Server Operating Systems

Lecture 13
Networking 2

Startup and Initialisation

- NFS
  - NFS Server
  - NFS Client
  - Installing the OS via NFS
  - Exporting home directories
- NIS
  - NIS Server
  - NIS Client
  - Problems with NIS
- LDAP

Network File System

Network File System (NFS) is a network file system protocol originally developed by Sun Microsystems in 1984.

It allows a user on a client computer to access files over a network as easily as if the files were on its local disks.

NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.

The Network File System is an open standard defined in RFCs, allowing anyone to implement the protocol.

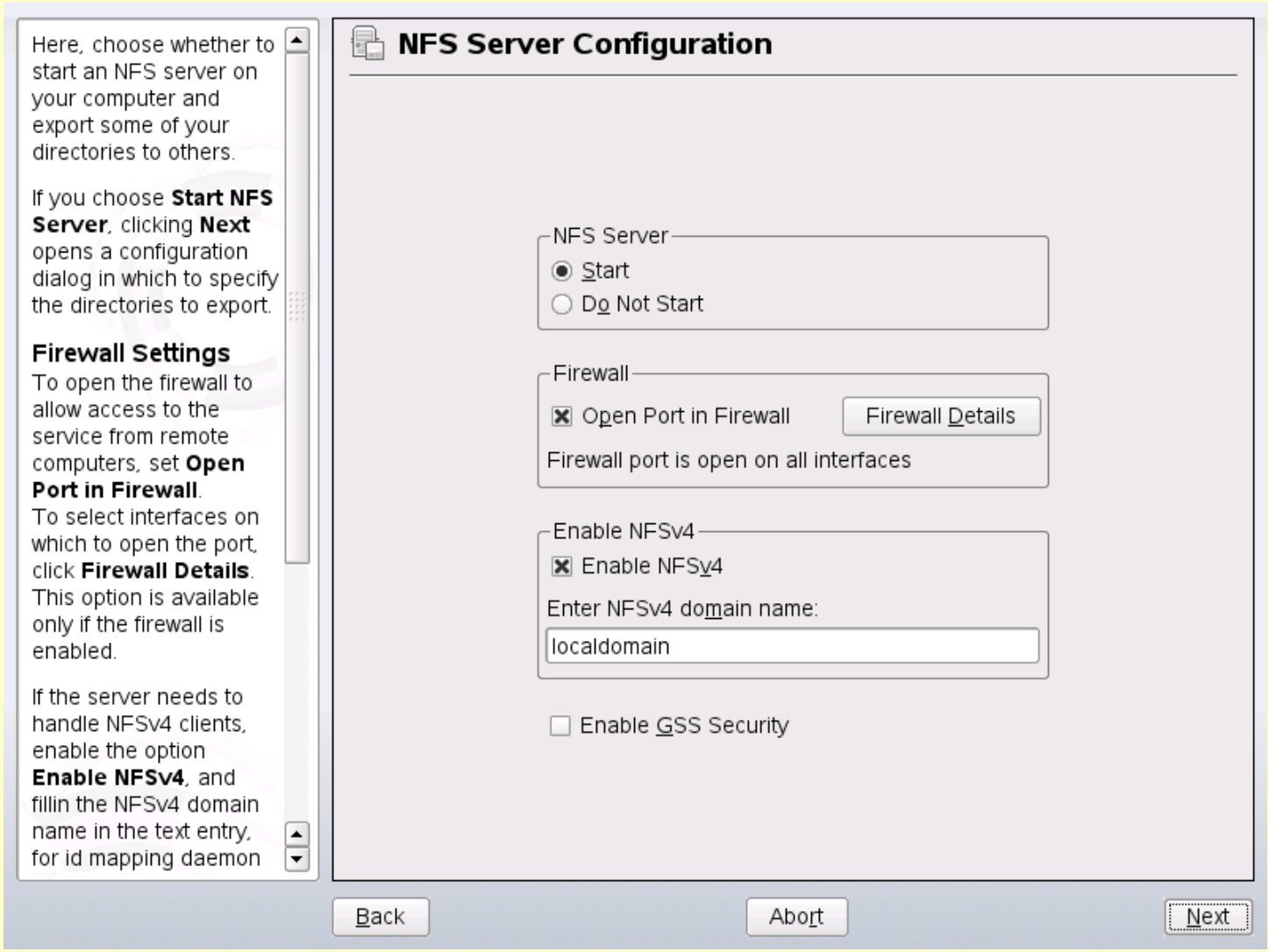
It is a client / server protocol.

