Possibilités réseau de Linux HOWTO

Daniel López Ridruejo, *ridruejo@esi.us.es*
Traduction française : Mathieu Arnold, *arn_mat@club-internet.fr* v0.31, 17 Septembre 1999

Le but de ce document est de donner une vue d'ensemble des possibilités réseau du système d'exploitation Linux et de donner des adresses pour de plus amples informations.

Table des matières

1 Introduction

Le but de ce document est de donner une idée des possibilités réseau du système d'exploitation Linux. De plus, une des grandes forces de Linux est qu'il est possible de trouver des tonnes d'informations sur presque tous les sujets, et la majorité de ces informations concernent surtout la manière dont les choses sont implémentées. La plupart des nouveaux utilisateurs de Linux, particulièrement ceux qui arrivent d'un environnement Windows, ne savent rien des possibilités réseau de Linux. Ce document a donc pour but de donner une vue d'ensemble de toutes ces possibilités avec une petite description pour chacune et des adresses pour aller chercher d'autres informations. Les informations ont été récoltées à partir de nombreuses sources : HowTos, faqs, pages web de projets et ma propre expérience. Tous les auteurs de ces documents sont cités. Sans eux, et sans leurs programmes, ce document n'aurait pas été possible, ni nécessaire.

2 Linux.

2.1 Qu'est ce que Linux ?

L'auteur principal de Linux est Linus Torvalds. Depuis la première version, ce système a été amélioré par un nombre impressionnant de personnes. C'est un clone, écrit à partir de rien, du système d'exploitation Unix. Le plus intéressant à propos de Linux, c'est que son développement se fait simultanément tout autour du monde.

Linux est protégé par la Licence GNU (GPL). Cette licence a été écrite par la Free Software Foundation (FSF), elle est faite pour empêcher les gens de restreindre la distribution des logiciels. En gros, ça dit que bien que l'on puisse demander de l'argent pour la distribution, la personne qui a reçu la copie a le droit de la redistribuer gratuitement. Cela dit aussi que le code source doit être disponible. C'est très utile pour les programmeurs. N'importe qui peut modifier Linux et même distribuer ses modifications, tant que le code reste dans le même copyright.

2.2 Qu'est ce qui fait que Linux est différent ?

Pourquoi travailler sur Linux ? Linux est généralement moins cher (ou du moins pas plus cher) que les autres systèmes d'exploitation, et crée fréquemment moins de problèmes que les systèmes commerciaux. Mais ce qui fait que Linux est différent n'est pas le prix (après tout, pourquoi voudrait-on d'un système - même s'il est gratuit - s'il n'est pas bien ?), mais ses étonnantes capacités :

- Linux est un vrai système d'exploitation multitâche 32 bits, suffisamment solide et puissant pour être utilisé depuis les universités jusque dans les grandes entreprises.
- Il fonctionne sur un nombre impressionnant de machines, depuis les 386 bas de gamme, jusqu'aux machines massivement parallèles des centres de recherches.
- Il y a des versions disponibles pour les architectures Intel, Sparc et Alpha, et un support expérimental des Power PC et des systèmes embarqués, tels SGI, Ultra Sparc, AP1000+, Strong ARM, MIPS R3000/R4000.

– Finalement, quand on arrive à la partie réseau, Linux est "le" choix ; non seulement parce que la couche réseau est profondément intégrée dans le système, ainsi qu'à cause du nombre impressionnant d'applications disponibles, mais aussi grâce à sa robustesse lorsque le système est très chargé, chose qui ne peut être accomplie dans un tel projet qu'après des années de débuggage et de tests.

3 Protocoles réseau

Linux supporte beaucoup de protocoles réseau différents :

3.1 TCP/IP

Le protocole internet (IP) a été conçu à l'origine, il y a une vingtaine d'années, pour le département de la défense des États Unis (DoD), avec pour but principal de pouvoir connecter des ordinateurs de différentes marques. La suite de protocoles TCP/IP a permis, grâce à sa structure en couches, d'isoler les applications de la couche réseau matérielle.

De plus, ce modèle en couches est plus tourné vers les possibilités d'interconnections que vers la rigidité de couches fonctionnelles. C'est d'ailleurs pour cette raison que TCP/IP est devenu le standard international inter réseau et non pas ISO.

TCP/IP est présent dans Linux depuis ses débuts. Son implémentation est partie de rien. Il fait partie des implémentations les plus robustes, rapides et fiables et c'est d'ailleurs un facteur clé du succès de Linux.

HowTo : *http ://metalab.unc.edu/mdw/HOWTO/NET34HOWTO.html*

3.2 TCP/IP version 6

IPv6, aussi connu sous le nom de IPng (IP Next Generation) est une mise à jour du protocole IPv4 pour régler les problèmes liés aux adresses. Ces problèmes incluent : manque d'adresses IP, manque de mécanismes pour gérer le trafic prioritaire, manque d'une couche de sécurité...

Le plus grand espace d'adresses IP s'accompagnera d'un version plus élaborée des tables d'adressage , ce qui aura un gros impact sur les performances de routage. Une implémentation bêta existe déjà pour Linux, et une version stable est attendue pour la version 2.2.0 du noyau.

– Le HowTo Linux IPv6 : *http ://www.terra.net/ipv6/*
– La page de départ d'IPv6 : *http ://playground.sun.com/pub/ipng/html/ipng-main.html*

3.3 IPX/SPX

IPX/SPX (Internet Packet Exchange/Sequenced Packet Exchange) est un protocole propriétaire développé par Novell et basé sur le Xerox Nework System (XNS). IPX/SPX était très utilisé au début des années 1980 en tant que partie intégrante de Novell NetWare. NetWare est par conséquent devenu le standard des systèmes d'exploitation réseau des LANs de première génération. Novell a amélioré son système avec des applications orientées business et des utilitaires de connections.

