SUSE LINUX

School Server

User and Adminstration Guide

Contents

Preface

In the past, workgroups were often established for the purpose of preparing an easy-to-install, easy-to-use Linux distribution for the specific needs of schools. However, these attempts usually failed due to the lack of time and expertise. Teachers could not and cannot expect ongoing support from skilled students, as this would lead to a substantial distraction from their main responsibilities. Similarly, teachers and volunteers are not permanently available for maintenance tasks or the development of special software, as they have other important duties.

Accordingly, schools are in need of professional assistance. In view of this situation, the District of Fürth, Germany, commissioned SuSE Linux AG to develop a server that is tuned to the specific needs of schools.

Introduction to This Guide

As prospective SUSE LINUX School Server administrators usually have very little experience in the utilization of computers and especially of Linux-based systems, this guide endeavors to compensate this deficit by providing a detailed description of the operations required for the normal administration.

A wealth of literature such as the SuSE PRESS books (`http://www.susepress.de/`) and various online sources are available for those who wish to gain deeper insight on the elements used in SUSE LINUX School Server. However, this guide should be sufficient for all operations within the scope of the normal deployment of the server at schools.

Experienced users can use the extensive index at the back of the guide in order to find the information they are looking for. The first pages of this book provide some information on the hardware to be used and the network topology of a school network.

The third chapter presents detailed instructions for the installation and launch of SUSE LINUX School Server. Users of recent SuSE Linux distributions will notice how similar the installation is. Only the installation of the network (see 3 on page 34) and the basic configuration of the server (see 3 on page 43) are different from the installation of a normal SuSE Linux distribution.

Chapter 4 on page 51 provides information about the actual administration of the running server, guiding you step by step through the individual components of the administration interface. You will learn how to set up and administer user and machine accounts and adapt various server services to your needs.

Chapter 8 on page 151 contains the explanations of the teacher guide in abbreviated form, thus enabling you to provide quick assistance if teachers and students have questions regarding their server accounts.

Requirements for School Servers

The requirements for a computer network in a school environment – i.e. for a pedagogical network – are more complex than the requirements for an office environment. Crashed Windows workstations must be restorable with a button click within a few minutes, for example during a final exam on the computer or between lessons.

For some lessons, you may want to be able to deactivate the access to the Internet and various communication possibilities such as e-mail, FTP, SSH, and so forth. Of course, LAN (intranet) requirements such as the following must also be met:

- Security against external access (firewall)

- Controlled Internet access

- Intranet with internal WWW pages, FTP access, and e-mail

- Stable file server with backup

- Stable print server

- Easy graphical user administration (with the possibility of creating user accounts automatically)

- Easy network analysis

- Easy installation updates

These requirements can be met to a high degree by deploying one or several Linux servers. The advantages of Linux include low acquisition costs, high stability, and flexibility. A number of schools and educational institutions have already presented numerous concepts for the use of Linux as server platform in school environments. During their free time, many computing, mathematics, and physics teachers have produced excellent solutions on the basis of diverse Linux distributions. So far, however, there has not been any Linux product which not only fulfills specific school requirements but also includes long-term professional support and maintenance.

SUSE LINUX School Server meets these criteria by combining and adapting existing SuSE business products and technologies, by employing the expertise collected at schools, and by means of an effective network topology.

Our goal was and is to develop a product that meets the requirements of schools as fully as possible. As the size of schools varies, we designed our product to be highly scalable. Information on SuSE Linux Enterprise Server and the base products is available on the SUSE LINUX School Server CD-ROM in the directory `doku`.

Acknowledgement

We would like to express our gratitude to the beta testers and all others who assisted, especially the teachers and students of high schools and secondary schools in Franken (Markus Bölling, Dieter Kroemer, Gerhard Miedaner, Michael Schmidt, and others) and the DoSys staff (Markus Klappenbach, Ralf Grevinga, and others).

Typographical Conventions

The following typographical conventions are used in this book:

Format	Meaning
YaST	Program
/etc/passwd	File or directory
⟨*placeholder*⟩	Replace `placeholder` (and the angle brackets) with the actual value
PATH	Environment variable PATH
192.168.1.2	Value of a variable
ls	Command
user	User
earth:~ # **ls**	Input of `ls` in the shell of the user `root` in the home directory on the host "Earth"
newbie@earth:~ > **ls**	Input of `ls` in the shell of the user `tux` (official name of the Linux penguin) in the home directory on the host "Earth"
C:\> **fdisk**	DOS prompt with the command input `fdisk`
(Alt)	Key to press; keys to press sequentially are separated by spaces
(Ctrl) + (Alt) + (Del)	Keys to press simultaneously are connected with '+'
"Permission denied"	System message
'System Update'	Menu item, button

<

2

Preliminary Steps

SUSE LINUX School Server is a powerful product based on SuSE Linux Enterprise Server. It is designed to provide an efficient, full-featured e-mail, file, print, and groupware server without requiring intensive configuration.

Nevertheless, do not simply insert the CD in the drive and launch the installation. Though the procedure is speedy, the individual steps are very complex. Many individual elements must be considered and adapted.

Before you start the actual installation, consider how you want to utilize SUSE LINUX School Server and make some notes. This will save you a lot of work later on.

Use the memo in the annex 9 on page 167 for this purpose. The more information you record about your server, the easier the system maintenance will be.

Hardware Requirements

The installation of SUSE LINUX School Server on x86 systems is usually easy.
The following frame conditions are recommended:

- RAM: At least 256 MB; 512 MB or more recommended

- CPU: One CPU with at least 400 MHz (K6, Celeron, Pentium II); 1 GHz or
  more (Athlon, PIII) recommended.

- Hard disk: At least 20 GB of free space; 40 GB or more recommended.

- Network adapter: Network adapter(s) supported by SuSE Linux. If you
  want to run the server without an Internet connection or access the Inter-
  net by way of ISDN or a modem, one network adapter is sufficient. For all
  other constellations, we recommend at least 2 separate (different) network
  adapters.

- Graphics card: VGA card supported by SuSE Linux. We recommend a
  graphics card and a monitor with a resolution of 1024 x 786 @ 75 Hz.

Special Hardware Requirements

Normally, a server runs day and night on 7 days a week. Therefore, a failure of
the server usually triggers a failure of the entire system, resulting in the cancel-
lation of the respective lessons. For this reason, the operability of the hardware
is critical.

- As a defective RAM can cause server crashes that cannot be controlled or
  reconstructed, use quality products and run a memory test utility (such as
  Memtest – see 3 on page 17) for at least 24 hours prior to the installation.

- SCSI hard disks are designed for extended operation and usually last
  longer than comparable IDE hard disks.

- The processor and the hard disk(s) generate heat. Avoid an accumulation
  of heat!

- Use network adapters from different manufacturers. In this way, you can
  avoid the same driver from controlling the network adapters. This would
  make it difficult to check which card handles which network areas.

- For the installation in a large network, consider connecting the server with 1 GB network cards. In this case, the subsystem should also be equipped accordingly (RAID system, large RAM), and your switch should have the needed ports.

- An uninterruptible power supply (UPS) makes sure that the server has time to save open files and shut down properly in the event of a sudden power outage. Moreover, the UPS usually protects the hardware from harmful voltage fluctuations. When buying a UPS, make sure the server can read the UPS status by means of a data line.

- As the firmware or BIOS is responsible for initializing the hardware, it has a decisive effect on the system stability. Some hardware problems can be solved by means of a BIOS update.

- To protect your server from accidental physical impact and unauthorized access, place the server and the network hardware in a protected zone to which only authorized persons have access. If you do not have a special server room, you can place it in a cabinet which is set up in front of a power outlet. The cabinet should have adequate space for the Internet connection and the network cables.

The SUSE LINUX School Server Network Structure

Figure 2.1 on the following page shows the basic network structure. The school network is split into several logical subnets.

- The school servers are located in the first subnet ("server network"). If you wish, you can also configure a suitable subnet mask (255.255.255.0) to control the access to network printers by means of SUSE LINUX School Server shares.

- The second subnet is reserved for new, provisional, or mobile workstations.

- The stationary workstations of the school are placed in the other subnets. A separate IP address space is allocated to each room.

This network structure enables room-specific blocking of individual services and rapid identification of network problems.

```
┌─────────────────────────────────────────┐
│              Servernet                   │
│   10.0.0.1–10.0.0.254 resp.              │
│   172.16.0.1–172.16.0.254 resp.          │
│   192.168.0.1–192.168.0.254              │
└─────────────────────────────────────────┘
```

Schoolnet: 10.0.0.0/255.0.0.0 resp. 172.16.0.0/255.255.0.0
resp. 192.168.0.0/255.255.0.0

IP–Pool for new resp. temporary Computer: 10.0.1.1– 10.0.1.254 resp. 172.16.1.1 172.16.1.254 resp. 192.168.1.1 192.168.1.254	Schoolroom 1 10.0.2.1– 10.0.2.62 resp. 172.16.2.1 – 172.16.2.62. resp. 192.168.2.1 – 192.168.2.62	Schoolroom 2 10.0.2.65– 10.0.2.126 resp. 172.16.2.65 – 172.16.2.126. resp. 192.168.2.65 – 192.168.2.126

Figure 2.1: SUSE LINUX School Server Network Structure

SUSE LINUX School Server Services

Following the installation, SUSE LINUX School Server is assigned four different IP addresses. This enables a better control of the access to various SUSE LINUX School Server services and the relocation of various services to other hosts.