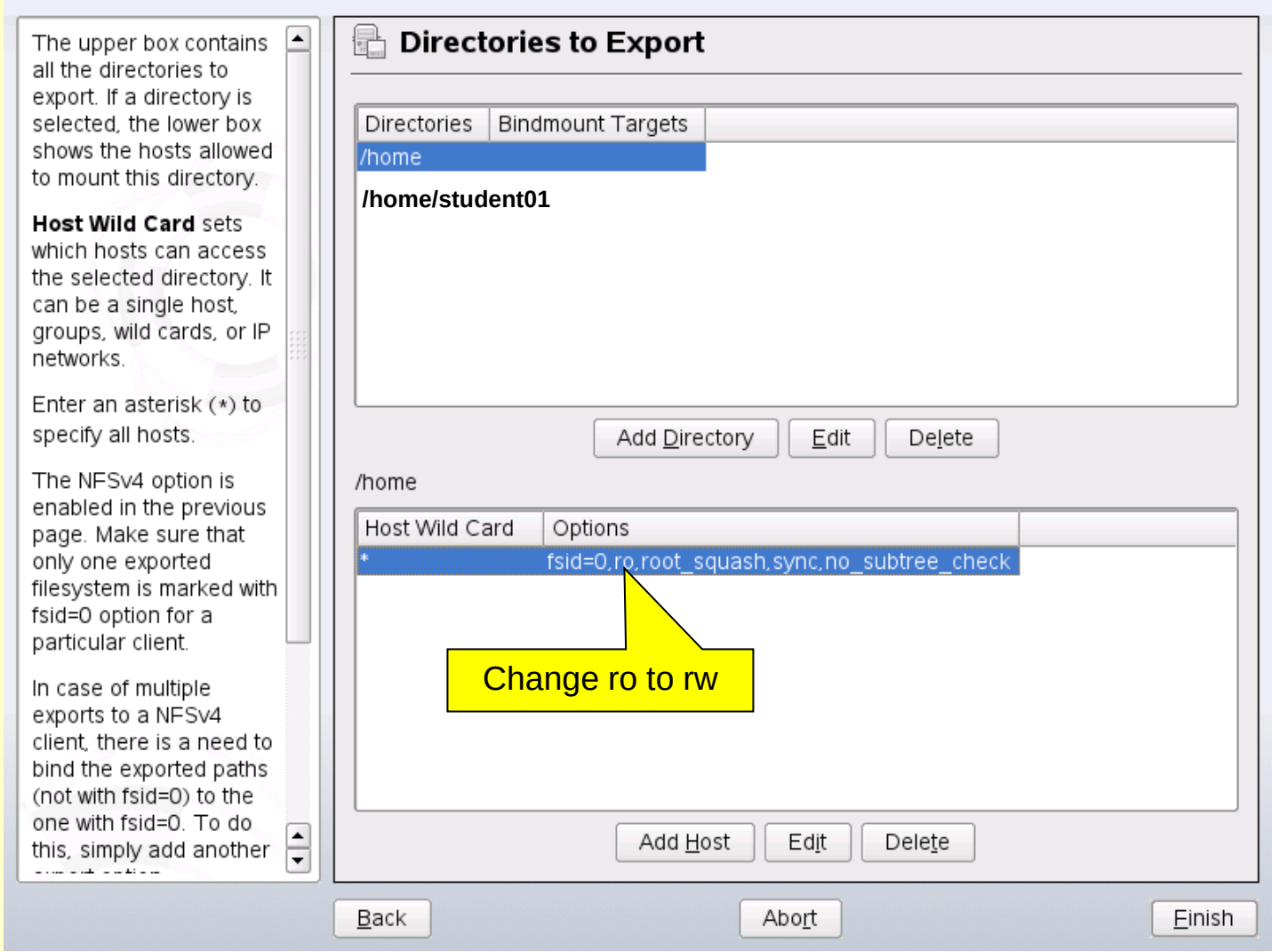
NFS Server Daemon

You need to specify:

Which directories you wish to export

Which hosts are allowed to access them

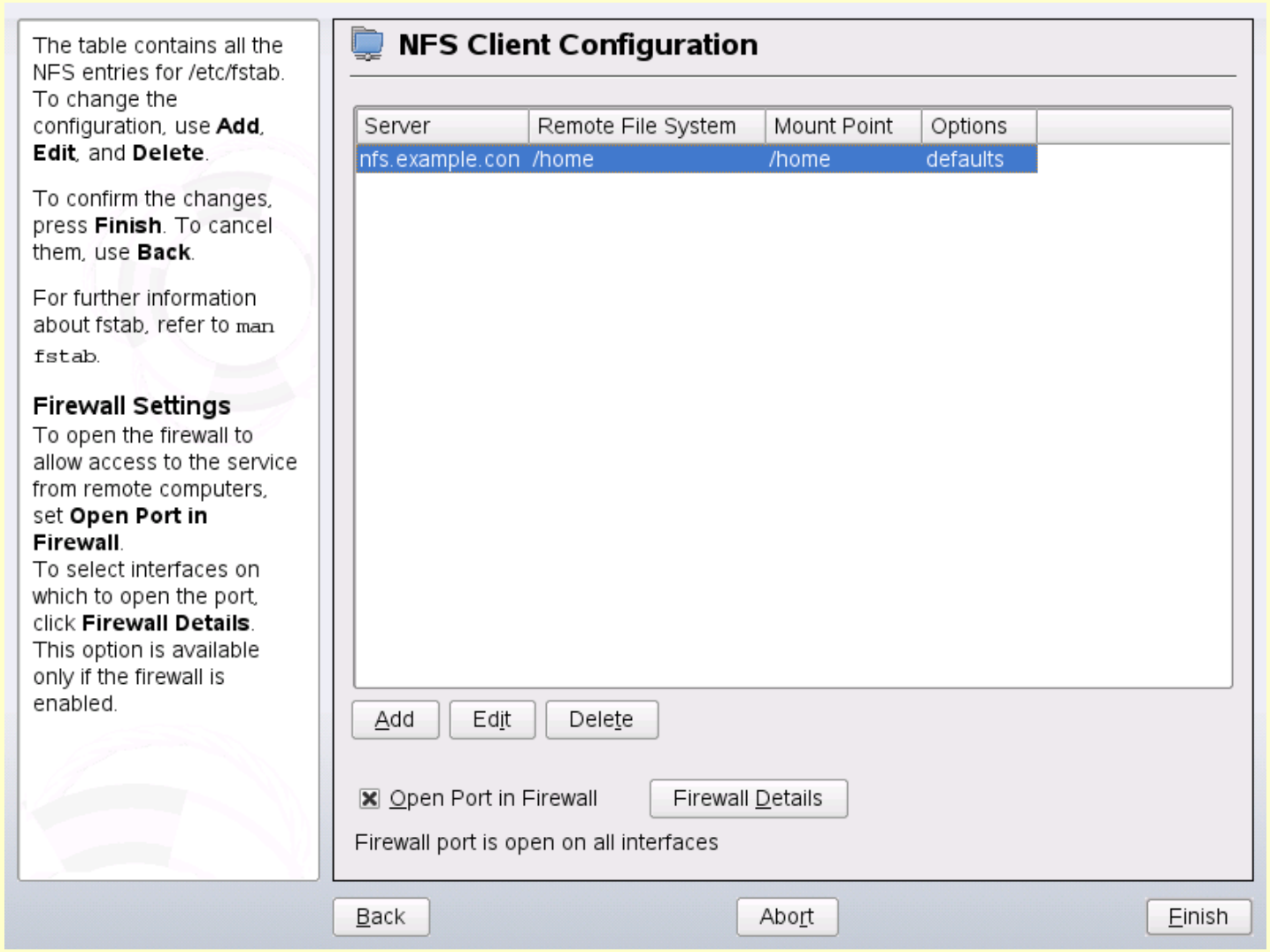

Here, choose whether to start an NFS server on your computer and export some of your directories to others.
If you choose Start NFS Server, clicking Next opens a configuration dialog in which to specify the directories to export.
Firewall Settings
To open the firewall to allow access to the service from remote computers, set Open Port in Firewall.
To select interfaces on which to open the port, click Firewall Details. This option is available only if the firewall is enabled.
If the server needs to handle NFSv4 clients, enable the option Enable NFSv4, and fillin the NFSv4 domain name in the text entry, for id mapping daemon
NFS Server Configuration
NFS Server
Start
Do Not Start
Firewall
Open Port in Firewall
Firewall Details
Firewall port is open on all interfaces
Enable NFSv4
Enable NFSv4
Enter NFSv4 domain name:
localdomain
Enable GSS Security
Back
Abort
Next


