

Clients légers

Ce tutoriel développe la mise en place de clients légers (diskless ou non) qui pourront ouvrir différents types de sessions (X, VNC, RDP, ...) sur des serveurs d'applications Linux ou Windows\$.

Les postes clients légers pourront booter sur plusieurs périphériques au choix (disquette, cdrom, bootrom, pxe) pour charger une image système en RAM.

Grâce à cette image système, vous pourrez ouvrir une session graphique sur le serveur désiré.

Vous avez la possibilité d'utiliser les périphériques présents sur votre client léger (lecteur CD, disquette, clef USB, imprimante locale ou disque dur local) et même de déporter le son.

Le logiciel de création d'image système utilisé dans ce tutoriel est PXES. Il demande beaucoup de dépendances pour s'installer !

La distribution Debian sarge possède toutes ces dépendances à la différence de la Mandrake 10.x. C'est pour cette raison que **le logiciel PXES sera présenté uniquement sous Debian.**

Installation des packages



Pour utiliser PXES :

Gnome (PXES a besoin de libraries gnome pour un affichage correcte)

glade-perl_0.61-1_all.deb

hwdata_0.145-1_all.deb

libgnome-perl_0.7009-1.1_i386.deb

mkisofs_2.0+a34-2_i386.deb

mknbi_1.4.3-2_i386.deb

squashfs-tools_2.0-1_i386.deb

(ftp://hiscpdftp01.upsa.es/debian/ et installer avec dpkg -i pxes...)

pxes_20040816_i386.deb (qui téléchargera la source pour l'installer)

pxesconfig_0.9.1-1_all.deb

Pour le **Serveur DNS, DHCP, TFTP** :

bind9_9.2.4-1_i386.deb

dhcp3-server_3.0.1-1_i386.deb

dhcp3-common_3.0.1-1_i386.deb

tftpd_0.17-11_i386.deb

Pour le **Serveur X et d'applications** :

xserver-xfree86_4.3.0.dfsg.1-8_i386.deb

xfree86-common_4.3.0.dfsg.1-8_all.deb

KDE ou/et Gnome

Utilisation de PXES

Une fois l'installation de PXES terminée, ajoutez dans le fichier **/etc/fstab** cette ligne qui servira à monter l'image pxes.initrd :

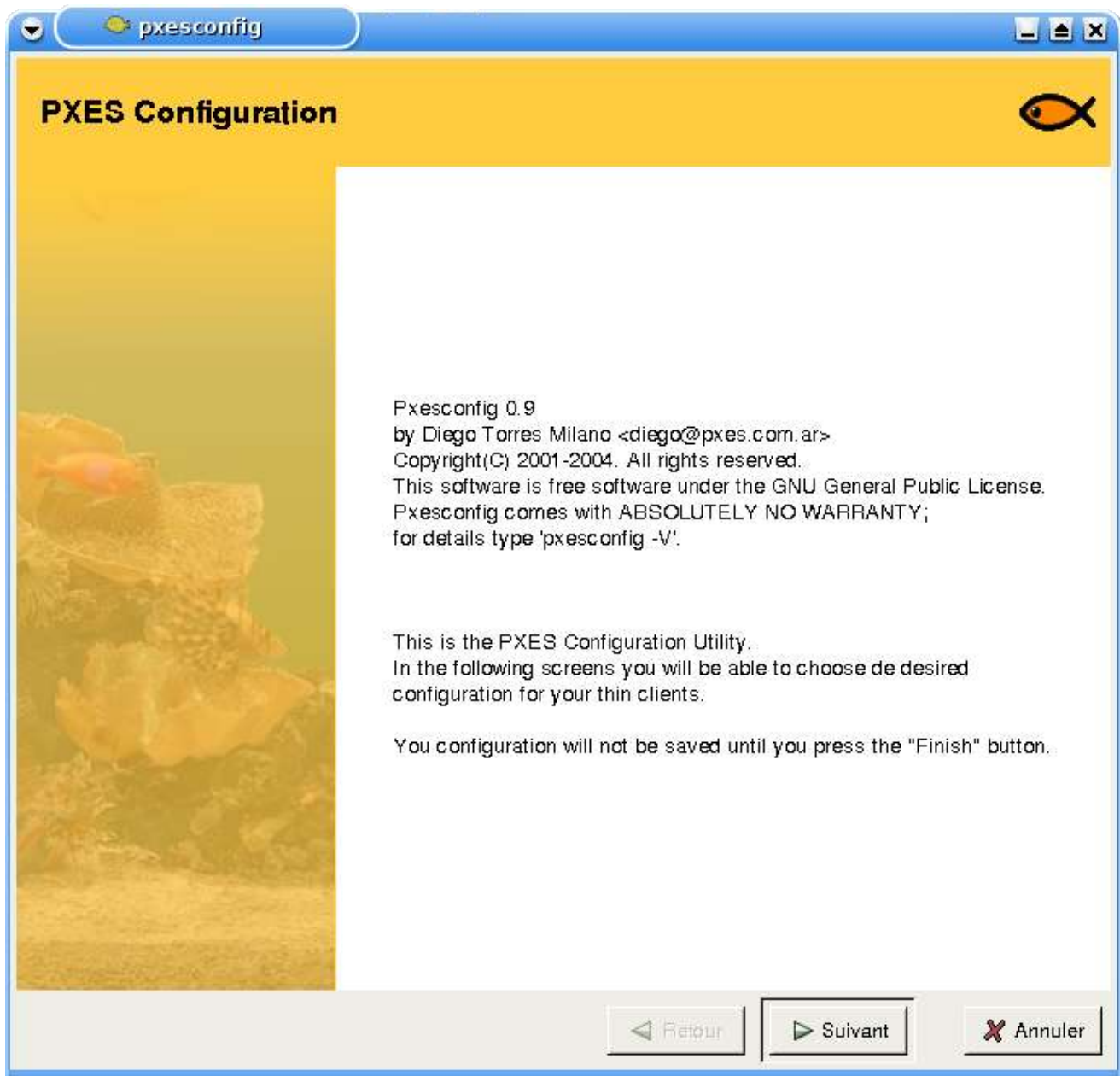
```
/tmp/pxes.initrd /tmp/pxes ext2 loop,noauto,user,owner 0 0
```