Linux a une implémentation très propre de IPX/SPX, permettant d'être configuré en tant que :

– Routeur IPX
– Pont IPX
– Client NCP et/ou serveur NCP (pour partager des fichiers)
– Client et Serveur d'impression Novell

Et de :

- Permettre PPP/IPX : une machine Linux de servir de client/serveur PPP
- Faire du tunnelling IPX à travers IP, permettant la connexion de deux réseaux IPX via un lien IP

En plus, *Caldera* <http://www.caldera.com> offre un support commercial pour Novell NetWare sous Linux. Caldera vend un client Novell NetWare complet basé sur une technologie achetée à Novell Corporation. Ce client fournit un accès complet aux serveurs de fichiers Novell 3.x et 4.x et inclut des trucs comme NetWare Directory Service (NDS) et le cryptage RSA.

- Le HowTo IPX : *http ://metalab.unc.edu/mdw/HOWTO/IPX-HOWTO.html*

3.4 Le protocole AppleTalk

AppleTalk est le nom de la pile réseau d'Apple. Elle permet des liaisons postes à postes, ce qui offre les fonctions de base telles que le partage de fichiers ou d'imprimantes. Chaque machine peut agir simultanément en tant que client et serveur. Les logiciels et le matériel sont inclus dans chaque ordinateur Apple.

Linux fournit une pile réseau AppleTalk complète. Netatalk, le port Linux d'AppleTalk, est implémenté au niveau du noyau, et provient de systèmes dérivés de BSD. Il inclut le support pour router l'AppleTalk, partager les systèmes de fichiers Unix et AFS via AFP (AppleShare), partager les imprimantes Unix et les imprimantes AppleTalk via PAP.

Aller voir la section 5.1 pour plus de renseignements.

3.5 Réseaux WAN : X.25, Frame-relay, etc...

Certains fournissent des produits T-1, T-3, X.25 et Frame Relay pour Linux. Généralement un matériel spécifique est nécessaire pour ce type de connections. Ceux qui vendent le matériel vendent aussi les drivers avec support du protocole.

- Ressources WAN pour Linux : *http ://www.secretagent.com/networking/wan.html*

3.6 RNIS

Le noyau de Linux a des capacités RNIS intégrées. Isdn4linux contrôle les cartes RNIS des PC et peut émuler un modem avec des commandes Hayes (commandes "AT"). Les possibilités vont de l'utilisation d'une connection type terminal via HDLC (utilisant les périphériques inclus), jusqu'à une connection Internet complète avec les possibilités PPP/Sons.

- FAQ pour isdn4linux : *http ://www.lrz-muenchen.de/~ui161ab/www/isdn/faq_ e.html*

3.7 PPP, SLIP, PLIP

Le noyau de Linux a un support intégré pour PPP (Point-to-Point-Protocol), SLIP (Serial Line IP) et PLIP (Parallel Line IP). PPP est la manière la plus populaire pour les utilisateurs individuels de se connecter à leurs FAI (Fournisseurs d'Accès Internet). PLIP permet des connections faciles entre deux machines. Il utilise un port parallèle et un câble spécial, atteignant des vitesses de 10kBps à 20kBps.

- Le *Linux PPP Howto* <http://metalab.unc.edu/mdw/HOWTO/PPP-HOWTO.html>
- L'*émulateur PPP/SLIP* <http://metalab.unc.edu/mdw/HOWTO/mini/SLIP-PPP-Emulator.html>
- Des informations complémentaires peuvent être trouvées dans *The Network Administrator Guide* <http://metalab.unc.edu/mdw/LDP/nag/nag.html>

3.8 Radio Amateur

Le noyau de Linux possède un support intégré pour les protocoles de radio amateur.

Un point intéressant est le support AX.25. Le protocole AX.25 offre des possibilités d'opérations avec ou sans connections, et est même utilisé par lui-même pour des connections d'un point à un autre, ou pour transporter d'autres protocoles tels TCP/IP ou NetRom.

Il est similaire au X.25 niveau 2 de par sa structure, avec quelques extensions qui le rendent plus utile pour l'environnement radio amateur.

– *Amateur radio how-to* `<http://metalab.unc.edu/mdw/HOWTO/HAM-HOWTO.html>`

3.9 ATM

Le support ATM de Linux en est en ce moment au stade pré-alpha. C'est une distribution expérimentale, qui supporte les connections ATM raw (PVC et SVC), IP via ATM, émulation LAN...

– *La page de l'ATM pour Linux* `<http://lrcwww.epfl.ch/linux-atm/>`

4 Matériel réseau supporté

Linux supporte une très grande variété de matériel réseau, certains même obsolètes.

Quelques documents intéressants :
– Le *Hardware How-To* `<http://metalab.unc.edu/mdw/HOWTO/Hardware-HOWTO.html>`
– L'*Ethernet How-To* `<http://metalab.unc.edu/mdw/HOWTO/Ethernet-HOWTO.html>`

5 Partage de fichiers et d'imprimantes

Le premier but de la majorité des réseaux locaux (LAN) basés sur des PC est de fournir un service de partage de fichiers et d'imprimantes aux utilisateurs. Linux en tant que serveur de fichiers et d'imprimantes pour l'entreprise apparaît comme une excellente solution.

5.1 Environnement Apple

Comme il a été souligné dans les sections précédentes, Linux supporte la famille de protocoles Appletalk. Le netatalk de Linux permet à un client Macintosh de voir les systèmes Linux comme des autres Macintosh sur le réseau, de partager les fichiers, et d'utiliser les imprimantes connectées aux serveurs Linux.

La FAQ de Netatalk et son HowTo :
– *http ://thehamptons.com/anders/netatalk/*
– *http ://www.umich.edu/˜rsug/netatalk/*
– *http ://www.umich.edu/˜rsug/netatalk/faq.html*

5.2 Environnement Windows

Samba est une suite logicielle qui permet à la majorité des Unix (et en particulier Linux) de s'intégrer à un réseau Microsoft en tant que client et serveur. En tant que serveur, il permet aux clients Windows 95, Windows pour Workgroups, DOS et Windows NT d'accéder aux fichiers et aux imprimantes de la machine Linux. Il peut remplacer complètement Windows NT pour le partage de fichiers et les services d'impression, incluant le chargement automatique des pilotes d'impression par les clients. En tant que client, la station Linux est capable de monter des systèmes de fichiers exportés par d'autres machines.