These four different IP addresses are assigned various (DNS) names in order to facilitate the allocation of the services running under these addresses.

First Range

- DNS names: `admin`, `dns`, `nfs`, `ldap`, `samba`, `install`, `PDC-SERVER`

- Web server for

  ▷ The self-administration of the users

  ▷ Administering the school server and network

  ▷ Administering of the workstation hosts

  ▷ Special activities for teachers

- File server (NFS/SAMBA/Netatalk)

- Password server (LDAP/SAMBA)

- DHCP server

- Workstation installation server for the automatic installation and updates of SuSE Linux clients

- Workstation configuration tool for the automatic installation

- Backup server

Second Range

- DNS names: `schoolserver`, `mailserver`

- Mail server (SMTP with postfix, IMAP/POP3 with Cyrus)

- Web server for

  ▷ Web mail client

  ▷ Appointment scheduler

  ▷ Forums

  ▷ Various other groupware applications

  ▷ Access to the personal web pages of the SUSE LINUX School Server users

Third Range

- DNS name: `printserver`

- Print server

Fourth Range

- DNS name: `proxy`

- Proxy server with integrated filter for the clients

As mentioned above, SUSE LINUX School Server enables the relocation of these ranges or individual services to other hosts in order to increase the overall system performance.

Domain Name Selection

Before you start with the installation, think of a suitable domain name for your school. It is very difficult to change the domain name after the installation.

> **Caution**
>
> Following the installation, SUSE LINUX School Server will be configured as DHCP server and name server for your intranet. To benefit from the full functionality of SUSE LINUX School Server, shut down any existing DHCP server or name server in your network.
>
> **Caution**

A correctly configured name service (DNS) is significant for the smooth operation of the mail server and facilitates the administration of the entire system. Even if your server does not have an official Internet connection and cannot be accessed directly from the Internet, assign your intranet a suitable domain name. Names such as "schoolname.local" are not suitable, as an e-mail message sent to the Internet with `user@schoolname.local` will never return. So how about something like `<schoolname>.com` – even if you do not yet have any e-mail traffic under this domain name. The advantage of a name like this is that you can continue using it if you set up an Internet presence.

Make sure that the name you want to use is not already reserved. To check whether the desired domain already exists, enter the name in a web browser as a URL (perhaps with `www.`). For details, check `http://www.internic.com/whois.html`.

Installation

The following pages describe the installation and basic configuration of SUSE LINUX School Server with YaST. For a complete installation, power on all hardware components such as printers or external drives. Of course, these devices can also be configured later on. The information in this chapter should be sufficient to tackle most difficulties. Contact our support disk if you need additional assistance.

┌─ **Caution** ───

During the installation, certificates are created for various server services.
If the system clock is not set correctly during the installation (e.g., if the
clock is ahead of time), these certificates may be invalid and the server
may not operate correctly. Therefore, check and adjust the system clock
prior to installation.

────────────────────────────────── **Caution** ─┘

Booting from the CD-ROM

Power the machine on and insert the CD in the drive. SuSE Linux will be loaded
for the installation.

Booting Problems

If the machine does not boot from the CD-ROM, adjust the BIOS settings as fol-
lows:

Adjusting the BIOS Settings

When the machine is booted, the hardware is initialized by the BIOS. Among
other things, the memory is tested. This is evident from the system memory
count. During this process, you can enter the BIOS setup. The key you need to
press to access the BIOS setup is displayed at the bottom of the screen. Usually,
this is (Del) or (F1). Press the respective key to enter the BIOS setup.

If your machine is equipped with an AWARD BIOS, the needed entry is 'BIOS
FEATURES SETUP'. Other manufacturers use similar entries such as 'AD-
VANCED CMOS SETUP'. Select the respective entry and confirm by pressing
(↵).

Look for the subitem that determines the boot sequence of the drive. The default
setting is often C, A or A, C. In the first case, the computer first looks for the
operating system on the hard disk (C) and then on the floppy disk (A). Select
'Boot Sequence' and press (Page ↑) or (Page ↓) (or other keys, depending on the
BIOS) until a suitable sequence such as A, CDROM, C is displayed. Then exit
this screen by pressing (Esc).

To save the changes, select 'SAVE AND EXIT SETUP' or press (F10). You will be
asked whether you want to exit the BIOS setup and save the new settings.

> **Note** ──────────────────────────────
>
>   By default, most machines use a US keyboard layout.
>
> ────────────────────────────── **Note** ┘

For an EIDE (ATAPI) CD-ROM Drive

Set the boot sequence in the BIOS to `CDROM`, `C`, `A` or a similar setting in which the CD-ROM drive is listed first. See 3 on the preceding page.

For a SCSI CD-ROM Drive

Set the boot sequence in the BIOS to `SCSI`, `CDROM`, `A` or a similar setting in which the SCSI adapter is listed first. See 3 on the facing page.

When the machine is booted, the BIOS becomes active. This is followed by the activation of the SCSI host adapter, which has its own BIOS. During this initialization (usually indicated by a special message), you can access the BIOS of the host adapter with the indicated key combination. For example, the BIOS of an Adaptec host adapter can normally be accessed with the key combination (Ctrl) + (A). For a Tekram adapter, the key is (F2) or (F6).

Select the 'Disk Utilities'; the system will check and display the connected hardware. Make a note of the SCSI ID for your CD-ROM drive. Exit the menu with (Esc), go to 'Configure Adapter Settings' → 'Additional Options' → 'Boot Device Options', and press (↵). Enter the ID of the CD-ROM drive and press (↵). Press (Esc) twice in order to return to the start screen of the SCSI BIOS. Confirm with 'Yes' to reboot the machine.

Machine Does Not Support Booting from CD-ROM

If the machine does not support booting from CD-ROM, it has to be booted with a boot disk. Refer to the following Support Database article for more information:

```
http://sdb.suse.de/de/sdb/html/swiegra_bootdiskette80.html
```

Welcome Screen

While the welcome screen is displayed, YaST continues to prepare the installation. The welcome screen offers several options for the further installation procedure.

If you press any key except for the ⏎ key before the timeout, the installation will not be started automatically and you have time to select a different option.

If you have older hardware or hardware that is not optimized for certain functions, problems may occur during the installation. These difficulties are usually caused by the power management mode or the DMA capability of the drives. These problems cannot be checked in advance and sporadically occur during the installation. If you encounter such a problem, reboot the machine and select the item 'Installation – Safe Settings' in the welcome screen. In this mode, some of the new hardware properties are deactivated, which usually enables a correct installation in problematic cases.

Different Graphics Modes for YaST

For the installation, you can choose one of several screen resolutions or a text-based variant. Use the function keys F3 to F5 to select the resolution for the graphical installation mode. The `VGA Graphics Mode (640x480)` should work with all graphics cards.

If necessary, select the text mode with F2 . In the YaST text mode, use the Tab key to navigate between the items in a dialog. Use the ↑ and ↓ to navigate between the menu entries, and press ⏎ to access the next dialog.

Kernel Parameters

Special kernel parameters can be specified in `boot options`. However, these are only needed for very special hardware.

Further Options

Options in the welcome screen:

Installation: The normal installation for which all hardware functions are activated.

Installation - Safe Settings: The DMA function (for the CD-ROM drive) and the power management are deactivated. Additionally, experienced users can specify or edit kernel parameters.

Installation - APIC Enabled: Required for machines with APIC (Advanced Programable Interrupt Controller) support in case the standard installation fails.

Manual Installation: If certain drivers that are loaded automatically for the installation cause problems, select this item to perform a manual installation. In this case, these drivers will not be loaded automatically. However, this will not work if you use a USB keyboard for your machine.

The text mode of YaST will be started, allowing you to specify the needed drivers.

Rescue System: If you no longer have access to your installed Linux system, boot the machine with the inserted DVD or CD1 and select this item which will start a small Linux system without graphical interface, enabling advanced users to access the hard disks and repair errors in the installed system.

More information is available in the annex of the online manual at `http://admin/manual/manualEN.pdf`.

Memory Test: Tests the system memory by means of repeated write and read cycles. As memory errors often occur sporadically and can only be detected after many write and read cycles, this test runs continuously. If you suspect the memory of being defective, allow the test to run for several hours. If no errors are reported, you can assume that the memory is intact. Reboot the machine to terminate the test.

Boot Installed OS: Boots your system from the hard disk (the system that is normally booted when the machine powered on).

A few seconds after the welcome screen, SUSE LINUX School Server will load a small Linux system that controls the further installation procedure. Various messages and copyright notes will appear on the screen. When the loading process is completed, the installation utility YaST will be started. After a few seconds, you will see the graphical interface that will guide you through the installation procedure.

YaST Takes Over

This is where the actual installation with the installation utility YaST begins. YaST dialogs follow a consistent pattern; all input fields, selection lists, and buttons can be controlled with the mouse.

