

Administration système en réseau : «voisinage réseau»

Philippe Latu

philippe.latu(at)linux-france.org

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

Historique des versions		
\$Revision: 1384 \$	\$Date: 2009-05-06 19:55:13 +0200 (mer 06 mai 2009) \$	\$Author: latu \$
Année universitaire 2008-2009		
Résumé		
Avant d'administrer les accès aux systèmes de fichiers réseau sur un réseau local, l'objectif de ces travaux pratiques est d'étudier quelques exemples simples d'utilisation du «voisinage réseau» avec les systèmes GNU/Linux. À l'issue de ces travaux pratiques d'introduction, les outils et les méthodes sont en place pour avancer vers des conditions d'exploitation plus proches des réalités professionnelles. La notion de «voisinage réseau» permet d'aborder en douceur les tests sur le fonctionnement des systèmes de fichiers réseau.		

Table des matières

1. Copyright et Licence	1
1.1. Méta-information	2
2. Adressage IP des postes de travail	2
3. Serveur d'information LAN : LISa	2
3.1. Travaux pratiques	2
4. Service SSH et protocole FISH	3
4.1. Travaux pratiques	4
5. Samba par l'exemple	4
5.1. Travaux pratiques	4
6. Documents de référence	5

1. Copyright et Licence

Copyright (c) 2000,2009 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2009 Philippe Latu.
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.2 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

1.1. Méta-information

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 : admin.reseau.neigh.pdf³ | admin.reseau.neigh.ps.gz⁴.

2. Adressage IP des postes de travail

À partir de l'infrastructure type, on constitue des couples de postes de travail qui vont partager le même domaine de diffusion ou le même «voisinage réseau» dans le contexte de ces travaux pratiques.

Ces opérations de réaffectation du plan d'adressage IP sont répétées à chaque début de séance de travaux pratiques. Elles s'appuient sur les indications données dans le document *Architecture réseau des travaux pratiques*.

Tableau 1. Affectation des adresses T.P. «voisinage réseau»

Poste 1	Poste 2	Passerelle par défaut
alderaan	bespin	10.4.4.1/23
centares	coruscant	192.168.109.1/25
dagobah	endor	10.0.117.1/27
felucia	geonosis	10.7.10.1/23
hoth	kamino	172.19.112.1/26
mustafar	naboo	192.168.111.1/25

Une fois la connectivité réseau validée, on étudie un premier mode d'exploitation du «voisinage réseau». On s'appuie sur des fonctionnalités directement utilisables avec le gestionnaire graphique KDE.

3. Serveur d'information LAN : LISa

Dans cette section, on étudie le fonctionnement du service d'information LAN LISa. L'objectif de ce service est de recenser les autres services disponibles sur un réseau local. Sa caractéristique particulière réside dans la minimisation de la quantité d'informations échangées pour les opérations de recensement.

Avec ce service on illustre les pratiques usuelles d'utilisation des services sur un réseau local.

- Plus l'utilisation doit être transparente pour l'utilisateur, plus on a recours à la diffusion ou multi-diffusion sur le réseau. Cet usage conduit à augmenter considérablement le trafic et à exposer des informations sensibles susceptibles d'être capturées à l'aide d'un dispositif d'écoute et d'analyse.

Cette philosophie a logiquement été retenue pour les systèmes Micro\$oft™ puisque la transparence dans l'utilisation des services réseau est une priorité absolue pour ces systèmes.

- Plus on veut exercer un contrôle important sur les informations échangées sur un réseau, plus les opérations d'administration des services réseau sont importantes. C'est à ce prix que l'on optimise l'utilisation des équipements et que l'on limite l'exposition d'informations sensibles. La situation idéale dans ce contexte est que l'utilisateur final parvienne à une utilisation transparente du service tout en étant sensibilisé aux contraintes de sécurité.

La documentation sur le fonctionnement du service LISa est fournie avec le gestionnaire graphique KDE. Il suffit donc de consulter l'aide en ligne à partir de l'URL : `help:/lisa`.

3.1. Travaux pratiques

1. Quel est le paquet *Debian GNU/Linux* correspondant au service LISa ? Donner un exemple de commande permettant de vérifier que le paquet est bien installé ?

¹ <http://www.docbook.org>

² <http://www.debian.org>

³ <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.neigh.pdf>

⁴ <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.neigh.ps.gz>

2. D'après la documentation, quel est le numéro de port utilisé par le service LISa ? Quel est le protocole de couche transport utilisé ?