The upper box contains all the directories to export. If a directory is selected, the lower box shows the hosts allowed to mount this directory.
Host Wild Card sets which hosts can access the selected directory. It can be a single host, groups, wild cards, or IP networks.
Enter an asterisk (*) to specify all hosts.
The NFSv4 option is enabled in the previous page. Make sure that only one exported filesystem is marked with fsid=0 option for a particular client.
In case of multiple exports to a NFSv4 client, there is a need to bind the exported paths (not with fsid=0) to the one with fsid=0. To do this, simply add another
Directories to Export
Directories
Bindmount Targets
/home
/home/student01
Add Directory
Edit
Delete
/home
Host Wild Card
Options
*
fsid=0,ro,root_squash,sync,no_subtree_check
Change ro to rw
Add Host
Edit
Delete
Back
Abort
Finish

NFS Client

You need to specify:

- The server name / ip address
- The directories you wish to import
- The mount point on your local system for the directory.


The table contains all the NFS entries for /etc/fstab. To change the configuration, use **Add**, **Edit**, and **Delete**.
To confirm the changes, press **Finish**. To cancel them, use **Back**.
For further information about fstab, refer to `man fstab`.
Firewall Settings
To open the firewall to allow access to the service from remote computers, set **Open Port in Firewall**.
To select interfaces on which to open the port, click **Firewall Details**. This option is available only if the firewall is enabled.
NFS Client Configuration
Server
Remote File System
Mount Point
Options
nfs.example.con
/home
/home
defaults
Add
Edit
Delete
Open Port in Firewall
Firewall Details
Firewall port is open on all interfaces
Back
Abort
Finish

Remote Installation Using NFS

You would need to set up a directory containing the contents of the installation DVD.

Export that directory using NFS.

It is possible to export the DVD itself (/media/dvd).

DVD drives are not as fast as hard drives.

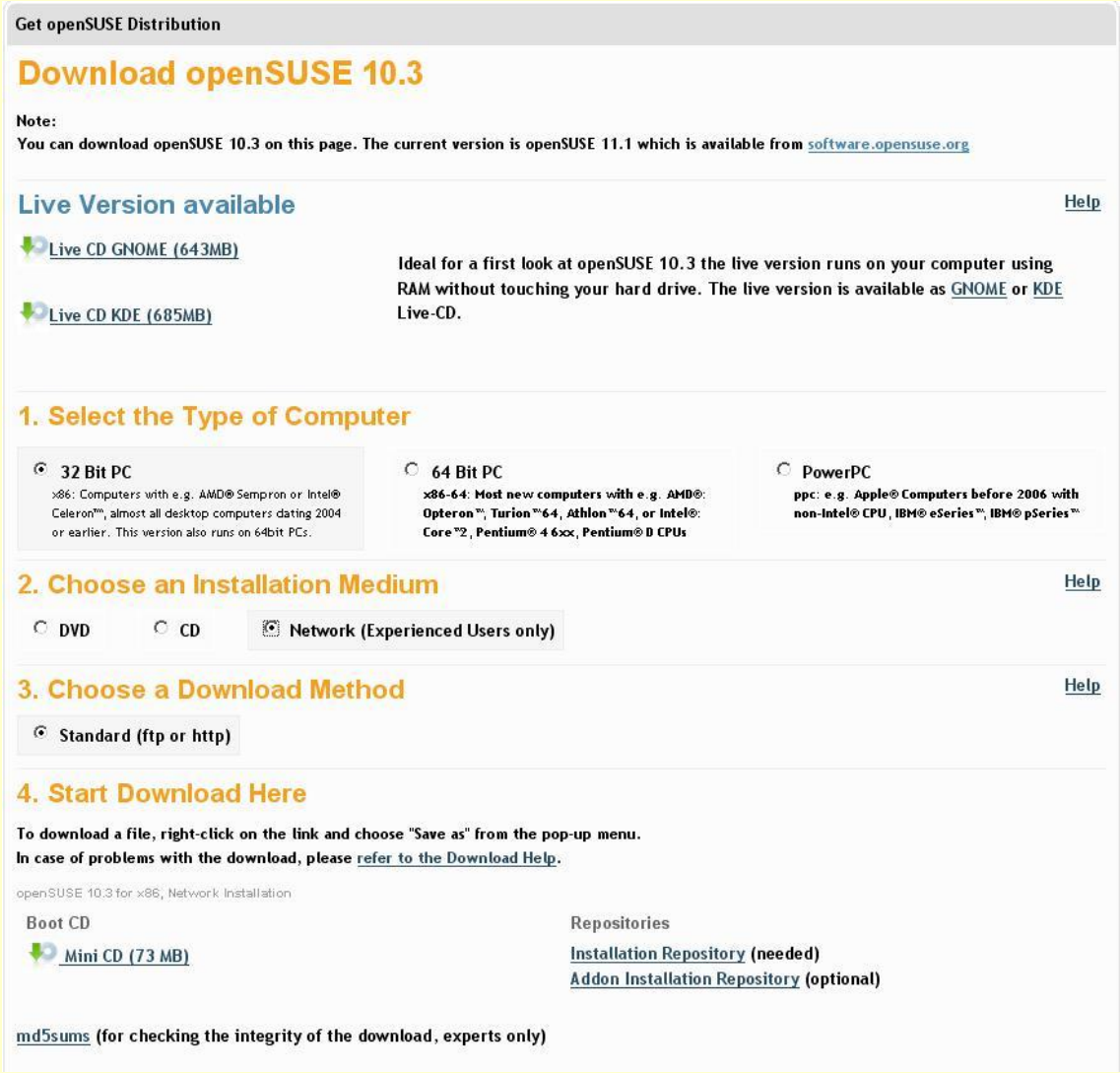
Problem

The client computer has no operating system.

It does not know how to access the NFS Server - or even the network - or even its own disk drives.

You need to have some way of enabling it to do these things.

Suse make available a boot disk iso on their website, specifically designed for network installs.