D'après la Meta-FAQ SAMBA :

```
"Beaucoup d'utilisateurs ont déclaré qu'en comparaison avec d'autres
implémentations SMB, Samba est plus stable, plus rapide, et compatible avec
plus de clients. Les administrateurs de grosses installations disent que Samba
est le seul serveur SMB disponible qui peut servir plusieurs dizaines de
milliers d'utilisateurs sans planter."
```

– La *Page du projet Samba* <http://samba.anu.edu.au/samba/>
– Le *HowTo Samba* <http://metalab.unc.edu/mdw/HOWTO/SMB-HOWTO.html>
– Le *Printing How-to* <http://metalab.unc.edu/mdw/HOWTO/Printing-HOWTO.html>

5.3 Environnement Novell

Comme il a été dit dans les sections précédentes, Linux peut être configuré en tant que client ou serveur NCP, et donc, permettre l'accès à ses fichiers et ses imprimantes à travers un réseau Novell, aussi bien pour les clients Novell que pour les clients Unix.

– Le *HowTo IPX* <http://metalab.unc.edu/mdw/HOWTO/IPX-HOWTO.html>

5.4 Environnements Unix

La façon la plus simple de partager les fichiers dans un réseau Unix est d'utiliser NFS. NFS signifie Network File Sharing, c'est à dire, partage de fichiers en réseau ; son protocole a été développé à l'origine par la société Sun Microsystems. C'est un moyen simple de partager des fichiers entre les machines comme s'ils étaient locaux. Un client "monte" un système de fichier "exporté" par un serveur NFS. Le système de fichier monté apparaîtra au client comme s'il faisait partie du système de fichier local.

Il est possible de monter un système de fichier racine au démarrage, permettant ainsi à des clients sans disque de démarrer et d'accéder à tous les fichiers du serveur. En d'autres termes, il est possible d'avoir un ordinateur pleinement fonctionnel bien que n'ayant pas de disque.

Coda est un système de fichier en réseaux (comme NFS) qui supporte le fait d'être déconnecté, du cache persistant, entre autres choses. Il est inclus dans les noyaux 2.2. Il est très pratique pour les réseaux lents ou peu fiables, et pour les ordinateurs portables.

Document en rapport avec NFS :
– *http ://metalab.unc.edu/mdw/HOWTO/mini/NFS-Root.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Diskless.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/NFS-Root-Client.html*
– *http ://www.redhat.com/support/docs/rhl/NFS-Tips/NFS-Tips.html*
– *http ://metalab.unc.edu/mdw/HOWTO/NFS-HOWTO.html*
CODA se trouve à : *http ://www.coda.cs.cmu.edu/*

6 Internet/Intranet

Linux est une très bonne plate-forme pour agir en tant que serveur Internet / Intranet. Le terme Intranet se réfère à l'application des technologies d'Internet au sein d'une entreprise pour la diffusion d'informations dans l'entreprise. Les services Internet et Intranet offerts par Linux incluent Mail, News, serveur WWW, et bien plus encore qui seront détaillés dans les sections suivantes.

6.1 Mail

6.1.1 Serveurs de Mail

Sendmail est de facto, le serveur de mail standard (appelé MTA pour Mail Transport Agents) pour les plate-formes UNIX. Il est robuste, extensible, et proprement configuré avec le matériel nécessaire, peut supporter une charge de plusieurs milliers d'utilisateurs sans ciller. D'autres serveurs de mails existent, comme smail, qmail ou postfix qui sont des produits de remplacement pour sendmail.

– Le *Site de Sendmail* `<http://www.sendmail.org/>`
– La *FAQ de Smail* `<http://www.sbay.org/smail-faq.html>`
– Le *Site de Qmail* `<http://www.qmail.org>`
– Le *Site de Postfix* `<http://www.postfix.org>`

HowTo Mail :

– *http ://metalab.unc.edu/mdw/HOWTO/Mail-HOWTO.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Qmail+MH.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Sendmail+UUCP.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Mail-Queue.html*

6.1.2 Accès distant aux mails

Dans une entreprise ou chez un FAI, les utilisateurs accéderont à leur boite à lettres électronique depuis leur bureau. Plusieurs alternatives existent sous Linux, incluant des serveurs POP (Post Office Protocol) et IMAP (Internet Message Access Protocol). Le protocole POP est généralement utilisé pour transférer les messages du serveur au client. IMAP permet la manipulation des messages sur le serveur, création et suppression à distance de répertoires sur le serveur, accès à des dossiers de mails partagés, etc.

– *Brève comparaison de IMAP et POP* `<http://www.imap.org/imap.vs.pop.brief.html>`

HowTo en rapports avec le courrier électronique :
– *http ://metalab.unc.edu/mdw/HOWTO/Mail-HOWTO.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Cyrus-IMAP.html*

6.1.3 Lecteurs de Mail

Il y a un bon nombre de lecteurs de mail sous Linux, soit en mode graphique, soit en mode texte. Les plus utilisés sont pine, elm, mutt et Netscape.

– *Liste des logiciels en rapport avec le courrier électronique* `<http://www.linuxlinks.com/Software/Internet/Mail/>`
– *http ://metalab.unc.edu/mdw/HOWTO/mini/TkRat.html*

6.1.4 Logiciels de liste de diffusion

Il y a beaucoup de programmes de gestion de listes de diffusion disponibles pour UNIX en général et pour Linux en particulier.

– Une bonne comparaison des gestionnaires de listes peut être trouvé à : *ftp ://ftp.uu.net/usenet/news.answers/mail/list-admin/*
– *Listserv* `<http://www.lsoft.com/>`
– *Majordomo* `<http://www.greatcircle.com/majordomo/>`
– *Sympa* `<http://listes.cru.fr/sympa/>`

6.1.5 Fetchmail

L'un des utilitaires très pratique pour la gestion du courrier électronique est fetchmail. Fetchmail est un programme de récupération et de reroutage de mails gratuit, robuste, complet et très bien documenté, fait pour être utilisé avec une connection TCP/IP à la demande (comme des connections SLIP ou PPP). Il supporte tous les protocoles de mail distants en vigueur de nos jours sur Internet. Il supporte même IPv6 et IP-SEC.