If your mouse pointer does not move, your mouse was not autodetected. In this case, use the arrow keys and the ⎸Tab⎹ key to navigate to the desired menu item and press ⎸↵⎹. The configuration of the mouse is described in 3 on the next page.

Language Selection

For the installation, YaST will be set to the language you select. The language setting will also be used for your keyboard layout. Moreover, YaST will set the standard time zone that is most likely for your language setting.

Installation Settings

Following the hardware detection (and possibly the manual configuration of the mouse), the proposal screen will display information about the detected hardware and proposals for the installation and partitioning. After entering and configuring a module, you will be taken back to the proposal screen with the modified values. The individual configuration settings are described below.

Mode

This item should always be set to 'New installation'. Do not change this setting.

Keyboard Layout

Select a keyboard layout in this dialog. Usually, the keyboard layout corresponds to the selected language. Press special characters to make sure that they are displayed correctly. Click 'Next' to return to the proposal screen.

Mouse

If YaST did not autodetect the mouse, use the (Tab) key to highlight 'Change', press (Space), and use the arrow keys to select the menu item 'Mouse'.

Use (↑) and (↓) to select the mouse type. Refer to your mouse documentation for details. Confirm the selected mouse type by pressing (Alt) + (T) or by pressing (Tab) and then (↵).

Test the mouse. If the mouse pointer on the screen follows your movements, this installation step was successful. If the pointer does not move, select a different mouse type and try again.

Click 'Accept' to save the settings and return to the proposal screen.

Partitioning

During the installation, you can split the available disk space into several sections (partitions). This process is called partitioning. The partitioning proposal of YaST can be changed as needed.

During the installation of SUSE LINUX School Server, the YaST partitioning tool will submit a suitable proposal. Normally, this proposal does not require any modification.

If you do not want to partition the hard disk manually or configure an LVM or software RAID system, skip the chapters containing the respective information and continue reading 3 on page 31.

> ## Caution
>
> Normally, the partitioning tool configures *all* installed hard disks for use with SUSE LINUX School Server. Any existing data will be deleted during the installation.
>
> To install SUSE LINUX School Server alongside another system, you have to partition the hard disk manually.
>
> Caution

The YaST Partitioning Tool

If you decide to partition the hard disk manually, you have the possibility to adapt it to your personal needs. For example, you may want to install several versions or operating systems or be able to expand your partition with LVM (by including additional hard disks).

If you want to install SUSE LINUX School Server alongside another operating system on your hard disk for test purposes, configure at least three partitions (`swap`, `/`(root), and `/home`) and do not forget the fstab options `acl,usrquota,defaults` for `/home`.

Manual Partitioning

In the 'Partitioning' module, you can modify the YaST proposal or configure different partitions. In 'Partition according to your own wishes', all hard disks found in the systems are listed. Select the menu item 'Custom partitioning – for experts' in order to partition the hard disks manually.
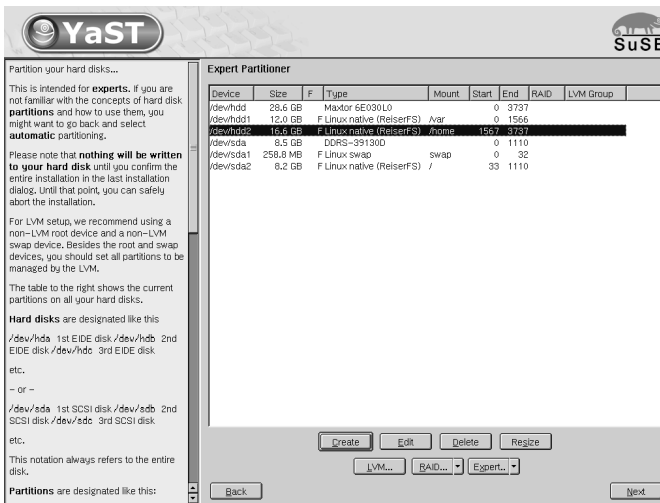
Figure 3.1: The SUSE LINUX School Server Partitioning Tool

YaST lists all existing partitions of the hard disks (see Figure 3.1). Here you can manually create, edit, or delete partitions. Furthermore, you can configure LVM (Logical Volume Manager) or software RAID.

Check if the free hard disk space is adequate for installing SUSE LINUX School Server (at least 20 GB). If necessary, delete or resize some of the existing hard disk partitions.

Partition Types

Every hard disk has a partition table with room for four entries. An entry can represent a primary or an extended partition. Only *one* extended partition is possible.

Primary partitions have a simple structure: they consist of a contiguous range of disk cylinders (physical areas on the disk) that are allocated to an operating system. A maximum of four primary partitions can be set up for each hard disk.

If more than four partitions are needed, an extended partition has to be set up. The extended partition is also a contiguous range of disk cylinders which can be split into *logical partitions* that do not have an entry in the partition table. Thus, the extended partition is a container for logical partitions.

Accordingly, if you need more than four partitions, configure one of the four partitions as an extended partition and assign it the entire free cylinder space.

In this extended partition, you can set up as many logical partitions as you need (up to a maximum of 15 logical partitions for SCSI hard disks and 63 logical partitions for (E)IDE disks).

Primary partitions and logical partitions are equally suitable for the installation of SUSE LINUX School Server.

Normally, SUSE LINUX School Server only needs four partitions, so you can safely use primary partitions. If you need additional partitions, you first have to set up an extended partition. The recommended format is the Reiser file system.

Set up and configure the following partitions with the specified parameters:

swap This partition serves the temporary storage (swapping) of RAM contents. The swap area should be the same size as the RAM (see Figure 3.2).
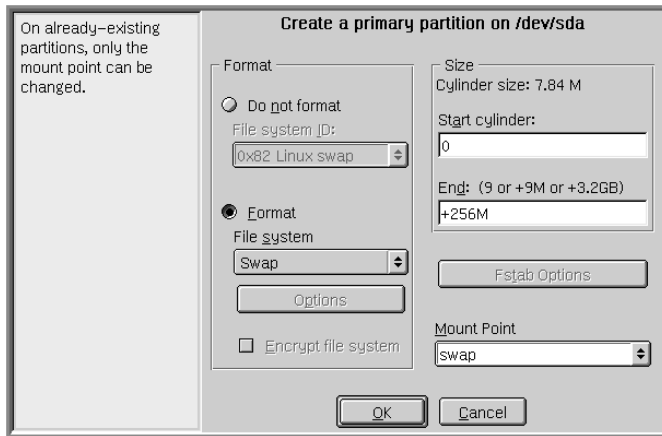
Figure 3.2: Creating the swap *Partition*

/ The root directory of the system. The size of this partition should be about 4-6 GB (see Figure 3.3 on the next page).

/var This directory mainly contains the spool directories of the print system, the e-mail messages of the users, and the user database.

If you want to autoinstall SuSE Linux clients (see 6 on page 125), the installation CDs of the latest SuSE Linux distribution have to be copied to a subdirectory (/var/SuSE/akt) in this partition. Therefore, it makes sense to put this directory in a separate partition.
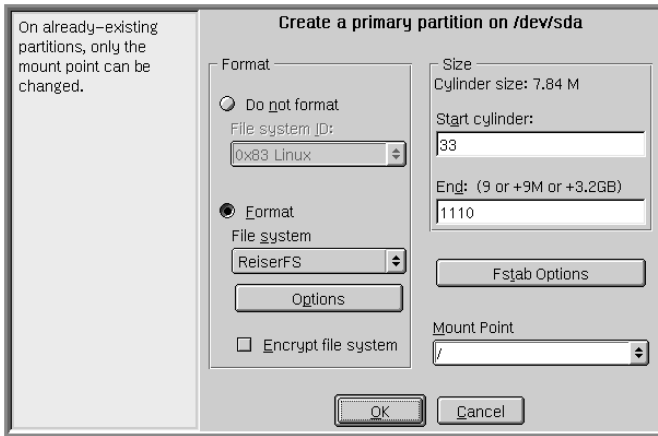
Figure 3.3: *Creating the* / Partition

The size of this partition is primarily determined by the number and size of the mailboxes. For example, if your school has 800 students and 80 teachers and the mailboxes of the teachers are limited to 25 MB and those of the students to 5 MB, add about 4.5 GB for the directory `/var/SuSE/akt` and some extra space for the system log files.

Accordingly, you would need about

```
(800 students * 5 MB) + (80 teachers
 * 25 MB) + 2 GB + 4.5 GB = 12.5 GB
```

to be on the safe side.

Furthermore, enter the following values in 'Arbitrary Option Value' under the menu item 'Fstab options' for this partition: `defaults,data=writeback,noatime`

/home This is where the files of the users are stored. Make this partition as large as possible. For performance reasons, use of a separate hard disk is recommended.