Autorisez temporairement root dans votre session X pour lancer l'interface de PXES :

```
user@serv2:~$ xhost +  
access control disabled, clients can connect from any host
```

Passez en root et lancez l'interface de PXES :

```
user@serv2:~$ su  
serv2:/home/user# pxesconfig
```





Kernel and initial ram disk selection

Select the desired splash screen image, kernel and initial ram disk.

If you want to initialize the ram disk image check "Initialize ram disk", the image must exist.

If the ram disk image already exist and you want to re-read the configuration

check "Read saved configuration"

Image visible au démarrage lorsque l'on boot sur le Cdrom

Splash screen: / Parcourir...

Initial ram disk **Pour créer une nouvelle image ram disk**



Ram disk name: / Parcourir...

☒ Initialize ram disk contents ☐ Read saved configuration

Kernel configuration



Kernel architecture:

Kernel file name: / Parcourir...

Network bootable image **Nom de l'image système qui sera téléchargée après avoir booté.**



☒ Enable network bootable image generation (needed by Etherboot)

Tagged image name: / Parcourir...

ISO bootable image **Nom de l'image système en ISO à graver sur un CD. Evite le téléchargement par le réseau, ainsi que l'utilisation d'un serveur TFTP.**



☐ Enable ISO 9660 bootable image generation

ISO 9660 image name: / Parcourir...

Squashed image

☐ Enable Squashfs image generation

Squashed image name: / Parcourir...

Retour

Suivant

Annuler

Required Local Devices



Select the desired characteristics of the local devices

Keyboard configuration



Layout:

Mouse configuration



Device: Protocol:

☐ Enable mouse wheel support

☐ Left handed mouse

Acceleration:

Sensitivity:

Network configuration



Network card:

Kernel module options:

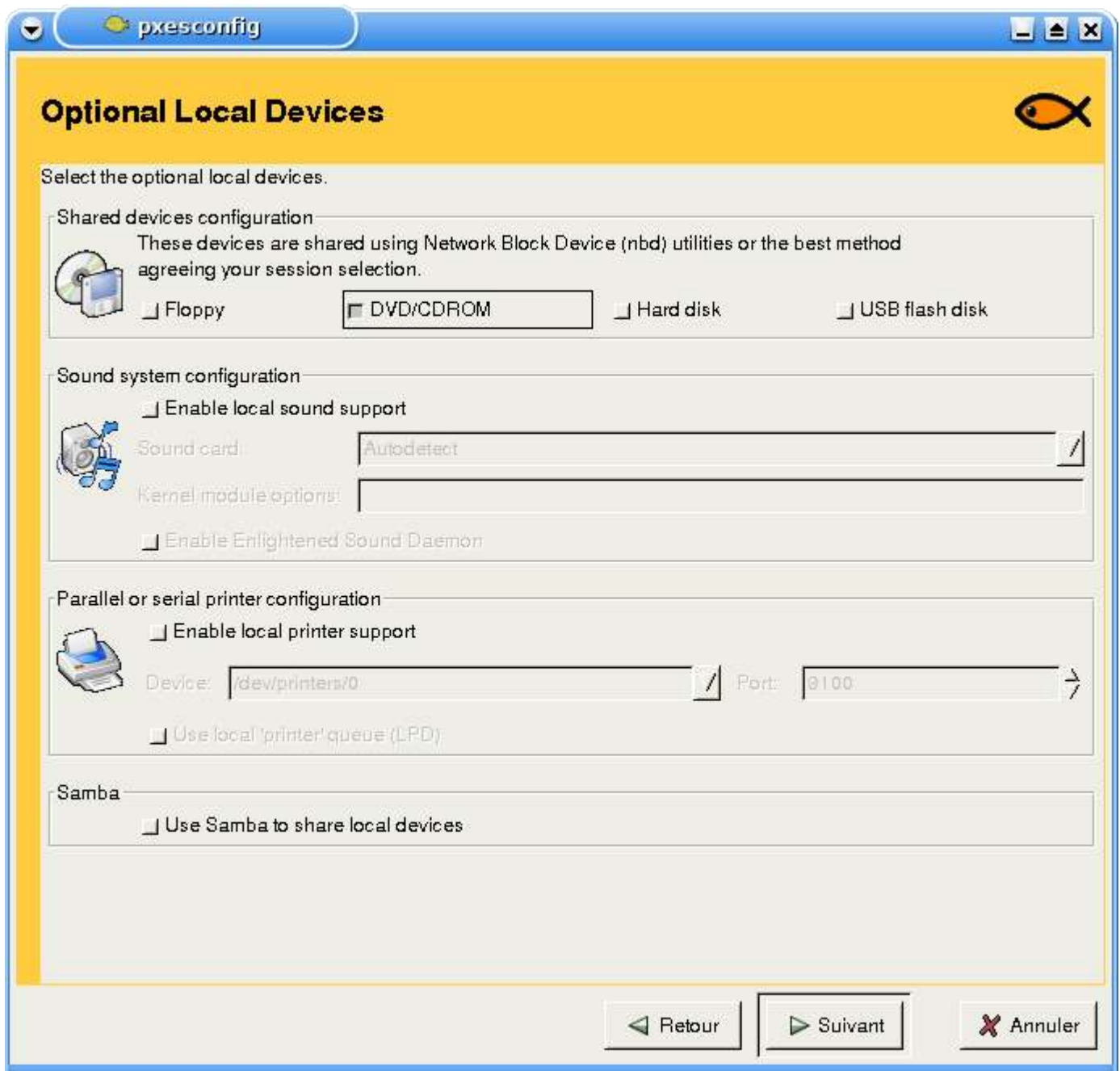
Retour

Suivant

Annuler

Si vous choisissez d'utiliser des périphériques présents sur votre client léger, par exemple ici le lecteur CD.

Vous pouvez aussi déporter le son vers votre client léger et partager son disque dur.



The image shows a window titled "pxesconfig" with a yellow header bar. The main title is "Optional Local Devices" in bold black text. Below the title is a small orange fish icon. The window contains several sections for configuring optional local devices:

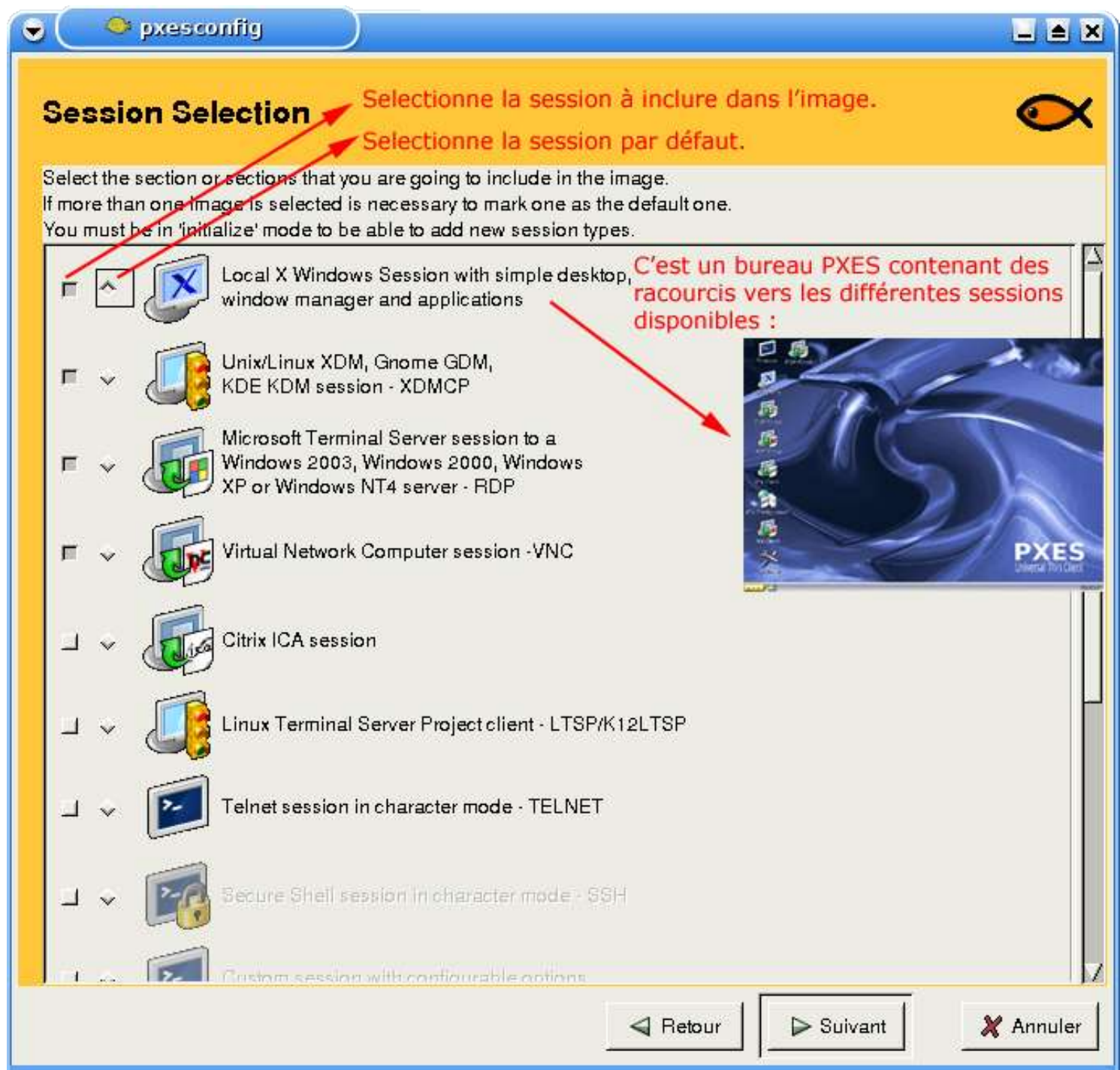
- Select the optional local devices.**
- Shared devices configuration**
These devices are shared using Network Block Device (nbd) utilities or the best method agreeing your session selection.
Icons: Floppy, DVD/CDROM, Hard disk, USB flash disk.
Checkboxes: ☐ Floppy, ☒ DVD/CDROM, ☐ Hard disk, ☐ USB flash disk
- Sound system configuration**
Icon: Sound card.
Checkboxes: ☐ Enable local sound support
Sound card: Autodetect
Kernel module options:
☐ Enable Enlightened Sound Daemon
- Parallel or serial printer configuration**
Icon: Printer.
Checkboxes: ☐ Enable local printer support
Device: /dev/printers/0
Port: 0100
☐ Use local 'printer' queue (LPD)
- Samba**
☐ Use Samba to share local devices