Get openSUSE Distribution
Download openSUSE 10.3
Note:
You can download openSUSE 10.3 on this page. The current version is openSUSE 11.1 which is available from software.opensuse.org
Live Version available
Help
Live CD GNOME (643MB)
Live CD KDE (685MB)
Ideal for a first look at openSUSE 10.3 the live version runs on your computer using RAM without touching your hard drive. The live version is available as GNOME or KDE Live-CD.
1. Select the Type of Computer
32 Bit PC
x86: Computers with e.g. AMD® Sempron or Intel® Celeron™, almost all desktop computers dating 2004 or earlier. This version also runs on 64bit PCs.
64 Bit PC
x86-64: Most new computers with e.g. AMD®: Opteron™, Turion™64, Athlon™64, or Intel®: Core™2, Pentium® 4 6xx, Pentium® D CPUs
PowerPC
ppc: e.g. Apple® Computers before 2006 with non-Intel® CPU, IBM® eSeries™, IBM® pSeries™
2. Choose an Installation Medium
Help
DVD
CD
Network (Experienced Users only)
3. Choose a Download Method
Help
Standard (ftp or http)
4. Start Download Here
To download a file, right-click on the link and choose "Save as" from the pop-up menu.
In case of problems with the download, please refer to the Download Help.
openSUSE 10.3 for x86, Network Installation
Boot CD
Mini CD (73 MB)
Repositories
Installation Repository (needed)
Addon Installation Repository (optional)
md5sums (for checking the integrity of the download, experts only)

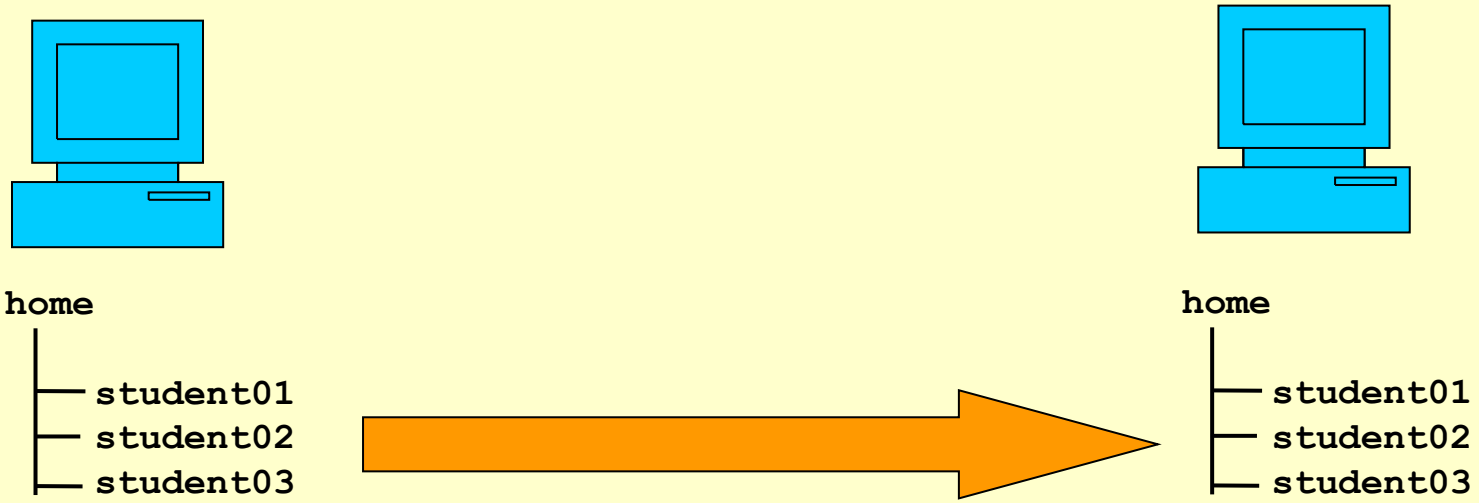
This boot CD must contain at least

- Hardware detection
- Lots of drivers (esp for network cards)
- Kernel
- NFS Client software

Enough to allow it to communicate with the NFS server, and locate the installation DVD.

Installation will then proceed as though the DVD were in the drive of the local machine.

Exporting Home Folders to Clients



Create 3 student accounts on server computer.

This will create 3 home directories in /home.

Change protections on all folders to rwx------

Configure NFS Server to export each home directory.

Create 3 empty folders in home on client computer.

These will act as mount points for the exported NFS folders.

Configure NFS client to import each home directory and mount it on the appropriate mount point.

Network Information Services - NIS

A distributed database service that allows a single set of configuration files to be maintained for an entire network.

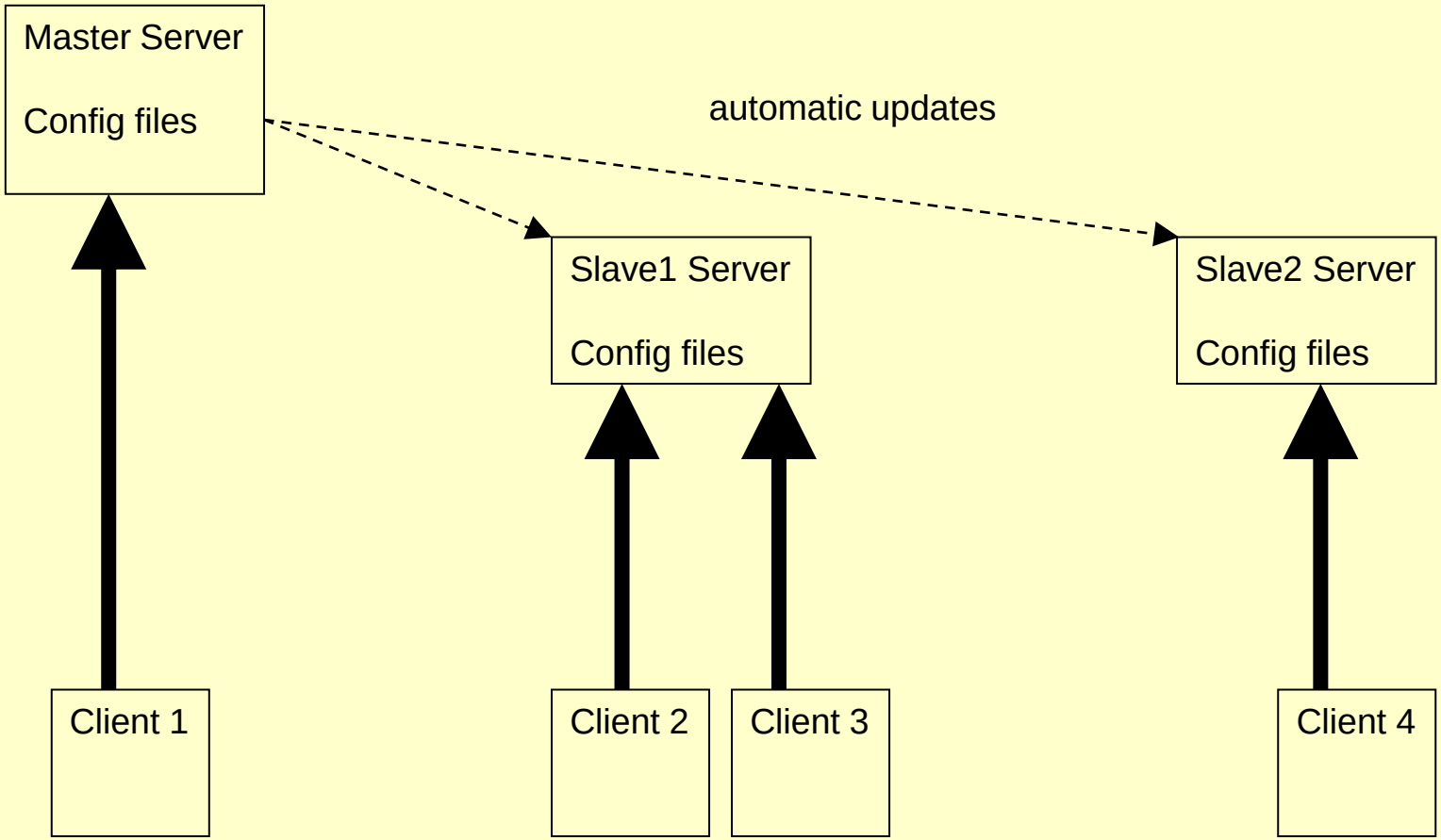
eg a single password file can be used by all hosts.