Fetchmail récupère les mails depuis des serveurs de mails distants et les reroute via SMTP, par conséquent, ils peuvent être normalement lus par des clients mails normaux tels mutt, elm ou BSD Mail. Il permet à tous les systèmes de filtrage, de reroutage et d'aliasing des serveurs mail de fonctionner comme s'il s'agissait de mails normaux.

Fetchmail peut être utilisé en tant que passerelle POP/IMAP-vers-SMTP pour un domaine DNS entier, récupérant les mails d'une seule boite aux lettres chez le FAI, et transférant le tout en se basant sur les en-têtes.

Une petite entreprise peut centraliser tous ses comptes mails dans une seule boite, configurer fetchmail pour récupérer tous les mails en partance, les envoyer via une simple boite aux lettres chez le FAI et récupérer les messages arrivant de la même boite aux lettres .
– La *page de Fetchmail* `<http://sagan.earthspace.net/~esr/fetchmail/>`

6.2 Serveurs Web

La majorité des distributions Linux incluent *Apache* `<http://www.apache.org>`. D'après *http ://www.netcraft.co.uk/survey/* Apache est le premier serveur Web sur internet, plus de la moitié des sites internet utilisent Apache, ou un de ses dérivés. Les avantages d'Apache incluent sa conception modulaire, sa stabilité, et sa vitesse. Avec une configuration appropriée et un matériel adéquat, il peut supporter les plus grosses charges : Yahoo, Altavista, GeoCities, Hotmail sont basés sur des versions customisées de ce serveur.

Un support optionnel des SSL (qui permettent des transactions cryptées) est aussi disponible à :
– *http ://www.apache-ssl.org/*
– *http ://raven.covalent.net/*
– *http ://www.c2.net/*
HowTo en relation :
– *http ://metalab.unc.edu/mdw/HOWTO/WWW-HOWTO.html*
– *http ://metalab.unc.edu/mdw/HOWTO/Virtual-Services-HOWTO.html*
– *http ://metalab.unc.edu/mdw/HOWTO/Intranet-Server-HOWTO.html*
– *Serveurs Web pour Linux* `<http://www.linuxlinks.com/Software/Internet/WebServers/>`

6.3 Navigateurs Web

Un bon nombre de navigateurs WWW existent pour les plate-formes Linux. Netscape Navigator est l'un des choix depuis le début, le tres attendu *Mozilla* `<http://www.mozilla.org>` aura une version Linux. Un autre navigateur en mode texte populaire est lynx. Il est rapide et pratique quand aucun environnement graphique n'est disponible.

– *Navigateurs pour Linux* `<http://www.linuxlinks.com/Software/Internet/WebBrowsers/>`
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Public-Web-Browser.html*

6.4 Serveurs et clients FTP

FTP signifie File Transfer Protocol, protocole de transfert de fichier. Un serveur FTP permet aux clients de se connecter et de récupérer des fichiers. Il y a beaucoup de clients et de serveurs FTP qui existent pour Linux et sont inclus dans les distributions. Il y a des clients en mode texte ainsi que des clients avec une interface graphique. Les logiciels en rapport avec le FTP peuvent être trouvés à : *http ://metalab.unc.edu/pub/Linux/system/network/file-transfer/*

6.5 Services de News

Usenet (aussi appelé news) est un énorme BBS qui couvre tous les sujets possibles et qui est organisé hiérarchiquement. Un réseau d'ordinateurs au travers d'Internet (Usenet) échange des articles grâce au protocole NNTP. Plusieurs implémentations existent pour Linux, que ce soit pour un site très chargé ou un petit site recevant peu de groupes.

– La *page de INN* `<http://www.isc.org/>`
– Les *logiciels en rapport avec les news* `<http://www.linuxlinks.com/Software/Internet/News/>`

6.6 Noms de domaines (DNS)

Un serveur DNS a pour tâche de traduire les noms (compréhensibles par les humains) en adresses IP. Un serveur de DNS ne connaît pas toutes les adresses IP du monde, mais, il est capable de demander à un autre serveur une adresse inconnue. Le serveur de DNS retournera alors, soit l'IP demandée, ou répondra qu'il ne trouve pas ce nom dans ses tables.

Les serveurs de noms sous Unix (et majoritairement sur Internet) sont gérés par un programme appelé named. Il fait partie du paquetage bind de l'Internet Software Consortium.
– *BIND* `<http://www.isc.org/>`
– Le *HowTo DNS* `<http://metalab.unc.edu/mdw/HOWTO/DNS-HOWTO.html>`

6.7 DHCP, bootp

DHCP et bootp sont des protocoles qui permettent à une machine cliente d'obtenir des informations sur le réseau (comme son adresse IP) depuis un serveur. Beaucoup d'entreprises commencent à l'utiliser car cela rend plus facile l'administration des réseaux, spécialement dans les cas de grands réseaux ou de réseaux avec beaucoup d'utilisateurs mobiles.

Documents en relation :

– Le *HowTo DHCP* `<http://metalab.unc.edu/mdw/HOWTO/mini/DHCP.html>`

6.8 NIS

NIS est l'abréviation de Service d'Information Réseau (Network Information Service). Il fournit un simple service de consultation comprenant bases de données et processus. Son objectif est de fournir des informations qui doivent être connues à travers le réseau par toutes les machines qui s'y trouvent. Les informations distribuées par NIS sont :

– nom de login, mots de passe, répertoires parents (`/etc/passwd`) ;
– renseignements sur le groupe d'utilisateurs (`/etc/group`).

Par exemple, si votre mot de passe est enregistré dans la base de données NIS, vous pourrez vous loger sur n'importe quelle machine située sur le réseau qui possède les clients NIS.

HowTo en relation :
– *NIS How-to* <http://metalab.unc.edu/mdw/HOWTO/NIS-HOWTO.html>

6.9 Authentification

Il y a aussi plusieurs méthodes pour authentifier des utilisateurs dans un réseau hétérogène.