At the bottom of the window are three buttons: "Retour", "Suivant", and "Annuler".

Sélectionnez les sessions que vous voulez utiliser.

Dans l'exemple ci-dessous :

- J'inclus les sessions Bureau PXES, X, RDP et VNC.
- Par défaut, après le boot du client léger, le bureau PXES sera lancé.




Choisissez le serveur Xfree86-4.3

pxesconfig

X windows


▼ XFree86 3.3.6 ▲ XFree86 4.3.0

Font Server

 ☐ Enable font server

Server: Port: →

Video Hardware


 Video driver: /

Video Modes


☐ 1600x1200 ☐ 1280x1024 ☒ 1024x768 ☐ 800x600 ☐ 640x480

☐ Custom x Modeline:

Color Depth

 ▼ 32 bits ▲ 24 bits ▼ 16 bits ▼ 8 bits

Monitor Frequency

 ☒ Autodetect Horizontal: / kHz Vertical: / Hz

Options

☐ No acceleration ☐ No hardware cursor ☐ Don't zap ☐ Don't VT switch ☐ No screensaver ☐ DPMS

Extra options:

◀ Retour ▶ Suivant ✕ Annuler

Local Session Configuration



Local session with a simple desktop, a task-bar and a local window manager.

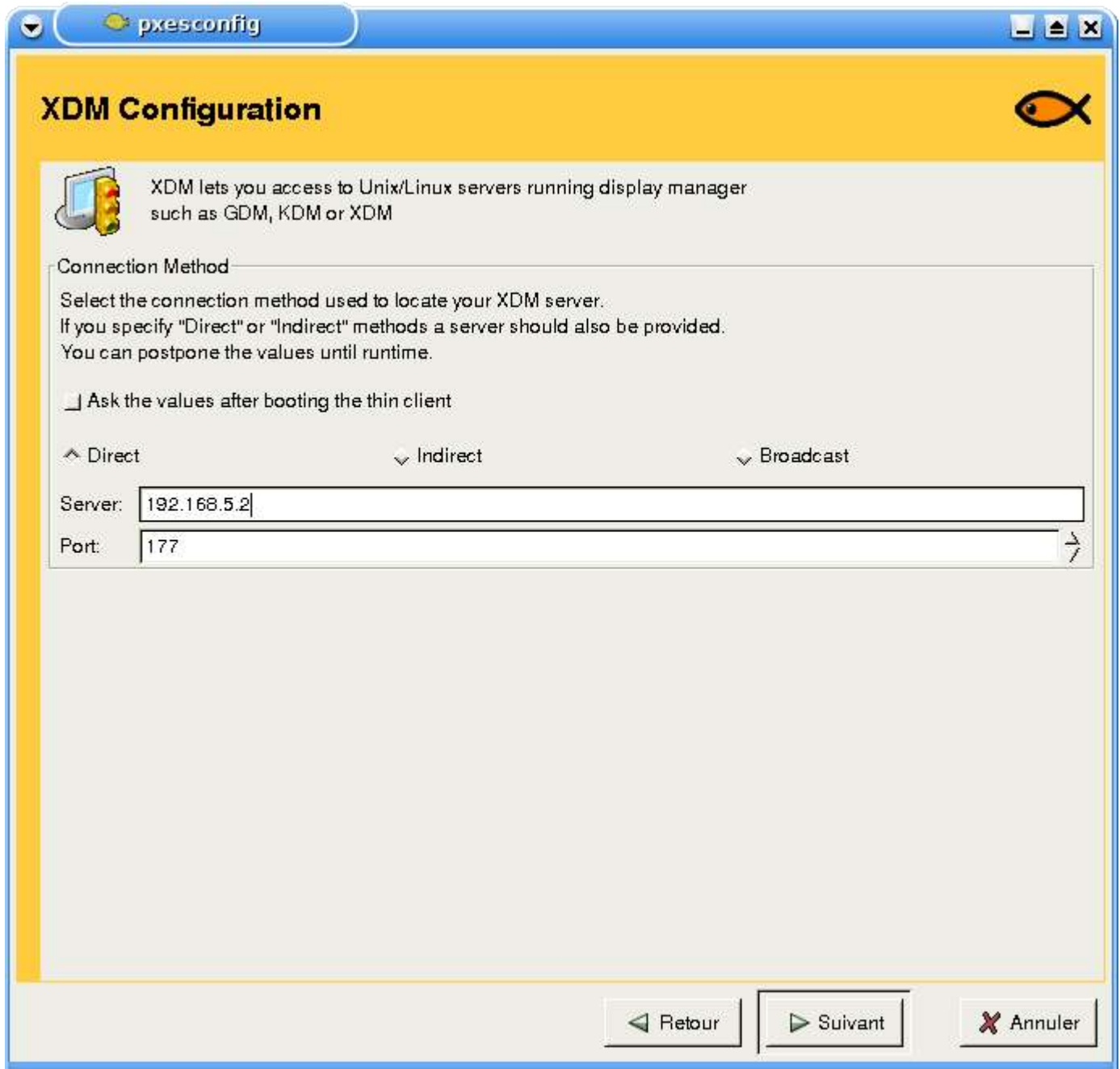
No configuration yet. You can edit the desired configuration files manually.