Pour traiter les questions suivantes, il faut utiliser l'analyseur réseau Wireshark. La documentation sur l'utilisation de cet analyseur est disponible sur le support *Introduction à l'analyse réseau*.

La manipulation d'appel au service `lisa` consiste à ouvrir `konqueror` sous sa forme gestionnaire de fichiers ou navigateur Web puis à saisir une URL du type `lan:<mon_voisin>`. Dans le même temps, Wireshark doit capturer l'ensemble des flux réseau.

Les questions suivantes sont à traiter sans modifier la configuration du service.

1. Retrouver avec l'analyseur réseau les informations demandées précédemment : numéro de port et protocole de couche transport.
2. Quels sont les numéros de ports utilisés lors du recensement ?
3. À quels services correspondent ces numéros de port ?
4. Quels services ont été reconnus ? Relever les identifiants de ces services à l'aide des données capturées.

On se propose maintenant de scruter le réseau local de façon à obtenir un «recensement transparent» des services disponibles. Il est donc nécessaire de modifier la configuration du service `lisa`. Voici un exemple de fichier de configuration permettant la scrutation du réseau `192.168.1.0/24/`.

```
PingAddresses      =      192.168.1.0/255.255.255.0
PingNames         =
AllowedAddresses  =      192.168.1.0/255.255.255.0
BroadcastNetwork  =      192.168.1.0/255.255.255.0
SearchUsingNmblookup =      1      #also try nmblookup
FirstWait        =      30      #30 hundredth seconds
SecondWait       =      -1      #only one try
#SecondWait      =      60      #the second time wait 0.6 seconds
UpdatePeriod     =      300     #update after 300 secs
DeliverUnnamedHosts =      0     #don't publish hosts without name
MaxPingsAtOnce   =      256     #send up to 256 pings at once
```

De plus, pour étoffer le catalogue des services, il faut quelques paquets supplémentaires correspondant à ces services sur le poste qui joue le rôle de serveur. Par exemple, on peut ouvrir un service Web en installant le paquet `apache` et reconfigurer le service SSH pour que le serveur soit en écoute sur l'interface de réseau local.

1. Sur le premier poste, installer le serveur Web. Reprendre les questions précédentes en identifiant le nouveau service. Quel est le nouveau numéro de port ouvert ? Quelles sont les informations relevées dans la fenêtre de données de l'analyseur réseau ?
2. Sur le second poste, modifier la configuration du service `lisa` et relancer le service. Toujours en utilisant la requête `lan:/` dans le gestionnaire de fichiers.

Reprendre les questions précédentes en identifiant les services. Quel sont les numéros de port ouverts ? Quelles sont les informations relevées dans la fenêtre de données de l'analyseur réseau ?

4. Service SSH et protocole FISH

Dans cette section on étudie le protocole `FISH`. L'objectif de ce protocole est de superposer les opérations de transferts de fichiers au protocole `SSH`. On dispose ainsi d'un pseudo serveur `FTP` sécurisé puisque toutes les transactions sont chiffrées. Comme `SSH` n'utilise que le seul port `tcp/22` pour l'ensemble des communications, le protocole `FISH` est facile à exploiter sur des architectures étendues complexes avec des pare-feux.

L'utilisation de `FISH` avec le gestionnaire de fichiers `KDE` rend les opérations transparentes. On reproduit ainsi un fonctionnement «*Windoze-like*» du voisinage réseau en traversant l'Internet avec un *niveau de sécurité très supérieur*.

4.1. Travaux pratiques

Les questions suivantes supposent que les services SSH et LISa sont actifs sur les deux postes de travail du même réseau local. Comme dans les sections précédentes, il faut utiliser les supports de documentations *Configuration d'une interface réseau* et *Introduction à l'analyse réseau* pour traiter les questions.

1. Quelles sont les 2 commandes qui permettent de lister les services réseau actifs en écoute sur le système ?
2. Quelle est la commande qui permet de reconfigurer le paquet SSH pour activer le serveur `sshd` sur le système ?

Sachant que les services sont actifs, on peut passer à l'analyse du fonctionnement des transferts de fichier via le gestionnaire de fichiers du gestionnaire graphique KDE.

On lance la capture avec l'analyseur Wireshark et on ouvre un nouveau gestionnaire de fichier avec une URL du style `lan:/<mon_voisin>` ou `lan://localhost/<mon_voisin>`.