– Pour Linux/Windows NT : *http ://www.mindware.com.au/ftp/smb-NT-verify.1.1.tar.gz.*
– PAM (pluggable authentication module) qui est une méthode flexible d'authentification sous UNIX : *librairie PAM* <http://www.kernel.org/pub/linux/libs/pam/index.html>.
– Et enfin, *LDAP pour Linux* <http://www.umich.edu/~dirsvcs/ldap/index.html>

7 Exécution d'applications à distance

L'une des plus folles fonctionnalités d'UNIX (et pourtant une des plus méconnues pour les nouveaux utilisateurs) est le superbe support pour l'exécution répartie et à distance des applications.

7.1 Telnet

Telnet est un programme qui permet à une personne d'utiliser un ordinateur distant comme s'il était sur place. Telnet est l'un des plus puissants outils d'UNIX, permettant une réelle administration à distance. C'est aussi un programme intéressant au niveau de l'utilisateur, parce qu'il permet à un utilisateur d'accéder à distance à tous les fichiers et les programmes qu'il utilise depuis n'importe où sur Internet. Combiné avec un serveur X, il n'y a pas de différence (à part le délai) entre être sur place ou à l'autre bout du monde. Les clients et daemons telnet sont disponibles avec toutes les distributions de Linux.

Des shells sécurisés existent via *SSH* <http://http://www.ssh.fi/sshprotocols2/index.html> permettant une administration sécurisée.

– *Logiciels en rapport avec Telnet* <http://metalab.unc.edu/pub/Linux/system/network/telnet/>

7.2 Commandes exécutées à distance

Sous Unix, et en particulier sous Linux, il existe des commandes qui permettent d'interagir avec d'autres ordinateurs depuis la ligne de commande. Par exemple : rlogin, qui permet de se loger sur une machine distante d'une manière équivalente à telnet ou rcp, qui permet de faire des transferts entre machines, etc. Et bien sûr la commande rsh (remote shell) permet d'exécuter des commandes sur une machine distante sans pour autant s'y loger.

7.3 X-Window

Le système X-Window a été développé au MIT à la fin des années 80 et il est rapidement devenu l'interface graphique standard de l'industrie pour les stations de travail graphiques UNIX. Le tout est disponible gratuitement, est très polyvalent, et est porté pour une très grande variété de plate-formes. Tout système X-Window consiste en deux parties, le serveur X, et un ou plusieurs clients X. Il est important de faire la distinction entre le serveur et le client. Le serveur contrôle l'affichage directement, et gère les entrées et les sorties via le clavier, la souris ou l'affichage. Le client, d'un autre côté, n'accède pas à l'écran directement, il communique avec le serveur, qui gère les entrées et les sorties. C'est le client qui fait tout le "vrai" travail, exécution d'application ou quoi que ce soit. Le client communique avec le serveur, demandant au serveur d'ouvrir une ou plusieurs fenêtres, et de gérer entrées et sorties pour le client.

Pour résumer, le système X-Window permet à un utilisateur d'accéder à une autre machine, d'exécuter un programme (par exemple, un navigateur WWW) et d'avoir les sorties affichées sur sa propre machine. Parce que ce processus est en réalité exécuté sur le serveur, très peu de puissance CPU est nécessaire sur le client. En fait, il est possible d'avoir des ordinateurs dont la fonction essentielle est d'être des serveurs X-Window et ils sont appelés terminaux X.

Un port gratuit du système X-Window existe pour Linux et peut être trouvé à : *Xfree* `<http://www.xfree86.org/>` Il est normalement inclus dans la plupart des distributions Linux.

HowTo en relation :

- *Application X à distance* `<http://metalab.unc.edu/mdw/HOWTO/mini/Remote-X-Apps.html>`

7.4 VNC

VNC signifie Virtual Network Computing c'est à dire, réseau virtuel d'ordinateurs. C'est un système d'affichage à distance qui permet de voir un 'bureau' d'ordinateur non seulement depuis la machine où il marche mais aussi depuis n'importe quelle machine sur Internet, et sur des architectures très variées. Des clients et des serveurs existent pour Linux et bien d'autres plate-formes. Par exemple, il est possible d'exécuter MS-Word depuis une machine sous Windows NT ou 95 et d'avoir le résultat affiché sur n'importe quelle autre machine, une machine Linux par exemple. Le contraire est bien sûr aussi possible, ainsi que d'exécuter une application sur une machine Linux et d'avoir l'affichage sur une autre machine Linux, ou une machine Windows... Un client Java existe aussi, permettant l'affichage dans un navigateur Web. Finalement, un port Linux utilisant la librairie graphique SVGAlib permet à des 386 avec 4 Mo de RAM de devenir de vrais terminaux X.

- Le *site VNC* `<http://www.uk.research.att.com/vnc>`

8 Interconnection de réseaux

La couche réseau de Linux est pleine de fonctionnalités. Un ordinateur sous Linux peut être configuré pour agir en tant que routeur, passerelle, etc... Quelques unes des options disponibles sont décrites ci-dessous.

8.1 Routeur

Le noyau de Linux supporte les fonctions de routage. Un ordinateur sous Linux peut aussi bien fonctionner en tant que routeur IP ou IPX pour un coût bien moins élevé qu'un routeur commercial. Les noyaux récents incluent des options spéciales pour les machines jouant le rôle de routeurs :

- Multicasting : permet à la machine Linux de fonctionner en tant que routeur pour des paquets IP qui ont plusieurs adresses de destination. C'est nécessaire sur le MBONE, un réseau à grande bande passante, qui diffuse du son et de la vidéo.
- IP policy routing : Normalement, un routeur décide quoi faire quand il reçoit un paquet en se basant principalement sur l'adresse finale du paquet, mais il peut aussi prendre en compte l'adresse d'origine et l'endroit d'où le paquet arrive.

Il y a quelques projets qui ont pour but de faire marcher un routeur Linux avec juste une disquette : *Projet de routeur Linux* `<http://www.linuxrouter.org/>`

8.2 Pont

Le noyau de Linux sait agir en tant que pont Ethernet, ce qui signifie que les différents segments Ethernets auxquels il est connecté apparaîtront comme un seul Ethernet aux participants. Plusieurs ponts peuvent collaborer, pour créer d'encore plus larges réseaux Ethernet en utilisant l'algorithme d'arbre (spanning tree) IEEE802.1. Comme c'est un standard, les ponts Linux pourront fonctionner avec des ponts d'autres sortes. D'autres paquetages permettent le filtrage basé sur les adresses IP, IPX ou MAC.