The password file contains a list of users and their logon details

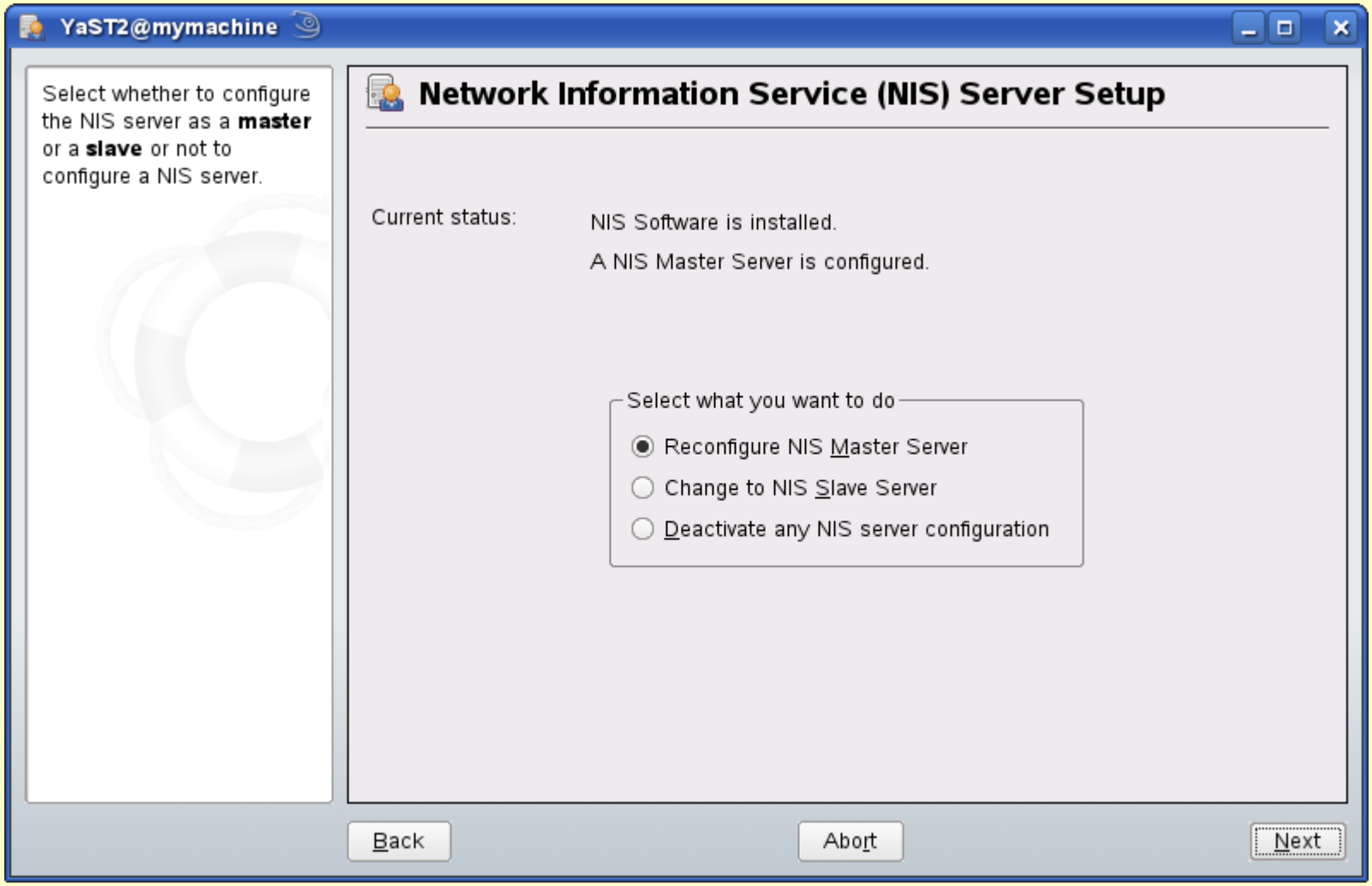
You can log on, on any host on the network.