◀ Retour

▶ Suivant

✖ Annuler

Vous pouvez indiquer sur quelle(s) machine(s) XDM vos clients légers se connecteront.



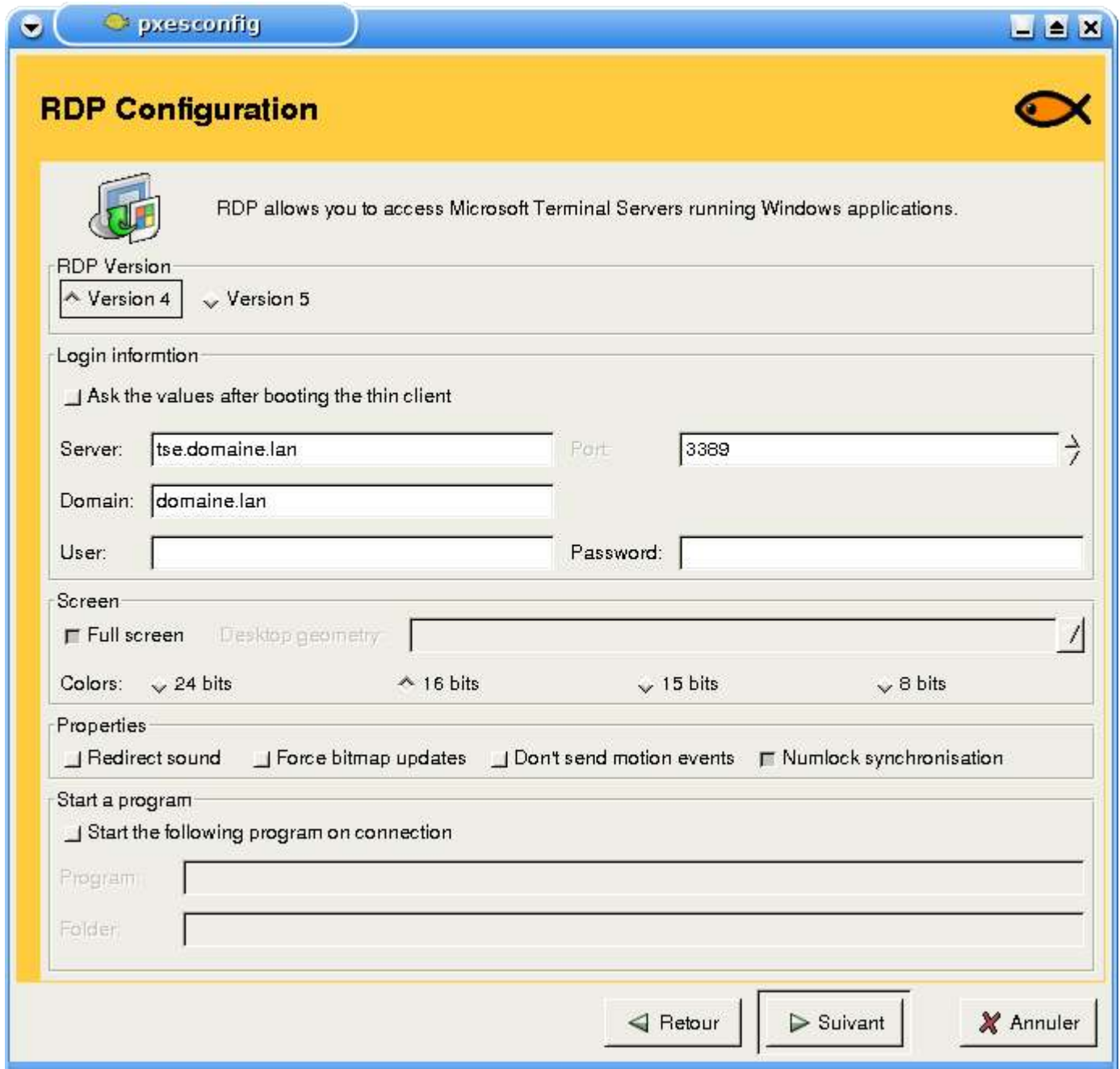
The screenshot shows a window titled "pxesconfig" with a yellow header bar. The main title is "XDM Configuration" in bold black text. Below the title bar, there is a small icon of a computer monitor and a traffic light. To the right of the icon, the text reads: "XDM lets you access to Unix/Linux servers running display manager such as GDM, KDM or XDM".