HowTo en relation :

- *Bridge+Firewall* `<http://metalab.unc.edu/mdw/HOWTO/mini/Bridge+Firewall.html>`
- *Bridge* `<http://metalab.unc.edu/mdw/HOWTO/mini/Bridge.html>`

8.3 IP-Masquerading

IP Masquerade est une fonction de développement de réseau pour Linux. Si une machine Linux est connectée à Internet avec IP Masquerade activé, les ordinateurs s'y connectant (soit sur le même réseau, soit se connectant par modems) peuvent accéder à Internet sans problèmes, même s'ils n'ont pas de réelle IP d'assignée. Ceci permet de réduire les coûts, puisque pas mal de personnes pourront accéder à Internet en utilisant une simple connection par modem. Cela permet aussi de réduire les risques de sécurité car d'une certaine façon, la machine agit en tant que firewall, puisque les adresses non officielles ne peuvent pas être accédées depuis l'extérieur de ce réseau.

Pages et documents se rapportant à l'IP Masquerade :

- *http ://ipmasq.home.ml.org/*
- *http ://www.indyramp.com/masq/links.pfhtml*
- *http ://metalab.unc.edu/mdw/HOWTO/IP-Masquerade-HOWTO.html*

8.4 IP Accounting

Cette option permet au noyau de Linux de garder une trace de tout le trafic IP, d'enregistrer les paquets IP, et de produire quelques statistiques. Une série de règles peuvent être définies pour que, lorsque certains paquets ont certaines caractéristiques, un compteur soit incrémenté, que le paquet soit accepté ou rejeté, etc...

8.5 IP Aliasing

Cette fonctionnalité du noyau de Linux fournit la possibilité d'assigner plusieurs adresses réseau à la même interface (ex : deux adresses IP sur une carte Ethernet). Typiquement, pour être utilisé pour des services qui se comportent différemment selon l'adresse par laquelle ils sont appelés (ex : "multihosting" ou "domaines virtuel" ou "service d'hébergement virtuel").

HowTo en relation :

- *IP Aliasing How-to* `<http://metalab.unc.edu/mdw/HOWTO/mini/IP-Alias.html>`

8.6 Traffic Shaping

Le trafic shaper est une interface virtuelle qui permet de limiter le trafic montant vers une autre interface réseau. C'est particulièrement utile quand on veut limiter/contrôler la bande passante utilisée par un client. Une autre alternative (pour le web seulement) serait d'utiliser un module d'Apache qui restreint le nombre de connections par client, ou la bande passante utilisée.

– *http ://metalab.unc.edu/mdw/HOWTO/NET-3-HOWTO.html#ss6.15*

8.7 Firewall

Un firewall est une interface qui protège un réseau prive du reste d'Internet. Il est conçu pour contrôler le flux de paquets en se basant sur la source, la destination, le port et le type de paquet contenu dans chaque paquet.

Il existe différents outils de firewalls pour Linux, ainsi qu'un support intégré dans le noyau. D'autres firewalls sont TIX et SOCKS. Ces kits de firewall sont très complets, et combinés avec d'autres outils, permettent de bloquer/rediriger tous types de trafic et protocoles. Différentes règles peuvent être implémentées par le biais de fichiers de configuration ou grâce à des programmes graphiques.

– La *page de TIS* <http://www.tis.com>
– *SOCKS* <http://www.socks.nec.com/socksfaq.html>
– Le *Firewall How-to* <http://metalab.unc.edu/mdw/HOWTO/Firewall-HOWTO.html>

8.8 Reroutage de ports

Un nombre croissant de sites WWW deviennent interactifs en ayant des cgi-bins ou des applets Java qui accèdent à des bases de données ou à d'autres services. Puisque ces accès peuvent poser des problèmes de sécurité, la machine contenant la base de donnée ne devrait pas être connectée directement à Internet.

Le reroutage de ports peut fournir une solution presque idéale à ce problème d'accès. Avec un firewall, les paquets IP qui arrivent sur un port spécifique peuvent être réécrit et envoyés au serveur interne fournissant le service. Le paquet qui est reçu du serveur interne est réécrit pour le faire apparaître comme arrivant du firewall.

Des informations sur le reroutage de ports peuvent être trouvées *ici* <http://www.ox.compsoc.net/~steve/portforwarding.html>

8.9 Répartition de charge

Lorsqu'un serveur Web, qui utilise une base de donnée, est très chargé, il serait utile d'avoir plusieurs serveurs identiques et de rediriger les requêtes vers le serveur le moins chargé. Ceci peut être fait avec les techniques de translation d'adresses réseau (NAT : Network Address Translation) dont IP-Masquerading est un sous-ensemble. Les administrateurs réseaux peuvent remplacer un serveur simple fournissant des services Web - ou n'importe quoi d'autre - par un groupe de serveurs partageant la même adresse IP. Les connections arrivantes sont redirigées vers l'un des serveurs en utilisant un algorithme de répartition de charge. Le serveur virtuel réécrit les paquets entrants et sortants pour que les clients aient un accès transparent au serveur, comme s'il était unique.

Des informations sur Linux IP-NAT peuvent être trouvées *là* <http://www.csn.tu-chemnitz.de/HyperNews/get/linux-ip-nat.html>

8.10 EQL

EQL est intégré au noyau de Linux. Si deux connections séries existent vers un autre ordinateur (cela demande deux modems et deux lignes de téléphone) et si SLIP ou PPP (un protocole pour envoyer un trafic internet à travers une ligne de téléphone) sont utilisés dessus, il est possible de les faire se comporter comme une seule connection ayant une vitesse double en utilisant ce driver. Naturellement, EQL doit être supporté de l'autre côté aussi.