Configuration files that are shared

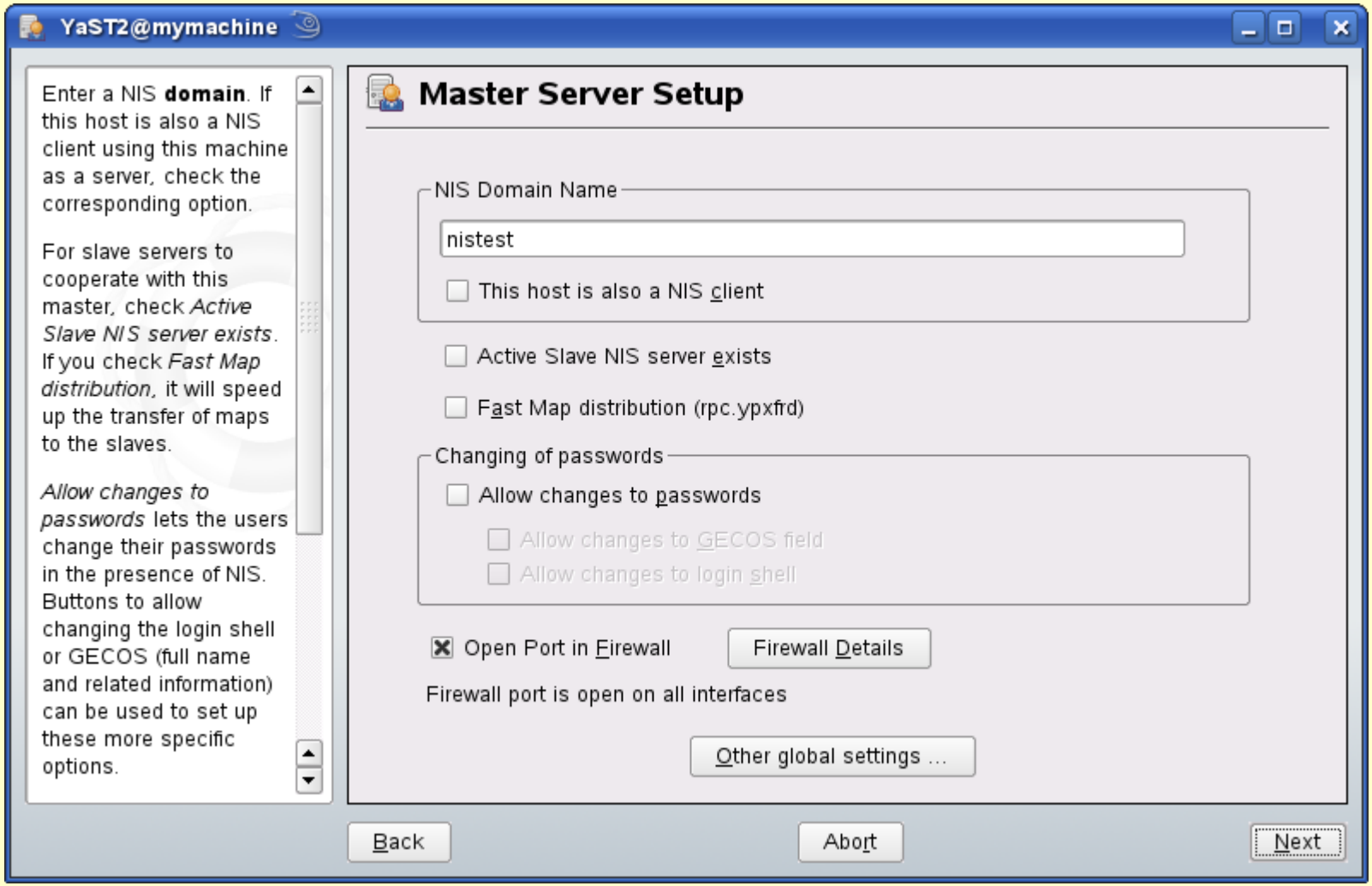
auto.master	list of disk partitions which should be mounted on filesystem
ethers	list of MAC addresses and IP addresses on network
group	user groups on system
hosts	hostnames and IP addresses
netgrp	network wide groups
networks	known local area networks
passwd	user accounts and passwords
printcap	installed printer settings
protocols	network protocols and port numbers
rpc	remote procedure call program numbers
services	network services and port numbers
shadow	encrypted user passwords


Master Server
Config files
automatic updates
Slave1 Server
Config files
Slave2 Server
Config files
Client 1
Client 2
Client 3
Client 4