Furthermore, enter the following values in 'Arbitrary Option Value' under the menu item 'Fstab options' for this partition (see Figure 3.5 on page 24): `defaults,acl,usrquota`

The following tables present two example proposals for partitioning the hard disk for SUSE LINUX School Server:
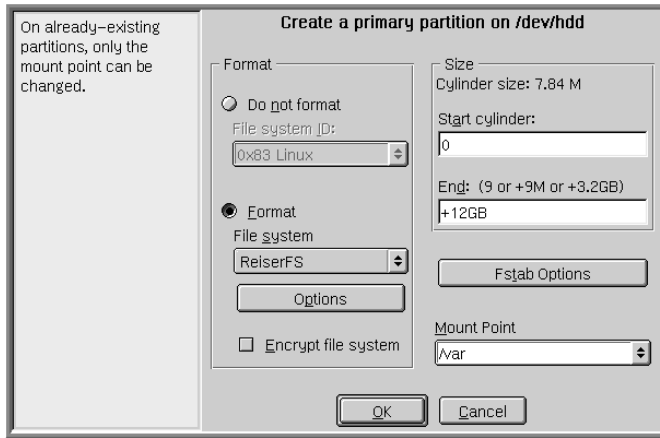
Figure 3.4: Creating the `/var` *Partition*

Partition	Mount point	Size	Form
Example for partitioning an EIDE hard disk			
/dev/hda1		256 MB	swa
/dev/hda2	/	4 GB	Reise
/dev/hda3	/var	5 GB	Reise
/dev/hda4	/home	10 GB (or the rest of the hard disk)	Reise
Example for distributing the system to 2 SCSI hard disks			
/dev/sda1		256 MB	swa
/dev/sda2	/	6 GB	Reise
/dev/sda2	/var	10 GB (or the rest of the hard disk)	Reise
/dev/sdb1	/home	24 GB (or the size of the hard disk)	Reise

Soft RAID

The purpose of RAID (Redundant Array of Inexpensive Disks) is to combine
several hard disk partitions into one large "virtual" hard disk for enhanced per-
formance and data security. However, if this approach is used, one advantage is
sacrificed for another. The "RAID level" defines the attachment and control of
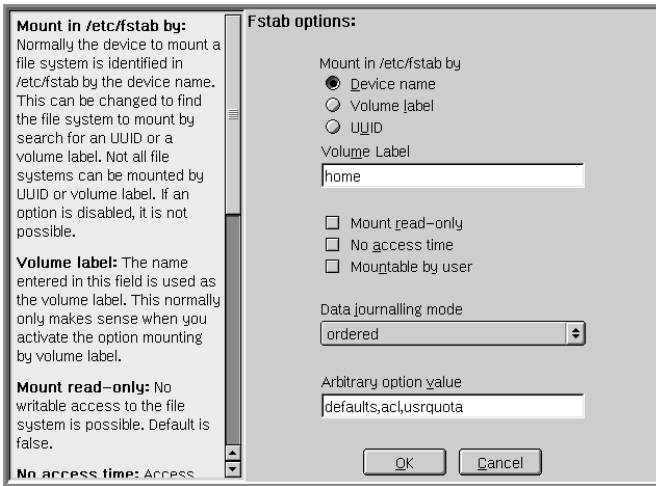
Figure 3.5: Setting the File System Options of the `/home` *Partition*

the hard disks by the RAID controller.

Instead of a RAID controller, which can often be quite expensive, soft RAID is also able to take on these tasks. SUSE LINUX School Server enables the combination of several hard disks in a soft RAID system. Compared to hardware RAID, this approach is much less expensive, but it also consumes some computing resources of the processor.

Common RAID Levels

RAID 0   This level improves the performance of your data access. Actually, this is not really RAID, as it does not provide a data backup. Nevertheless, this kind of system is commonly referred to as "RAID 0". In RAID 0, at least two hard disks are connected. The performance is very good. However, the RAID system will be destroyed and the data lost even if only one of several hard disks fails.

RAID 1   This level provides adequate security for your data, as all data are copied to another hard disk. This is known as "hard disk mirroring". If one disk is destroyed, a copy of its content will be available on another hard disk. Thus, all except for one hard disk can be damaged without losing any data. Due to the copying process, the writing performance in RAID 1 suffers a little (10-20% slower), but the read access is clearly faster

than on normal physical hard disks, as the data are redundant and can be read parallel.

RAID 5 RAID 5 is an optimized compromise between the two said levels in terms of performance and redundancy. The hard disk capacity corresponds to the number of utilized disks minus one. The data is distributed over the hard disks as in RAID 0. Security is ensured by the "parity blocks" that are created on one of the partitions in RAID 5. These are linked to each other with XOR, enabling the reconstruction of the contents by means of the respective parity block via XOR in the event of the failure of a partition. RAID 5 does not tolerate the failure of more than one hard disk fails at the same time. If a hard disk is destroyed, it must be replaced as soon as possible in order to avoid loss of data.

Soft RAID Configuration with YaST

Step 1: Partitioning

The partitions are listed under 'Expert Settings' in the partitioning tool. Any existing soft RAID partitions are also listed. If no soft RAID partitions are listed, set them up from scratch. At least two partitions are needed for RAID 0 and RAID 1. Usually, exactly two partitions are needed for RAID 1. For RAID 5, at least three partitions are needed. It is recommended to only use partitions of the same size.

In order to avoid loss of data due to the failure of a hard disk in RAID 1 and 5 and in order to optimize the performance in RAID 0, the individual RAID partitions should be located on separate hard disks.

Step 2: Setting Up RAID

Click 'RAID' to open a dialog in which you can select the RAID level 0, 1, or 5. In the following dialog, you can assign the partitions to the new RAID. The menu 'Expert Options' allows you to fine-tune the performance by specifying the "chunk size". If you activate the check box 'Persistent superblock', RAID partitions will be recognized as such when the system is booted.

After completing the configuration, the device `/dev/md0` and so on will be marked as "RAID" in the expert dialog.

┌─ **Tip** ─────────────────────────────────

Raid and LVM

Of course, you can also configure an LVM system on a RAID system. For this purpose, LVM even offers special functions by means of striping arrays. However, the combined use of soft RAID and LVM increases the system load and the risk of losing data.

───────────────────────────────── **Tip** ─┘

Logical Volume Manager (LVM)

The Logical Volume Manager (LVM) enables flexible distribution of hard disk space over multiple file systems. LVM was developed to facilitate the rather difficult modification of partitions in a running system. It provides a virtual storage pool (volume group – VG) from which logical volumes (LV) can be created as needed. The operating system will access these LVs instead of the physical partitions.

┌─ **Caution** ─────────────────────────────

The use of LVM is associated with increased risks such as loss of data due to program crashes, power outages, or faulty commands. Therefore, back up your data before you start using LVM or reconfigure volumes.

───────────────────────────────── **Caution** ─┘

Features:

- Several hard disks or partitions can be combined to a large logical partition.

- If the configuration is suitable, an LV (such as `/usr`) can be enlarged when the free space is exhausted.

- Using LVM, you can even add hard disks or LVs in a running system. However, this requires hot-swappable hardware that is capable of such actions.

- Several hard disks can be used with enhanced performance in the RAID 0 (striping) mode.

- The snapshot feature enables consistent backups (especially for servers) in the running system.

The use of LVM makes sense even for small servers. LVM enables use of file systems that are larger than a physical hard disk. Another advantage of LVM is the possibility of creating up to 256 LVs. However, keep in mind that working with LVM is quite different from working with conventional partitions.

┌─ **Caution** ────────────────────────────────────

Root File System

The root file system must be located in a normal partition in YaST. Select a partition from the list and click 'Edit' to configure it as root file system.

──────────────────────────────────── **Caution** ─┘

LVM Elements

Physical volumes   Physical volumes (PV) form the lowest level of a three-layer architecture. These storage media can be hard disks or other block-oriented devices. In this chapter, we mean hard disks when referring to PV.

Volume groups   One or several PVs are combined into volume groups (VG). Apart from a small administrative zone, the size of a VG corresponds to the total storage capacity of all its PVs.

Logical volumes   Logical volumes (LV) form the top layer and are addressed like normal block device files by the operating system. LVs can contain any file system, just like normal partitions.

Like normal partitions, a newly created PV is also assigned a name that appears in a subdirectory of the respective VG in the directory /dev.

LVM Configuration with YaST

Prepare the LVM configuration in YaST by creating an LVM partition during the installation.

┌─ **Tip** ────────────────────────────────────

To avoid overwriting partitions that are already in use while creating VGs, use fdisk to create (or set) one partition to the type "0x8E" which is reserved for LVM.

──────────────────────────────────── **Tip** ─┘

To do this, select 'Create' → ('Hard disk' →) 'Primary partition' → 'Do not format' and set the file system ID to '0x8E Linux LVM'.

Subsequently, continue partitioning with LVM by selecting the LVM partition and clicking 'LVM...'.

LVM – Partitioning

The volume groups are managed in the 'LVM' dialog. If no VGs exist on your system, a pop-up window will prompt you to create one. `system` will be suggested as the name for the first volume group.

