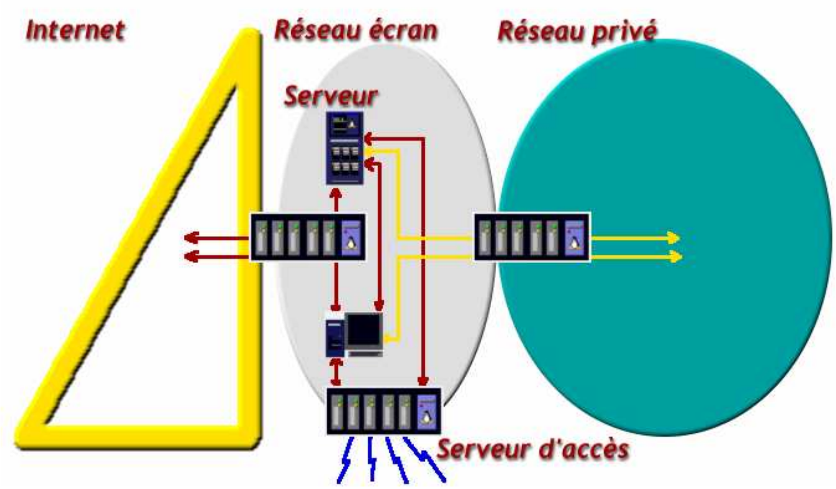
C'est la définition « historique » de l'interconnexion de réseaux. Dès qu'il y a routage, on crée deux périmètres ou domaines de diffusion [Segmentation].

1.1.3. 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.



1.1.3.1. 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 : *Quality of Service* [Policy Terms]) se définit au moins à deux niveaux :

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 *Integrated Services* [RFC1633] et services différenciés *Differentiated Services*. La signalisation est assurée par le protocole RSVP [RFC2205] pour les services intégrés et par le protocole DiffServ [RFC2475] 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 » qui les impose aux limites d'un périmètre. On parle de *routing policies*.