– *http ://metalab.unc.edu/mdw/HOWTO/NET-3-HOWTO-6.html#ss6.2*

8.11 Serveur Proxy

Le terme proxy signifie "faire quelque chose pour quelqu'un d'autre". En termes de réseau, un serveur proxy est un ordinateur qui agit pour plusieurs clients. Un proxy HTTP est une machine qui reçoit des requêtes à des pages Web d'autres machines (machine A). Le proxy récupère la page en question et retourne le résultat à la machine A. Le proxy peut avoir un cache contenant les pages déjà demandées, de façon à ce que , si une autre machine demande la même page, la copie du cache soit retournée à la place. Ceci permet de réduire la bande passante utilisée, et d'avoir un temps de réponse plus court. Comme effet de bord, les machines clientes n'accèdent pas directement au monde extérieur et cela peut rendre un réseau plus sûr. Un proxy bien configuré peut être aussi efficace qu'un firewall.

Plusieurs serveurs proxy existent pour Linux. La solution la plus populaire est le module proxy d'Apache. Il y a aussi SQUID qui est une implémentation plus complète et plus robuste de proxy HTTP.

– *Apache* `<http://www.apache.org>`
– *Squid* `<http://squid.nlanr.net>`

8.12 Connection à la demande

Le but des connections à la demande est de faire croire aux utilisateurs qu'ils ont une connection permanente d'un point à un autre. D'habitude, il y a un daemon qui surveille le trafic de paquets, qui établit la connection quand elle est nécessaire, puis après une période d'inactivité, clot la connection.

– Le *Diald How-to* `<http://metalab.unc.edu/mdw/HOWTO/mini/Diald.html>`

8.13 Tunnelling, IP mobile et réseaux privés virtuels

Le noyau de Linux permet le tunnelling (encapsulation) de protocoles. Il peut faire du tunnelling IPX via IP, permettant la connection de deux réseaux IPX via une simple liaison IP. Il peut aussi faire du tunnelling IP-IP, qui est majoritairement utilisé pour le support des IP mobiles, le support du multicast, et la radio amateur. (voir *http ://metalab.unc.edu/mdw/HOWTO/NET-3-HOWTO-6.html#ss6.8*)

Les IP mobiles sont une amélioration qui permet un routage transparent de datagrammes IP vers des noeuds IP sur Internet. Chaque noeud est toujours identifié par son adresse d'origine, quelque soit son point de rattachement à Internet. Quand il est éloigné de son point d'origine, un noeud mobile est aussi associé avec une adresse d'hébergement, ce qui fournit des informations sur son point de rattachement actuel sur Internet. Le protocole permet d'enregistrer l'adresse de l'hébergeur avec un programme spécifique. Ce programme envoie les datagrammes destinés au noeud mobile via le tunnel de l'adresse de l'hébergeur. Après être arrivé, chaque datagramme est alors délivré au noeud mobile.

Le Point-to-Point Tunneling Protocol (PPTP) est une technologie réseau qui permet d'utiliser Internet en tant que réseau privé virtuel (VPN : virtual private network). PPTP est intégré dans le serveur de services d'accès à distance (RAS : Remote Access Services) de Windows NT server. Avec PPTP, les utilisateurs peuvent se connecter à leur FAI local, ou se connecter directement à Internet, et utiliser leur réseau comme s'ils étaient devant leur bureau. PPTP est un protocole bien défini, et sa sécurité a récemment été compromise. Il est fortement conseillé d'utiliser l'une des alternatives proposées par Linux, car elles s'appuient sur des standards qui ont été examinés et testés très minutieusement.

– Un client PPTP pour Linux est disponible *ici* `<http://www.pdos.lcs.mit.edu/~cananian/Projects/PPTP/>`

– Plus d'informations sur PPTP peuvent être récupérées *là* <http://bmrc.berkeley.edu/people/chaffee/linux_pptp.html>

IP mobile :

– *http ://www-uk.hpl.hp.com/people/jt/mip.html*
– *http ://metalab.unc.edu/mdw/HOWTO/NET-3-HOWTO-6.html#ss6.12*

Document parlant des réseaux privés virtuels :

– *http ://metalab.unc.edu/mdw/HOWTO/mini/VPN.html*
– *http ://sites.inka.de/sites/bigred/devel/cipe.html*

9 Administration Réseau

9.1 Programmes d'administration réseau

Il y a une liste impressionnante d'outils qui sont dédiés à l'administration réseau et à l'administration à distance. Quelques projets intéressants sont linuxconf et webmin :

– *Webmin* <http://www.webmin.com/webmin/>
– *Linuxconf* <http://www.solucorp.qc.ca/linuxconf/>

D'autres outils incluent des outils d'analyse de trafic réseau, de sécurité réseau, de surveillance, de configuration, etc. Une archive de tous ces outils peut être trouvée à *Sunsite* <http://www.metalab.unc.edu/pub/Linux/system/network/>

9.2 SNMP

Le Simple Network Management Protocol (protocole d'administration réseau simple) est un protocole dédié à l'administration des services réseaux. Il permet l'administration et la surveillance à distance de routeurs, passerelles, cartes réseaux, switches, etc... Il y a un grand nombre de librairies, clients, daemons et programmes de surveillances SNMP disponibles pour Linux. Une bonne page pour démarrer est : *http ://linas.org/linux/NMS.html*

10 Réseaux d'entreprises sous Linux

Dans certaines situations, il est nécessaire d'avoir une infrastructure réseau comprenant des mécanismes lui permettant d'être disponible quasiment 100% du temps. Certaines de ces techniques sont décrites plus loin. La majorité des documents suivants peuvent être trouvés sur l'excellent site web de Linas : *http ://linas.org/linux/index.html* et dans le *HowTo Linux High-Availability* <http://metalab.unc.edu/pub/Linux/ALPHA/linux-ha/High-Availability-HOWTO.html>

10.1 Haute disponibilité

La redondance est utilisée pour éviter qu'Internet dans sa globalité ait un point faible. Un serveur avec une seule carte réseau ou un seul disque SCSI a deux points faibles. L'objectif est de cacher aux utilisateurs les problèmes imprévus de façon à ce qu'ils puissent continuer à travailler rapidement. Les logiciels de haute disponibilité sont un groupe de scripts et d'outils qui surveillent et détectent les problèmes, suivent une méthode appropriée pour restaurer l'état normal et préviennent les administrateurs systèmes.