1. À partir des résultats de capture, identifier les ports utilisés par les différents services : port source navigateur, port destination LISa local ou distant, port utilisé par le service FISH.
2. Est-il possible de visualiser les données échangées lors des opérations de transfert de fichiers ? Pourquoi ?

5. Samba par l'exemple

Dans cette partie, on se propose d'illustrer une démarche classique de travaux pratiques. Exploiter une documentation de référence et transposer son application sur le système GNU/Linux utilisé.

La documentation de référence à utiliser est la section intitulée *No-Frills Samba Servers* du guide *Samba-3 par l'exemple*. Cette section propose d'implanter 3 configurations basiques proches de la problématique «voisinage réseau» de ces travaux pratiques.

Le travail de transposition sur la distribution *Debian GNU/Linux* est relatif à la gestion des paquets. Il faut rechercher dans la base de données les paquets qui correspondent au service à installer et configurer.

Il est impératif de consulter le tableau de bord du serveur Web d'assurance qualité de façon à évaluer correctement la «maintenance» du service dans la distribution. Dans notre cas, la page à consulter est : *Overview of samba source package*⁵.

En consultant cette page, on constate qu'il s'agit d'un groupe de «paquets majeurs» qui bénéficie d'un excellent suivi. Il est donc vivement conseillé de consulter la documentation des paquets après leur installation. Les responsables de ce type de paquets ont capitalisé une très grande expérience d'exploitation sur de grosses infrastructures. Les «conseils» fournis dans la documentation des paquets sur les bonnes pratiques de configuration service sont particulièrement avisés.

Le travail de transposition ne s'arrête pas à l'installation des paquets. L'étape de configuration est essentielle à la continuité du service. On cherchera donc à donner la priorité aux indications données par le responsable de paquet et aux règles de la distribution *Debian GNU/Linux*.

5.1. Travaux pratiques

1. Quelles sont les commandes à utiliser pour rechercher les paquets relatifs au service Samba dans la base de données des paquets ?
2. Quels sont les fichiers de documentation importants fournis avec les paquets relatifs au service Samba ?
3. Quels sont les fichiers de configuration importants fournis avec les paquets relatifs au service Samba ?
4. Quelles différences ont été constatées lors de l'implantation du scénario *Drafting Office* entre la documentation de référence et l'application sur la distribution installée sur le poste ?

⁵ <http://packages.qa.debian.org/s/samba.html>

5. Reprendre la même démarche avec le scénario *Charity Administration Office* sans le service d'impression. Quelles différences ont été constatées lors de la transposition de ce scénario ?
6. Reprendre la même démarche avec le scénario *Accounting Office* sans le service d'impression. Quelles différences ont été constatées lors de la transposition de ce scénario ?

6. Documents de référence

Architecture réseau des travaux pratiques

*Architecture réseau des travaux pratiques*⁶ : présentation de l'implantation des équipements d'interconnexion réseau dans l'armoire de brassage et du plan d'adressage IP prédéfini pour l'ensemble des séances de travaux pratiques.

Introduction à l'analyse réseau

*Introduction à l'analyse réseau avec Wireshark*⁷ : présentation de l'utilisation de l'analyseur réseau et travaux pratiques d'introduction sur le fonctionnement de la pile de protocoles TCP/IP.

Configuration d'une interface réseau

*Configuration d'une interface de réseau local*⁸ : tout sur la configuration des interfaces réseau de réseau local ; notamment les explications sur les opérations «rituelles» de début de travaux pratiques :

```
# ifdown eth0
# ifconfig eth0 192.168.0.2 netmask 255.255.255.240
# route add default gw 192.168.0.1
# ping 192.168.0.1
# ping 172.16.80.1
# ping www.cict.fr
```

Samba-3 par l'exemple

*Samba-3 by Example*⁹ : exercices pratiques pour un déploiement réussi de Samba.

Cette introduction à l'utilisation de Samba basée sur des cas pratiques de complexité croissante est un exemple caractéristique de méthode de prise en main d'un logiciel libre.

⁶ <http://www.linux-france.org/prj/inetdoc/cours/archi.tp/>

⁷ <http://www.linux-france.org/prj/inetdoc/cours/intro.analyse/>

⁸ <http://www.linux-france.org/prj/inetdoc/cours/config.interface.lan/>

⁹ <http://www.samba.org/samba/docs/man/Samba-Guide/>