Create a Volume Group

Now we have to create a volume group.
Typically you don't have to change anything,
but if you are an expert, feel free to change
our defaults:

Volume Group Name:

system

Physical Extent Size

4M

[OK]   [Cancel]
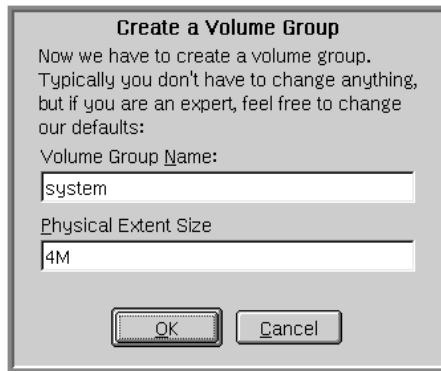
Figure 3.6: YaST: Creating a Volume Group

The physical extent (PE) size determines the maximum size of a physical and logical volume in this VG. Normally, this value is set to 4 MB. This allows for a maximum size of 256 GB for physical and logical volumes. The PE size should only be increased (e.g., to 8, 16, or 32 MB) if you want the logical volumes to be larger than 256 GB.

LVM – Configuring Physical Volumes

The following dialog lists all partitions whose type is "Linux LVM" or "Linux native". Swap and DOS partitions are not listed.
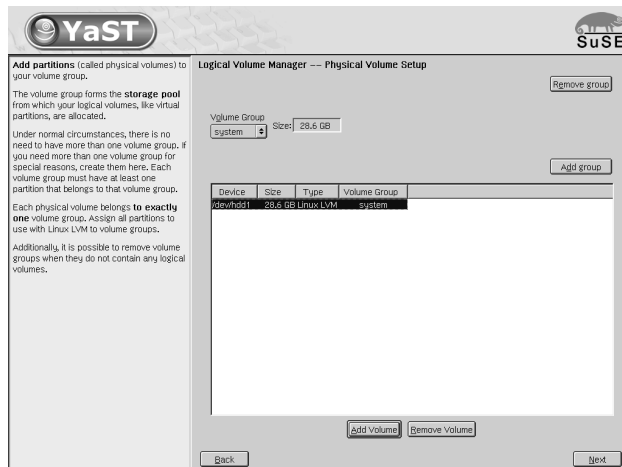
Figure 3.7: YaST: Overview of the Partitions

If a partition is already assigned to a VG, the name of the VG will be displayed in the list. Unassigned partitions are marked as "--".

The VG currently being edited can be modified in the selection box at the top left. Using the buttons at the top right, you can create additional VGs and delete existing VGs. However, only VGs to which no partitions are assigned can be deleted (see Figure 3.7 on the preceding page).

Tip

For a normal installation you do not need to create more than one VG.

Tip

To add a previously unassigned partition to the selected VG, select the partition and activate 'Add Volume' under the selection list. The name of the VG will be entered next to the selected partition. Assign all partitions reserved for LVM to a VG, as otherwise the space on the partition cannot be utilized. Before you exit the dialog, every VG must be assigned at least one PV (i.e., one real hard disk partition). After assigning all partitions to the VG, click 'Next' to access the LV management.

Logical Volumes

Logical volumes are managed in this dialog.
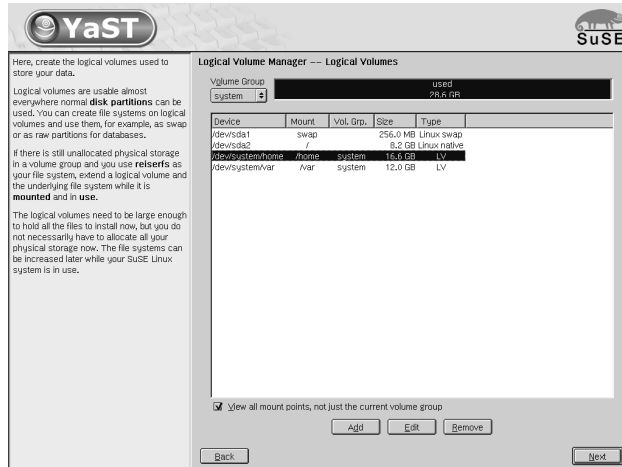
Figure 3.8: YaST: Logical Volume Management

LVs are assigned to a VG and have a specific size. Normally, a file system (such as ReiserFS) is created on an LV and associated with the mount point. In the installed system, the files stored in this LV can be found at this mount point. All normal Linux partitions to which a mount point is assigned, all swap partitions, and all existing LVs are listed here.

If you configure LVM for the first time in a system, no LVs will be displayed in this dialog. Click 'Add' to generate an LV for every mount point and specify the size, the file system type (e.g., ReiserFS), and the mount point (e.g., /var, /home) with the respective fstab options (see Figure 3.5 on page 24).

If you have created several VGs, you can switch between the individual VGs in the selection list at the top left. The created LVs are listed in the VG displayed at the top left. Once you have created all the LVs as required, exit the dialog and proceed with the software selection.

Software

The software of SUSE LINUX School Server is preselected. You cannot make any changes here. To guarantee the system integrity, do not install any addi-
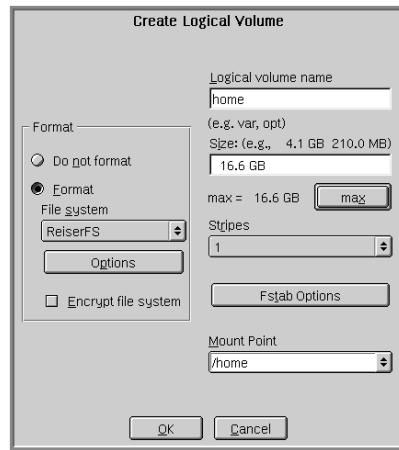
Figure 3.9: YaST: Creating Logical Volumes

tional packages on the server. SuSE Linux AG makes sure your system is always stable. You will be notified whenever you need to install bug fixes or security patches.

Set up an e-mail address for this information and specify it when you register your SUSE LINUX School Server, thus ensuring that you will always receive the latest information.

Booting

Here you can specify custom settings for the boot loader GRUB. For a standard installation, no changes are needed.

Note

The boot mode should only be modified by experienced users, as the system will not boot if the configuration is faulty.

Note

Time Zone

Select your time zone and the setting of the system clock in this dialog.

In 'Hardware clock set to', choose between `local time` and `UTC (GMT)`. Use the same setting as in the BIOS.

If set to to `UTC (GMT)`, SUSE LINUX School Server will automatically switch from standard time to daylight saving time and vice versa.

Language

Here you can select the language for the system. The language you set when you started YaST is preselected.

Starting the Installation

Click 'Next' to accept the installation proposal with all your changes. A green confirmation dialog will be displayed. Click 'Yes' to launch the installation.

Depending on the hardware performance, the installation usually takes about 15 to 30 minutes. During the installation, information on SuSE Linux AG and some of its products will be displayed. Click 'Details' to follow along as the installation proceeds.

Configuring the System

Following the installation of all software packages and the reboot of the server, a number of important settings have to be configured.

Root Password

`root` is the name of the system administrator who can modify the system, install new applications for all users, and configure new hardware components. If a user forgets his password or applications do not work, `root` can provide assistance.

┌─ **Caution** ───

The user `root` has all rights and can perform all kinds of changes in the system. The `root` password is needed for such tasks. Administrative tasks cannot be performed without this password.

───────────────────────────────────── **Caution** ─┘

Normally, the `root` identity should only be used for administrative tasks and maintenance operations. For daily work, this is too dangerous, as `root` could accidentally delete important files.

Enter the password for `root` twice. Use a complex password consisting of the numerals, uppercase letters, lowercase letters, and possibly some special characters (depending on the keyboard layout).

Tip

Never assign passwords that are listed in dictionaries. Personal data and names that people who know you could guess are not suitable either.

Tip

Do not forget the `root` password, as there is no possibility to retrieve the password later on.

As the actual administrator may be absent from time to time or the administrator may forget the password because he does not need to perform any maintenance tasks for a long time, make a note of the most important system data and passwords, using the template in 9 on page 170.

To be prepared for emergencies, keep this note in a closed envelope in a secure place in the school and inform the school administration about the location.

Regularly change the password for `root` and enter the changed password (and the date) on this note. In this way, you can make sure that the "emergency letter" has not been opened and improve the system security.

Screen Configuration

This dialog usually displays suitable settings for the graphics card and monitor. In most cases, you can accept this proposal. If necessary, the color depth, resolution, and refresh rate can be adapted to your specific needs.

Click 'Edit' to access the utility SaX2 for configuring the graphical interface.

If you change the proposal, the settings will be tested before the configuration is saved to the hard disk.

Network Configuration

The configuration of the network for SUSE LINUX School Server is much more complicated than for a workstation.

If you never thought of a concept for the network structure of your school, you should do so now! We recommend that you place all servers in the school (including network printers) in a subnet that is separated from other network areas by means of a suitable subnet mask. In this way, you will later be able to grant clients access to specific server services.

> **Caution**
>
> During the installation, specify the correct interfaces for the internal network and the Internet access. Following the configuration, the built-in firewall will automatically be configured and started in order to protect the server against attacks from the Internet.
>
> **Caution**

Configuring the Internal Network Adapter

Following the configuration of the graphics card, you will be taken to the dialog displayed in Figure 3.10 on the next page. First, select the network adapter connected to your internal school network.