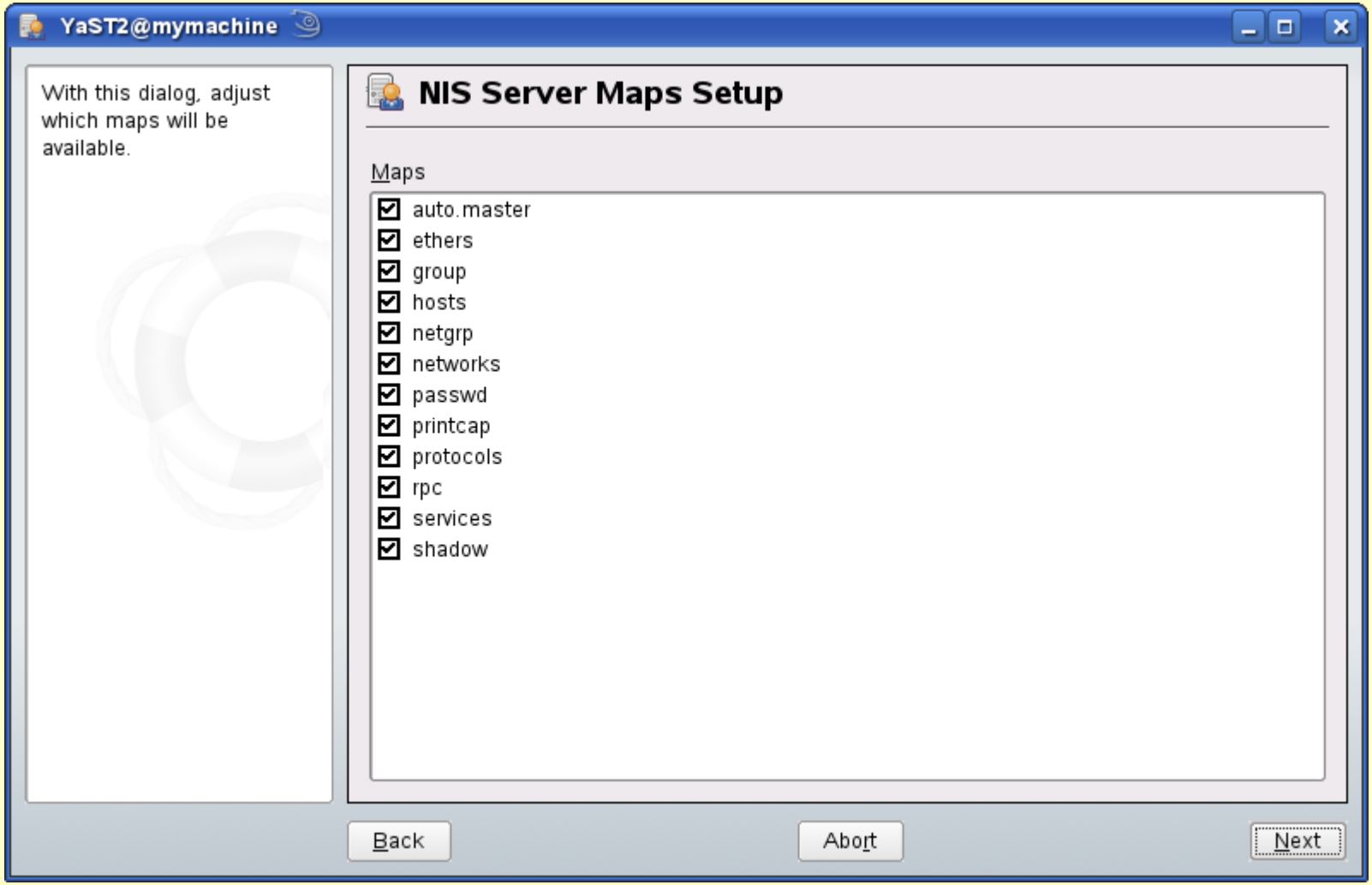
Yast2 > Network Services > NIS Server



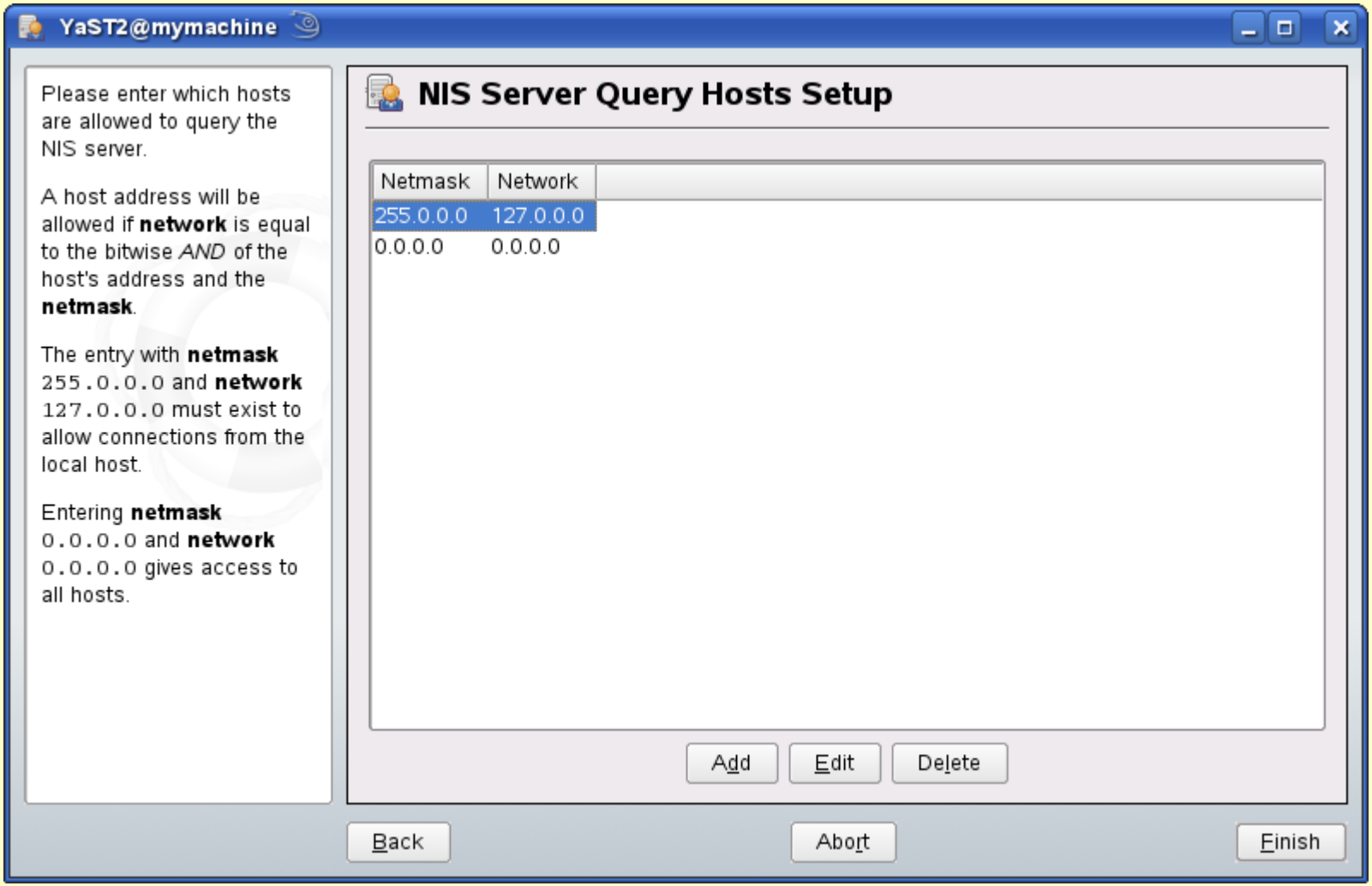
NIS Server


YaST2@mymachine
Enter a NIS domain. If this host is also a NIS client using this machine as a server, check the corresponding option.
For slave servers to cooperate with this master, check Active Slave NIS server exists. If you check Fast Map distribution, it will speed up the transfer of maps to the slaves.
Allow changes to passwords lets the users change their passwords in the presence of NIS. Buttons to allow changing the login shell or GECOS (full name and related information) can be used to set up these more specific options.
Master Server Setup
NIS Domain Name
nistest
This host is also a NIS client
Active Slave NIS server exists
Fast Map distribution (rpc.ypxfrd)
Changing of passwords
Allow changes to passwords
Allow changes to GECOS field
Allow changes to login shell
Open Port in Firewall
Firewall Details
Firewall port is open on all interfaces
Other global settings ...
Back
Abort
Next