Below this text is a section titled "Connection Method" with a tabbed interface. The first tab is selected and contains the following text: "Select the connection method used to locate your XDM server. If you specify 'Direct' or 'Indirect' methods a server should also be provided. You can postpone the values until runtime." Below this text is a checkbox labeled "Ask the values after booting the thin client".

Below the checkbox are three radio buttons: "Direct", "Indirect", and "Broadcast". The "Direct" radio button is selected. Below the radio buttons are two text input fields: "Server:" with the value "192.168.5.2" and "Port:" with the value "177".

At the bottom of the window are three buttons: "Retour" (with a left arrow), "Suivant" (with a right arrow), and "Annuler" (with a red X).

Version RDP 4 pour Window\$ 2000 Server et 5 pour 2003 Server.



The image shows a window titled "pxesconfig" with a yellow header bar. The main title is "RDP Configuration" in bold black text. Below the title is a small icon of a computer monitor with a green arrow pointing to it. To the right of the icon is the text: "RDP allows you to access Microsoft Terminal Servers running Windows applications."

The configuration is organized into several sections:

- RDP Version:** A dropdown menu showing "Version 4" selected, with "Version 5" as an option.
- Login information:** A section with a checkbox "Ask the values after booting the thin client" (unchecked). Below it are input fields for "Server:" (containing "tse.domaine.lan"), "Port:" (containing "3389"), "Domain:" (containing "domaine.lan"), "User:" (empty), and "Password:" (empty).
- Screen:** A section with a checkbox "Full screen" (checked) and a "Desktop geometry" input field. Below it are color depth options: "Colors:" with dropdowns for "24 bits", "16 bits", "15 bits", and "8 bits".
- Properties:** A section with checkboxes: "Redirect sound" (unchecked), "Force bitmap updates" (unchecked), "Don't send motion events" (unchecked), and "Numlock synchronisation" (checked).
- Start a program:** A section with a checkbox "Start the following program on connection" (unchecked). Below it are input fields for "Program:" and "Folder:".

At the bottom of the window are three buttons: "Retour" (with a left arrow), "Suivant" (with a right arrow), and "Annuler" (with a red X).

VNC Configuration



This allows you to access a Virtual Network Computing session

Login information

☐ Ask the values after booting the thin client

Server:

Display:

Password file:

Screen

☐ Full screen Desktop geometry:

Properties

Compression: fast best JPEG Quality: low high

Security

Shared: ☒ Yes ☐ No



General configuration

- ☐ Enable debug
- ☐ Wait for key press before starting X Windows
- ☐ Wait for key press before connecting to login server
- ☐ Wait for key press on error connecting to login server

Console and Remote Access

- ☐ Enable login shell (accessible through CTRL-ALT-F4 with no authentication)
- ☒ Enable login shell (accessible through CTRL-ALT-F3 authenticated)
- ☐ Enable telnet server
- ☐ Enable SSH server
- ☐ Set root password
- Root password:
- ☐ Enable tiny web server (no authentication)
- ☐ Enable session VNC shadowing (no authentication)

Boot Messages

You may also need 'console=null' in kernel command line to be completely silent

Level: less more

Remote Configuration

The remote configuration server lets you change aspects of the thin client in a per client basis.
The server should be accessible via TFTP.

- ☐ Enable remote configuration

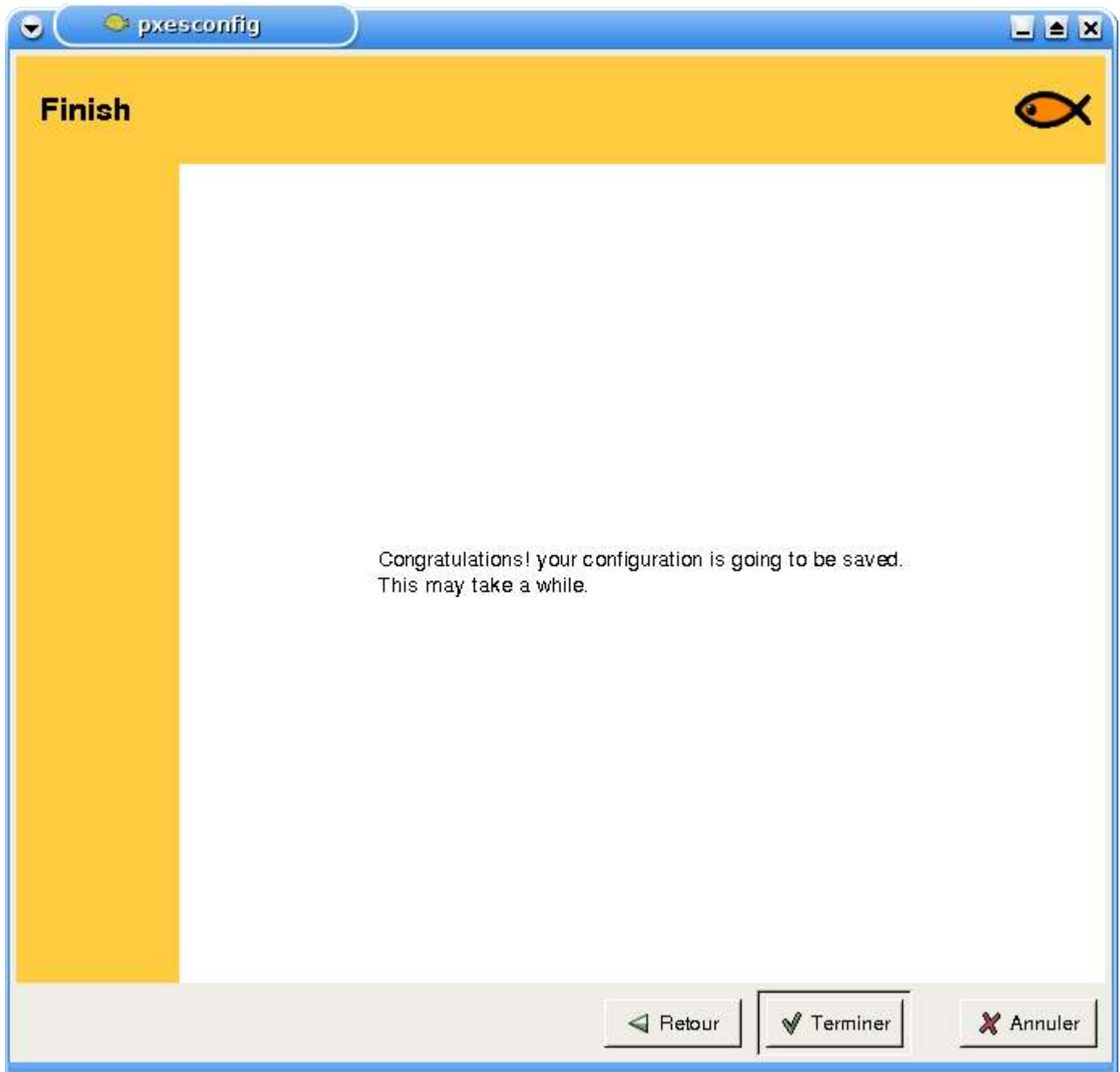
Server:

Directory:

◀ Retour

▶ Suivant

✖ Annuler



Création de ou des images (boot réseau ou boot cdrom) entre 1 et 3 minutes.



Configuration du DNS

Modifiez le fichier **/etc/bind/named.conf** :

```
// Définit les options du serveur dans son ensemble.
include "/etc/bind/named.conf.options";

// Zones locales, pour les résolutions propre à la machine.
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
    allow-transfer { 127.0.0.1; };
    notify no;
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};

// Zone racine contenant les adresses des serveurs DNS racine d'internet.
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

include "/etc/bind/named.conf.local";
```

Modifiez le fichier **/etc/bind/named.conf.options** :

```
options {
    directory "/var/cache/bind";
    pid-file "/var/run/bind/run/bind.pid";

    // Permet de masquer la version de BIND.
    version "SECRET";

    // Indique les serveurs vers lesquelles les requêtes seront
    // retransmettre si votre serveur DNS ne peut répondre.
    forward first;
    forwarders { 192.168.0.1; 192.168.0.5;};
}
```

```
// Indique que le port 53 est le port d'échange entre les serveurs DNS.
// Recommandé lorsque l'on traverse un Firewall.
query-source address * port 53;

// Contient une liste des adresses dont le serveur acceptera ou
// refusera les requêtes :
// 127.0.0.0/8 Autorise localhost.
// Autorise les réseaux 192.168.0.0/24 192.168.5.0/24.
Allow-query { 127.0.0.0/8; 192.168.0.0/24; 192.168.5.0/24; };

// Indique le port en écoute pour les clients et les interfaces.
// Indiquer {*;}; pour écouter toutes les interfaces.
listen-on port 53 { 127.0.0.1; 192.168.5.1; };
};
```

Modifiez le fichier **/etc/bind/named.conf.local** :

```
// Zone de recherche pour le domaine lexa.lan
zone "lexa.lan" {
type master;
file "/etc/bind/db.lexa.lan";
};

// Zone de recherche inversée pour le domaine lexa.lan
zone "5.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.lexa.lan.rev";
};
```

Modifiez le fichier **/etc/bind/db.127** en ajoutant simplement la ligne en rouge :

```
$TTL 604800
@ IN SOA localhost. root.localhost. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
    NS serv1.lexa.lan.
@ IN NS localhost.
1.0.0 IN PTR localhost.
```

Créez le fichier **/etc/bind/db.lexa.lan** :

```
$ORIGIN .
$TTL 259200 ; 3 days
lexa.lan IN SOA serv1.lexa.lan. root.serv1.lexa.lan. (
    31082015 ; serial
    28800 ; refresh (8 hours)
    7200 ; retry (2 hours)
```

```
        2419200      ; expire (4 weeks)
        86400       ; minimum (1 day)
)
NS serv1.lexa.lan.
$ORIGIN lexa.lan.
localhost A 127.0.0.1
serv1 A 192.168.5.1
serv2 A 192.168.5.2
```

Créez le fichier `/etc/bind/db.lexa.lan.rev` :

```
$ORIGIN .
$TTL 259200 ; 3 days
5.168.192.in-addr.arpa IN SOA serv1.lexa.lan. serv1.lexa.lan. (
    31082012 ; serial
    10800 ; refresh (3 hours)
    3600 ; retry (1 hour)
    604800 ; expire (1 week)
    86400 ; minimum (1 day)
)
IN NS serv1.lexa.lan.
IN NS serv5.lexa.lan.
$ORIGIN 5.168.192.in-addr.arpa.
; adresses IP inverses
1 IN PTR serv1.lexa.lan.
2 IN PTR serv2.lexa.lan.
```