> **Tip**
>
> Linux configures "aliases" with eth for the network adapters. Similar to hard disks, a number following the alias serves the exact definition. Thus, eth0 is the first network adapter in the system, eth1 the second. For SUSE LINUX School Server, additional virtual network adapters are configured on the first network adapter. These are assigned the numbers eth0:0 to eth0:2.
>
> **Tip**

Normally, the driver needed for your network adapter is configured by YaST during the installation. For this reason, manual configuration of the hardware parameters is only necessary if the network hardware is not autodetected. In this case, select 'Add' to select a driver module.

In this dialog, you can set the network adapter type as well as the interrupt and I/O address for ISA cards. For some network drivers, special parameters can be entered to specify the interface to use, such as the RJ-45 or BNC connection on the adapter. In this connection, refer to the documentation of the driver module.

Three preconfigured network models are available for the school network:

- ```10.0.0.0/8```
- ```172.16.0.0/16```
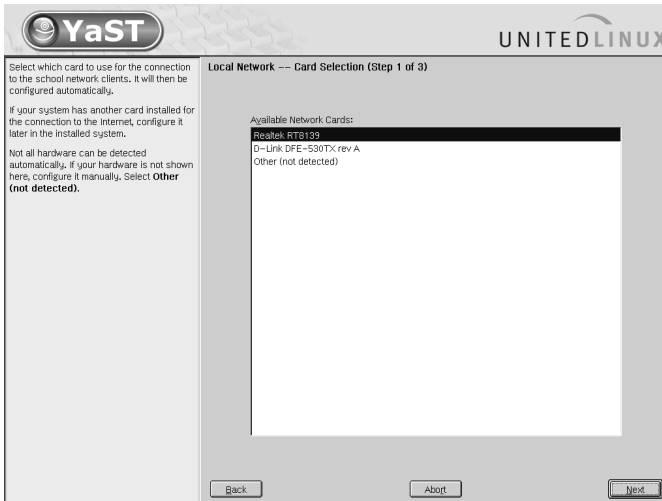
Figure 3.10: *Selecting the Internal Network Adapter*

■ `192.168.0.0/16`

If different address spaces are selected, they have to be entered manually. If you accept the default settings, you merely need to enter the domain name of the school in this dialog.

The preconfigured ranges are IP addresses for local networks. These IP addresses are not used and forwarded on the Internet. In this way, address conflicts with "real" IP addresses of the Internet are avoided.

If you select different address spaces and want to use the Internet, make sure these IP addresses are not used by any other hosts around the globe.

The first address space enables the setup of a very large local network. Theoretically, up to 16 million hosts are possible. If you limit the subnet mask (e.g., to 255.255.0.0), you can network several schools by assigning each school a separate range in this small subnet and enabling the main server to access these subnets by means of a subnet mask comprising all areas.

The other two ranges have frequently been used for SUSE LINUX School Server installations and still enable more than 65,000 hosts[1].

---

[1] For example, the well-known "GEE" and "Arktur" servers in Germany occupy the address spaces 172.16.xxx.yyy and 192.168.xxx.yyy. The address spaces of these two Linux servers have been included in the configuration to enable parallel operation with SUSE LINUX School Server or a migration.
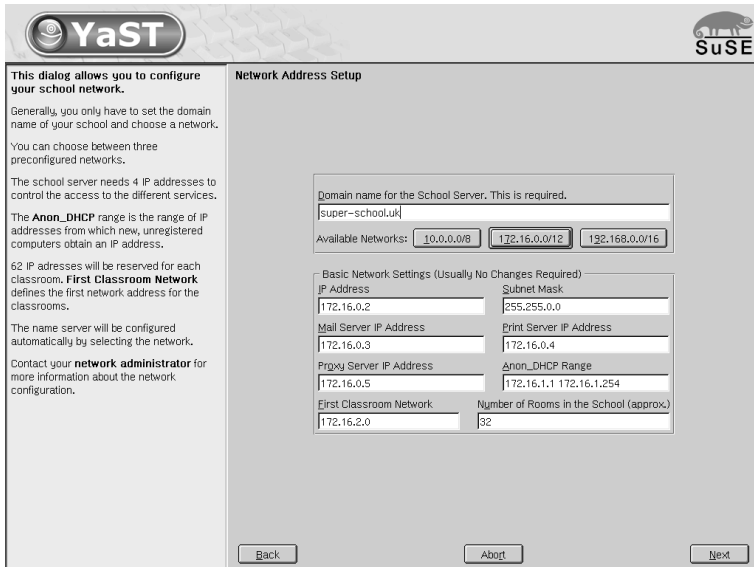
Figure 3.11: *Configuring the Internal Network*

If, for example, you adopt the configuration for the 192xyz network, SUSE
LINUX School Server will be configured as follows:

IP Address For example: `192.168.0.2`;
  DNS names: `admin`, `dns`, `nfs`, `ldap`, `samba`, `install`,
  `PDC-SERVER`, `gateway`, `timeserver`

Subnet Mask For example: `255.255.0.0`

Mail Server IP Address For example: `192.168.0.3`;
  DNS names: `mailserver`, `schoolserver`

Print Server IP Address For example: `192.168.0.4`;
  DNS name: `printserver`

Proxy Server IP Address For example: `192.168.0.5`;
  DNS name: `proxy`

Anon_DHCP-Range "DHCP range for unregistered hosts". New or non-
  registered hosts get their IP addresses from this IP address space.

For example, the standard space could be `192.168.1.1 bis 192.168.1.254`

All hosts of the IP address space for unregistered hosts are entered in the name server with the following name:

`dhpc1 - dhcp254.<domain.name.of.the.school>.`

First Classroom Network Registered hosts of the first classroom get their IP addresses from this IP address space (e.g., `192.168.2.1 to 192.168.2.64`).

Further classrooms are configured accordingly (see Chart 2.1 on page 10).

Number of Rooms in the School (approx.) A DHCP group and an IP address space of 62 IP addresses is reserved for every room. Enter the approximate number of rooms in which there are computers. Additional DHCP groups and IP address spaces can also be reserved later on using the DHCP configuration interface. However, as this requires a deeper understanding, it is better to be generous at this stage.

Configuring the Internet Connection

The next step is the configuration of the Internet connection. Here you can determine how SUSE LINUX School Server is connected to the Internet.

Figure 3.13 on page 40 shows three possibilities for connecting the school network to the Internet.

Default Gateway In this case, the protection of the school network depends on how well the router (firewall) is configured. Make sure the clients can only access the Internet gateway if you explicitly allow this. Furthermore, make sure that the router (firewall) gives the school server unlimited access to the Internet and provides protection against attacks from the Internet.

If you decide for this Internet connection type, you cannot utilize the following SUSE LINUX School Server functions:

- DynDNS configuration (see 4 on page 88).
- External access (see 4 on page 75).
- Allowing and prohibiting direct access to the Internet (see 8 on page 159).
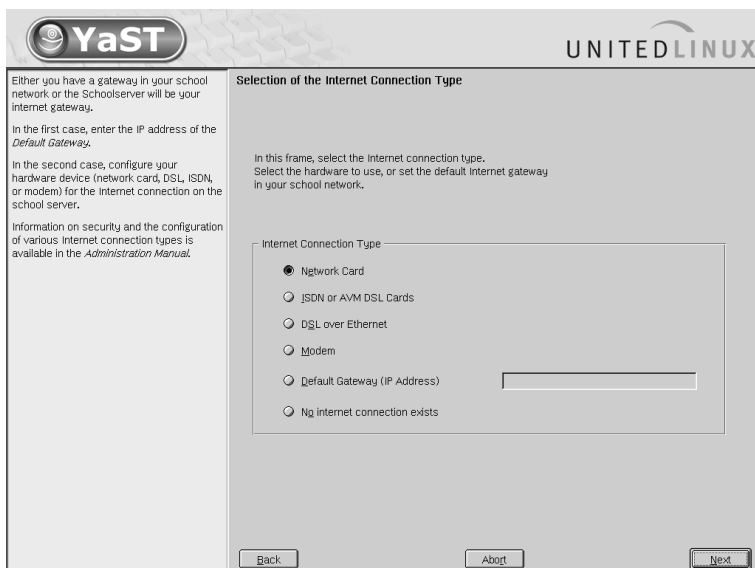
Figure 3.12: Configuring the Internet Connection

Direct Connection with the Internet The school network is protected by the
SuSE firewall script. All control options of SUSE LINUX School Server are
at your disposal.

If you use an ISDN, DSL, or modem connection with dynamic IP ad-
dresses to access the Internet, the danger from the Internet is relatively
low. However, if you use a dedicated line, we strongly discourage the use
of a direct connection to the Internet.

Connection is established over a transport network This is the most secure
method for connecting to the school network to the Internet. All control
options of SUSE LINUX School Server are at your disposal, except for the
DynDNS configuration (see 4 on page 88).

Make sure that the IP address spaces of the transport network and the
school network do not overlap and the router (firewall) gives only the
server unlimited access to the Internet and protects it against attacks.