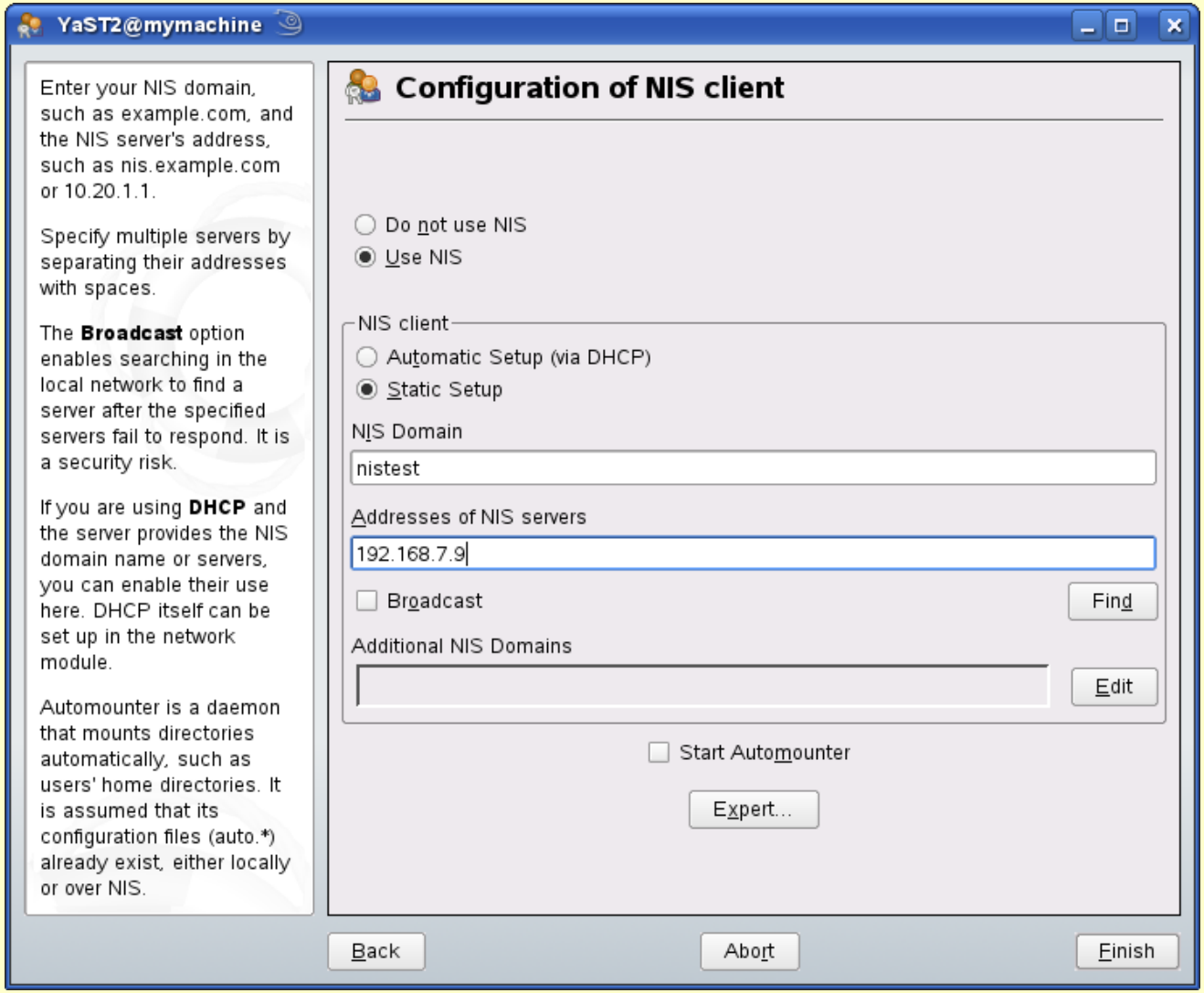
NIS Server


YaST2@mymachine
With this dialog, adjust which maps will be available.
NIS Server Maps Setup
Maps
auto.master
ethers
group
hosts
netgrp
networks
passwd
printcap
protocols
rpc
services
shadow
Back
Abort
Next

NIS Server


YaST2@mymachine
Please enter which hosts are allowed to query the NIS server.
A host address will be allowed if network is equal to the bitwise AND of the host's address and the netmask.
The entry with netmask 255.0.0.0 and network 127.0.0.0 must exist to allow connections from the local host.
Entering netmask 0.0.0.0 and network 0.0.0.0 gives access to all hosts.
NIS Server Query Hosts Setup
Netmask
Network
255.0.0.0
127.0.0.0
0.0.0.0
0.0.0.0
Add
Edit
Delete
Back
Abort
Finish

NIS Client


YaST2@mymachine
Enter your NIS domain, such as example.com, and the NIS server's address, such as nis.example.com or 10.20.1.1.
Specify multiple servers by separating their addresses with spaces.
The Broadcast option enables searching in the local network to find a server after the specified servers fail to respond. It is a security risk.
If you are using DHCP and the server provides the NIS domain name or servers, you can enable their use here. DHCP itself can be set up in the network module.
Automounter is a daemon that mounts directories automatically, such as users' home directories. It is assumed that its configuration files (auto.*) already exist, either locally or over NIS.
Configuration of NIS client
Do not use NIS
Use NIS
NIS client
Automatic Setup (via DHCP)
Static Setup
NIS Domain
nistest
Addresses of NIS servers
192.168.7.9
Broadcast
Find
Additional NIS Domains
Edit
Start Automounter
Expert...
Back
Abort
Finish

You should now find that you are able to log on to any of the user accounts on the server machine, as well as the client machine.

If you have exported the home directories using NFS, you will be able to store files in your home directory on the server from the client machine.

NIS Problems

Note that NIS was designed for an open environment where significant trust among the systems was assumed.

It has been called a security nightmare.

NIS+ only fixed some of the more gaping security holes.

The Unix system administrator traditionally uses the NIS service for name resolution and data distribution in a network.

The configuration data contained in the files in /etc and the directories group, hosts, mail, netgroup, networks, passwd, printcap, protocols, rpc, and services are distributed by clients all over the network.

These files can be maintained without major effort because they are simple text files.

Lightweight Directory Access Protocol - LDAP

The handling of larger amounts of data, however, becomes increasingly difficult due to nonexistent structuring.

NIS is only designed for Unix platforms. This means it is not suitable as a centralized data administration tool in heterogeneous networks.

Unlike NIS, the LDAP service is not restricted to pure Unix networks. Windows servers (from 2000) are LDAP compliant. Application tasks mentioned above are additionally supported in non-Unix systems.

The LDAP principle can be applied to any data structure that should be centrally administered.

A few application examples are:

- Employment as a replacement for the NIS service
- Mail routing (postfix, sendmail)
- Address books for mail clients, like Mozilla, Evolution, and Outlook
- Administration of zone descriptions for a BIND9 name server
- User authentication with Samba in heterogeneous networks

This list can be extended because LDAP is extensible, unlike NIS.

The clearly-defined hierarchical structure of the data eases the administration of large amounts of data, because it can be searched more easily

Windows Server 2003 Active Directory is essentially Microsoft's implementation of the LDAP standards.

The standards are laid down by the IETF (Internet Engineering Task Force).

Linux also has LDAP Server and client packages.

These would normally be used on:

- Large networks
- Secure networks
- Networks that also have some Windows machines.