10.2 RAID

RAID est l'abréviation de Redundant Array of Inexpensive Disks, c'est à dire Grappe redondante de disques, c'est une méthode grâce à laquelle les informations sont réparties sur plusieurs disques, utilisant des techniques telles que la mise bout à bout des disques (RAID niveau 0), la mise en miroirs (RAID niveau 1) pour obtenir la redondance, des temps d'attente plus faibles et/ou une plus grande bande passante pour la lecture et/ou l'écriture, et la récupération après un crash disque. 6 niveaux RAID différents ont été définis. Il y à 3 solutions RAID possibles pour les utilisateurs de Linux : RAID logiciel, boîtiers DASD externes, et contrôleurs de disques RAID.

– RAID Logiciel : Implémentation RAID purement logicielle, permet l'utilisation des différents niveaux RAID dans le code de gestion des disques du noyau (les bloc devices)
– Boîtiers DASD externes : les DASD (Direct Access Storage Device, c-a-d périphérique de stockage à accès direct) sont des boîtiers séparés ayant leur propre alimentation électrique, fournissent un châssis pour ranger les disques, et sont considérés par Linux comme un périphérique SCSI comme un autre. D'une façon générale, c'est la solution RAID la plus fiable.
– Contrôleurs de disques RAID : Les contrôleurs de disques sont des cartes qui se mettent dans les bus ISA/EISA/PCI. Un câble les rattache aux disques, comme pour les contrôleurs normaux. Mais contrairement aux contrôleurs normaux, les contrôleurs RAID implémentent le RAID sur la carte elle-même, avec tout ce qu'il faut pour fournir les différents niveaux RAID.

HowTo en relation :
– *http ://metalab.unc.edu/mdw/HOWTO/mini/DPT-Hardware-RAID.html*
– *http ://metalab.unc.edu/mdw/HOWTO/Root-RAID-HOWTO.html*
– *http ://metalab.unc.edu/mdw/HOWTO/mini/Software-RAID.html*
Le RAID à linas.org :
– *http ://linas.org/linux/raid.html*

10.3 Redondance réseau

Le takeover d'adresse IP (IPAT) :

Quand une interface réseau tombe en panne, son adresse IP devrait être prise par une carte en état de marche sur le même noeud du réseau, ou sur un autre noeud.

Le takeover d'adresse MAC :

Quand un takeover d'adresses IP survient, il faut s'assurer que tous les noeuds du réseau mettent à jour les caches de leurs tables ARP (les correspondances entre adresses IP et les adresses MAC).

Pour plus de détails, référez vous au : *HowTo High-Availability* `<http://metalab.unc.edu/pub/Linux/ALPHA/linux-ha/High-Availability-HOWTO.html>`

11 Sources d'informations

Si vous avez des problèmes de réseau avec Linux, n'envoyez pas d'email ni a l'auteur, ni au traducteur. Nous n'avons tout simplement pas le temps d'y répondre. Vous aurez plus de chance en vous adressant dans le groupe de discussions comp.os.linux.networking ou fr.comp.os.linux.configuration (que vous pouvez accéder depuis *http ://www.deja.com*). Avant d'aller poster la bas, assurez vous de bien avoir lu toute la documentation concernant votre problème. Ensuite, allez chercher dans les archives des news car il y a de fortes chances que quelqu'un, un jour aie déjà posé la même question (et que quelqu'un aie répondu). Si vous allez jusqu'à poser une question, expliquez bien toutes les étapes que vous avez fait et quel message d'erreur vous avez obtenus.

Où trouver de plus amples informations :

- Linux : *http ://www.linux.org*
- Le Linux Documentation Project : *http ://metalab.unc.edu/mdw/linux.html* (Allez lire le Linux Network Administrator Guide)
- Freshmeat : Les dernières nouveautés des logiciels Linux. *http ://www.freshmeat.net*
- Liens sur Linux : *http ://www.linuxlinks.com/Networking/*

12 Historique

- 0.31 (17 Sept 1999) Changement de l'adresse du linux router project (merci à John Ellis) et ajout d'un autre lien PPTP (merci à Benjamin Smith)
- 0.30 (6 avril 1999) Ajout de la section sur CODA (merci à *Brian Ristuccia* <mailto:brianr@osiris.978.org>
- 0.2-0.29 débuggage :-) (Allez regarder les remerciements a la fin du document)
- 0.1 (5 juin 1998)

13 Remerciements et mise en garde

Ce document est basé sur le travail de beaucoup d'autres personnes qui ont fait leur possible pour que Linux devienne ce qu'il est maintenant : un des meilleurs systèmes d'exploitation basé réseau. Tous les crédits leurs reviennent. Beaucoup de travail a été fait pour que ce document soit clair, ainsi qu'exact et complet, mais sans être excessivement long. Néanmoins, l'auteur décline toute responsabilité en cas de mauvaise utilisation des informations contenues dans ce document. N'hésitez pas à m'envoyer vos suggestions, corrections, ou commentaires généraux pour que je puisse l'améliorer. Ce HowTo grandira certainement avec le temps, par exemple avec radius, les outils pour dupliquer un web/ftp grâce à wget, des analyseurs de trafic, CORBA... Et tout ce qui me sera suggéré et qui me paraîtra intéressant. Vous pouvez me joindre *daniel@rawbyte.com* (et *là* <mailto:arn_mat@club-internet.fr> pour la traduction française)

Je voudrais finalement remercier *Finnbjorn av Teigum*, *Cesar Kant*, *Mathieu Arnold* et spécialement *Hisakuni Nogami* et *Phil Garcia* pour leur relecture et commentaires sur ce HOWTO. Leur aide a été tres appréciée.

Vous pouvez toujours trouver une version de ce document sur *http ://www.rawbyte.com/lno/* <http://www.rawbyte.com/lno> en vo et sur *http ://www.mat.cc/howto/* <http://www.mat.cc/howto/> pour la vf.

Daniel López Ridruejo 17 septembre 1999