Internet

| Router firewall | | School server |
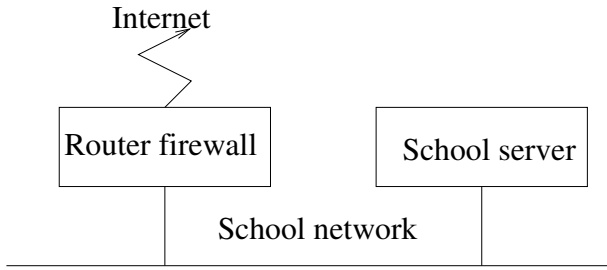
School network

a) Internet gateway is placed in the school network

Internet

Internet

| School server |

Router firewall

School network

Transport network

| School server |
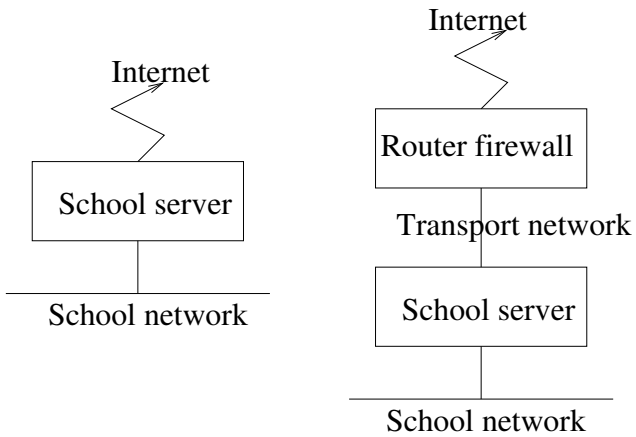
School network

b) School server is
connected directly to
Internet
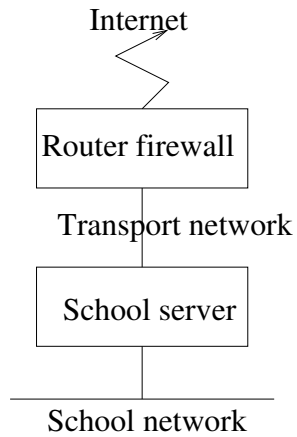
c) School server is
connected to Internet
over transport network

Figure 3.13: *Various Internet Connection Options*

Specify the respective hardware or enter the IP address of the default gateway in your school network (see Figure 3.12 on page 39).

Network Card   If you are connected to the Internet over a dedicated line or a separate firewall (e.g., SuSE Firewall on CD), you should install a separate network adapter for this connection in the server.

If you have a dedicated line, select this network adapter. In the configurations settings for this network adapter, enter the data you received from your provider.

If you have a static IP address, select the respective network adapter from the menu and click 'Configure...'. In the following dialog, select 'Static Address Setup' and enter the respective values.

Set the default gateway under 'Routing'. For advanced settings, click 'Configuration for Experts'.

Do *not* enter the name server specified by your provider in this dialog. Rather, change the respective addresses behind the option `forwarders` in the file `/etc/named.conf` following the installation of SUSE LINUX School Server.

You should also select this method using a separate network adapter if you have a hardware router or a separate firewall.

In this case, connect both devices (SUSE LINUX School Server and the firewall) by means of the network adapters (e.g., using cross-over cables) and configure the DHCP server on the firewall or on the hardware router. Then SUSE LINUX School Server can be configured with a "dynamic address" for this network adapter, and no additional settings are needed.

> **Note**
>
> **DHCP Server**
>
> Make sure that there are no conflicts between the DHCP server of the router and the DHCP server of the SUSE LINUX School Server. Thus, the DHCP server of the router should assign different addresses than the DHCP server of the SUSE LINUX School Server!
>
> **Note**

ISDN or AVM DSL Cards   If you connect to the Internet by means of an ISDN connection or an internal AVM DSL card, select this menu item and follow the instructions on the screen.

Normally, ISDN cards are autodetected. If this does not happen, select the ISDN card in the top frame. Leave the start mode set to 'OnBoot' if you want to enable this network adapter to be selected automatically.

DSL over Ethernet   To be able to use DSL, a separate network adapter has to be installed in the SUSE LINUX School Server.

Currently, SUSE LINUX School Server supports DSL connections using the Point-to-Point-over-Ethernet (PPPoE) protocol. All major providers use this protocol. If you are not sure which protocol your provider uses, contact your provider.

Dial-on-demand means that the connection is established automatically as soon as the user tries to access the Internet (e.g., by entering a URL in a browser or by sending e-mail). If no data are sent or received for a specified time (idle time) the connection is terminated. As the dial-up procedure with the ADSL protocol PPPoE is very speedy, users will get the impression they are connected to the Internet over a dedicated line.

Though a permanent connection would be possible with a DSL flatrate, there are several reasons in favor of temporary connections:

- Most providers disconnect the connection after some time.

- A permanent connection can be viewed as a waste of resources (e.g., the provider has less and less IP addresses available).

- Most importantly, being online permanently represents a substantial security risk, as it enables attackers to check the system for weak spots. A system that only connects to the Internet temporarily and changes its IP address every time is much more difficult to attack.

Dial-on-demand can be activated with YaST or configured manually. To do this, set the parameter DEMAND= in the file `/etc/sysconfig/network/providers/dsl-provider0` to "yes" and define an idle time with the variable IDLETIME="60". In this way, unused connections will be terminated after 60 seconds.

If you activate dial-on-demand, you have to specify a name server. Simply specify the internal IP address `127.0.0.1`, as SUSE LINUX School Server has its own name server which resolves names and prompts the server to establish a dial-up connection to the Internet.

Modem   Here you can configure a modem connected to the serial port. However, the use of a modem as the only Internet access makes little sense for a large school environment.

Default Gateway   If you use your DSL connection together with a hardware router that is directly connected to your network adapter for the internal network by means of a switch or hub, enter the internal address of the router as default gateway.

Hardware routers often have a built-in DHCP server that is incompatible with the DHCP server integrated in the SUSE LINUX School Server. In this case, deactivate the DHCP server of the hardware router.

No internet connection exists   If the server is merely intended for internal use without any Internet services, select this menu item. In this case, the Internet cannot be accessed by way of the SUSE LINUX School Server, and the firewall will not be configured.

Click 'Next' to proceed with the installation. The respective Internet connection will be set up and the firewall of the server will be configured to protect it against external attacks.

> **Caution**
>
> It is possible but not advisable to connect the server directly to the Internet, as external attacks are possible despite the firewall. A separate Internet access by way of a router or firewall is to be preferred.
>
> **Caution**

Basic Configuration

In the next step, the school-specific data (administrator password, name of the school, number of classes) will be queried and the system will be configured accordingly:

In most schools, the classes are called `4A`, `4B`, `4C`, `5A`, `5B`, `5C`, and so on. In order to reduce the typing effort during the installation, the YaST installation dialog features two fields with predefined values:

- 'Classes in the School'

- 'Parallel Classes in the School' for the letters of the class names

A '–' preceding the number indicates that there are no parallel classes.

Both fields can contain all alphanumeric characters of the *English alphabet*. Accented characters are not permitted. The names have to be separated by a blank space. If you have special class names that cannot be derived by permutation, enter "*" in the 'Classes in the School' field and the names of the classes in the 'Parallel Classes' field.
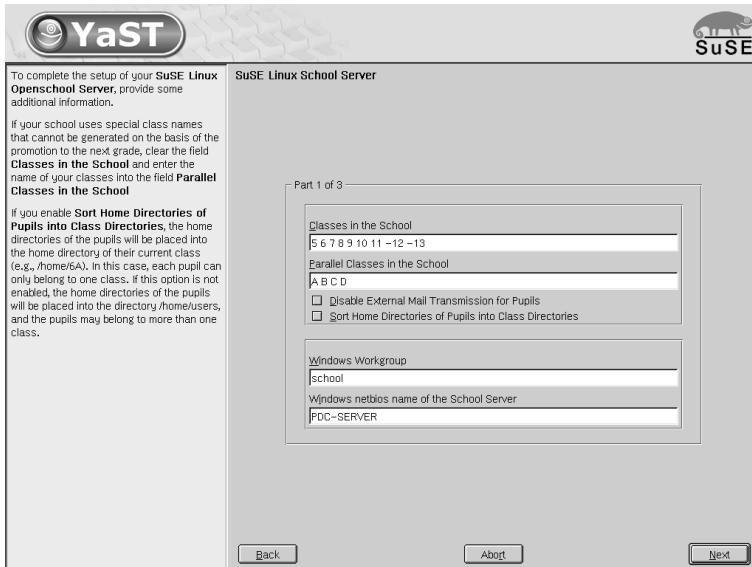
Figure 3.14: School Server Configuration: Configuring Workgroups and Classes

Note

As Linux distinguishes between uppercase and lowercase letters, the class names are converted into uppercase letters in order to avoid problems later on when users are imported.

Note

User groups are created for every class[2]. Furthermore, the classes are assigned a shared mail and file system folder:

`<class.name>@<domain.name.of.the.school>` or
`/home/groups/<class.name>`.

The members of a class can read group messages in the group mail account. This setting can be changed later on. However, the delivery of the group messages of the students to the private mail accounts can generate an enormous mail load. Therefore, the default setting should be kept.

The students only have read access for the class mailboxes, which prevents the danger of accidental deletion by the students. On the other hand, teacher have

---

[2]The gid numbers for the classes are as follows: `gid number > 999`

full access to the class mailboxes. Thus, a teacher can delete the messages of another teacher.