Modifiez le fichier `/etc/resolv.conf` du serveur DNS :

```
search lexa.lan local
nameserver 127.0.0.1
nameserver 192.168.0.1
```

Configuration du DHCP

Modifiez le fichier **/etc/dhcp3/dhcpd.conf** :

```
# Pas de mise à jour DNS.
ddns-update-style none;

# Indique que notre serveur fait autorité sur le réseau.
authoritative;

# Refuse les adresses MAC en double.
deny duplicates;

# Ignore les messages DHCPDECLINE des clients, permet d'éviter
# l'abandon successif d'adresses.
ignore declines;

# Nom ou adresse du DNS.
option domain-name-servers 192.168.5.1;

# Divers renseignements sont disponible pour paramétrer les clients.
# voir man dhcp-options pour la liste.
option netbios-name-servers 192.168.0.2, 192.168.0.6;

# Indiquez l'adresse de votre réseau ou sous réseau avec son masque.
subnet 192.168.5.0 netmask 255.255.255.0 {

# Nom de votre domaine pour cette zone.
option domain-name "lexa.lan";

# Information sur votre réseau.
option routers 192.168.5.254;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.5.255;

# Plages d'adresses couvertes par DHCP.
range 192.168.5.20 192.168.5.250;
default-lease-time 21600;
max-lease-time 43200;

# Déclaration des adresses fixes.
host serv2 {
hardware ethernet 00:30:04:8C:41:3B;
fixed-address 192.168.5.2;
option host-name "serv2";
}
host fw {
hardware ethernet 00:0B:6E:72:68:01;
fixed-address 192.168.5.254;
option host-name "fw";
}
```

```
# Adresse du serveur TFTP.
next-server 192.168.5.1;

# Nom de l'image à télécharger.
filename "pxes-0.9.nbi";

}
```

Configuration du serveur TFTP

```
# /etc/inetd.conf:  see inetd(8) for further informations.
# Internet server configuration database
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
# Chroot du serveur TFTP dans /var/lib/tftpboot/pxes
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /
var/lib/tftpboot/pxes
```

Relancez inetd :

```
serv2:/home/user# /etc/init.d/inetd restart
```

Création de la disquette etherboot

Pour créer la disquette de boot, vous aurez besoin de récupérer un fichier image etherboot-pci.zdisk sur <ftp://ftp.linbox.com/pub/lbs/pxe/etherboot-pxe/> contenant tous les drivers pour cartes réseau PCI.

Les fichiers .zdisk ou .disk sont des images de disquette.

Les fichiers .iso ou .liso sont des images ISO prêtes à être gravées.

Si vous avez des cartes ISA vous pouvez essayer les images individuelles contenues dans les répertoires 'disk', 'iso' ou 'liso'.

Le fichier 'NIC' peut vous aider à trouver le bon driver d'après l'identifiant PCI de votre carte.

Création de la disquette avec dd :

```
user@serv2:~$ dd if=etherboot-pci.zdisk of=/dev/fd0
```


Configuration du serveur XDM

Pour **KDM** :

Editez le fichier de configuration principal de KDE :

/etc/kde3/kdm/kdmrc pour Debian ou **/usr/share/config/kdm/kdmrc** pour Mandrake et modifiez les sections [Xdmcp] et [X*-Core] :

```
[Xdmcp]
# Whether KDM should listen to XDMCP requests.
#Enable=false
Enable=true
# The UDP port KDM should listen on for XDMCP requests. Don't change the 177.
Port=177
...

[X*-Core]
...
# Allow root logins? Default is true
AllowRootLogin=false
# Allow to log in, when user has set an empty password? Default is true
AllowNullPasswd=false
# Who is allowed to shut down the system. This applies both to the
# greeter and to the command FiFo. Default is All
# "None" - no "Shutdown..." button is shown at all
# "Root" - the root password must be entered to shut down
# "All" - everybody can shut down the machine (Default)
AllowShutdown=Root
...
```

Pour **GDM** :

Editez le fichier de configuration principal de GDM :

/etc/gdm/gdm.conf pour Debian ou **/etc/X11/gdm/gdm.conf** pour Mandrake et modifiez les sections [security] et [xdmcp] :

```
[security]
AllowRoot=false
AllowRemoteRoot=false
# This will allow remote timed login
AllowRemoteAutoLogin=false
...

[xdmcp]
# Distributions: Ship with this off. It is never a safe thing to leave
# out on the net. Setting up /etc/hosts.allow and /etc/hosts.deny to only
# allow local access is another alternative but not the safest.
# Firewalling port 177 is the safest if you wish to have xdmcp on.
# Read the manual for more notes on the security of XDMCP.
Enable=true
...
# The port. 177 is the standard port so better keep it that way
```

```
Port=177
```

```
...
```

Editez le fichier de contrôle d'accès des connexions XDMCP **/etc/X11/xdm/Xaccess** et dé-commentez cette ligne :

```
...
```

```
*    #any host can get a login window
```

```
...
```

Redémarrez la machine pour que les modifications soient prise en compte.

Connexion des clients légers XDM

Vous pouvez authentifier les utilisateurs qui se connecteront au serveur X et d'applications en local et auprès d'un serveur OpenLDAP.

Merci à Thierry et Charlyp pour leur travail.

Document mis à jour : 12/12/04