Three main user groups are set up:

`users; gid = 100` Main student group

`teachers; gid = 102` Main teacher group

`administration; gid = 104` Main school administration clerk group

The groups `teachers` and `administration` are assigned a shared mail account and file system folder:

`teachers@<domain.name.of.the.school>` and
`administration@<domain.name.of.the.school>`

`/home/groups/teachers`
`/home/groups/administration`

The teachers and school administration clerks receive all group messages in their private mail accounts. This setting can be changed later on.

The server is also configured as PDC (Primary Domain Controller), file server, and print server for Windows hosts.

The 'Windows workgroup' or domain name is generated from the DNS domain name you entered. If you wish, you can change the domain name. The PDC server is proposed as NETBIOSNAME for the server. This entry can be modified in the field 'Windows netbios name of the School Server' (see Figure 3.14 on the preceding page).

LDAP Settings and Admin Password

In the next step, enter the passwords for the "school admin" who will be responsible for the administration of the server (see Figure 3.15 on the following page).

Do not change the default setting for 'LDAP BaseDN' unless you know exactly what you are doing. The default setting is the domain name you entered during the configuration of the network.

The administrator password does *not* have to be the same as the password for the system administrator `root` which you entered earlier on. This dialog serves the configuration of the administrator who will be responsible for the configuration of the school-specific settings and mail administrator. The administrators
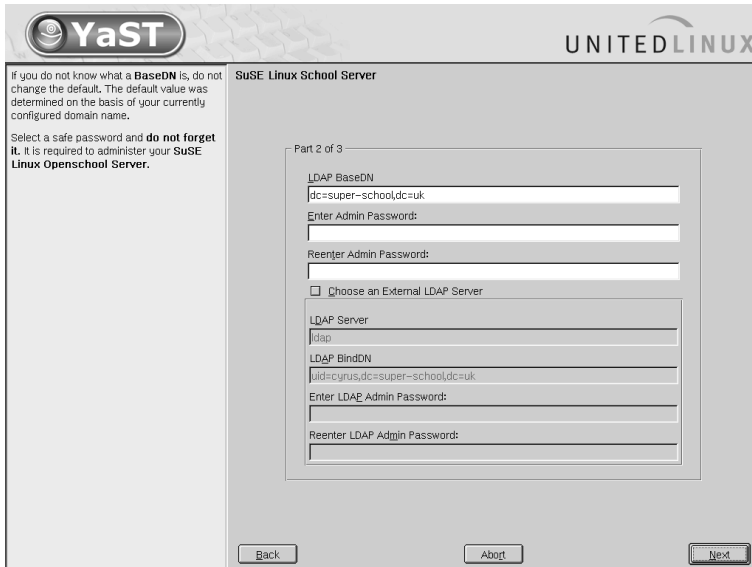
Figure 3.15: *School Server Configuration: LDAP Settings and Admin Password*

are called `admin` and `mailadmin`. The same password is set for both administrators. The Windows administrator (`Administrator`) is also assigned the same password. This password can be changed later on in the web interface.

To use an existing LDAP server, activate the menu button 'Choose an External LDAP Server' and enter the needed data. Do not use this option unless you know the effects on your system. If you decide to use this option, the external LDAP server should be preconfigured to give the main administrator (`admin`) of your newly installed SUSE LINUX School Server write access to the entire LDAP subtree.

School Name and Language Packages

Enter the name of your school and select the language extensions to be installed and your country.

Click 'Finish' to create the basic SUSE LINUX School Server configuration. The selected language extension packages will be installed. Insert the respective CDs when prompted to do so.

Hardware Configuration

In the following screen, you can install any printers connected to the local ports of the server.

Printers connected to external print servers and network printers can only be configured later on with YaST.

After the Installation

When the configuration is completed, SUSE LINUX School Server will boot to the final operating state. The messages displayed on the screen provide information on start-up of the individual server services. When the system is up, you can log in to the system as root.

Caution

Working as root

Do not forget that working as root is always dangerous!

Incorrect commands can cause major damage in the system. Therefore, caution is needed when performing administrative tasks.

Caution

Testing the Installed System

After you log in to the server, the graphical user interface will be started. To make sure everything works properly, perform a number of tests before you start utilizing the server officially.

Links on the Interface

To facilitate the administration, links to the respective web interfaces are created on the desktop of root during the installation.

First, click the 'Web-Mail, Groupware, Forum' link and try to log in as mailadmin. You should receive an alert indicating that the authentication of the server certificate failed. As this certificate was generated for your school just now, the message is correct, and you can continue and accept the certificate permanently.

Then click the "Administration" link in order to log in to the administration interface as admin. Here too, an alert will be displayed.

Service Monitoring

In the web interface of the admin under the menu item 'Monitor' → 'Service Monitoring', check if all needed services have the status "running". If not, enter the respective entry for the service to "active" and reboot the server.

If the respective service is still not reported as "active", there is an error.

Note

Netatalk

The `Netatalk` service is only needed if you have Mac hosts. Normally, this service is and should remain deactivated.

Note

Proxy

To test the functionality of the proxy server and the built-in content filter, you have to configure the proxy correctly in your browser. Otherwise, the proxy would be circumvented, as you are working directly on the server.

In the Konqueror menu bar, go to 'Settings' → 'Configure Konqueror' and click 'Proxy' to the left. Activate the fields 'Use proxy' and 'Specified script file' and enter the following path:

```
/srv/www/htdocs/proxy.pac
```

(Of course you can also look for the file `proxy.pac` in the directory `/srv/www/htdocs/`.)

Subsequently, enter `http://www.sex.de/`. Even if there is no connection to the Internet, you will be prompted to enter a user name and password. If you log in as `mailadmin`, you will be taken to the locked page.

Configuring the Archiving Application Sesam2000

SEP AG `http://www.sep.de` provides a free version of Sesam2000 for SUSE LINUX School Server. Using this application, you can archive SUSE LINUX School Server to a single-tape drive or a (separate) hard disk.

Note

Though the company makes the product available to schools free of charge, it has to be registered at the company's web site if you want to use it at your school.

Note

The program package is installed during the installation. You merely need to execute a configuration script. To do this, log in to the system as `root`, start a console, and execute the command `/opt/sesam/bin/sesam_serv_setup`. The execution of all configuration stages will take some time. Do not interrupt the execution.

More information on using this product is available in the online documentation or at the URL `http://www.sep.de`.

The Administration Interface

The Start Page in the Browser

Following the successful installation, SUSE LINUX School Server is at your command with all its functions. Open a browser on one of your client hosts and enter the URL:

```
https://admin.<school.com>
```

The following start page should be displayed (see Figure 4.1 on the next page).

> **Caution**
>
> As the certificate of the server is generated for your school during the installation, the browser will not recognize it and issue an alert.
>
> **Caution**

The System Administrator `admin`

To administer the server as the school administrator, log in to the configuration menu with the user name admin and your administrator password. In this menu, you can modify almost all configuration parameters of the server.

The navigation in the configuration menu is easy and efficient. The menu features a tab bar as the main menu and a second bar as a sub menu (see Figure 4.2 on page 53).

Click an icon in the main bar to display the respective subbar. The icon in the main bar will be highlighted. Click a submenu to access the respective dialog. To change the language, click the 'Language' icon.

Figure 4.1: Start Page of SUSE LINUX School Server

Click the question mark at the top right edge of the respective submenu dialog to get help for the displayed input options in a separate window.

To close your session, click 'Logout'. If you log out, you must enter your name and password anew before you can perform any further changes.

> **Note**
>
> **Web frontend and YaST2**
>
> Remember: The basic configuration is handled by way of the web front-end using a browser.
>
> For some server settings, you need the graphical configuration tool YaST.
>
> However, do *not* use YaST for adding new users!
>
> **Note**

User Management

After installing SUSE LINUX School Server, create the users. The user `admin` (responsible for the configuration of the server) and the user (reads the e-mail messages to the administrator) already exist.

Figure 4.2: Administration of SUSE LINUX School Server by the User `admin`

Users can be created by means of two menu items:

'New' Creation of an individual user.

'Import' Import of users from a text file. See 4 on page 56 for details.

Creating Individual Users

To create the first users, select 'User' in the main menu and 'New' in the sub-menu (see Figure 4.3 on the following page).

Fill in or set the following fields for the creation of a new user:

- Last Name

- First Name

- Primary Group: Student, Teacher, or Administration

- Class. If the newly created user is a student, he has to be associated exclusively with one class. A teacher can be associated with multiple classes or no class at all. Click `all` at the end of the selection in order to associate a teacher with all classes.

- Birthday

If no user ID (UID) is specified, it will be generated from the first name and the last name. The way how this is done is controlled by the system variable SCHOOL_LOGIN_SCHEME in the file /etc/sysconfig/schoolserver. The default value is N4V4.

This means that the login is generated from the first four letters of the last name and the first four letters of the first name. If a user with the same UID already exists in the system, a number will be appended in order to make the UID unique. If you wish, you can specify the UID for the new user yourself. In this case, enter a unique UID consisting of lowercase letters only. Do not use any special characters or blank spaces.
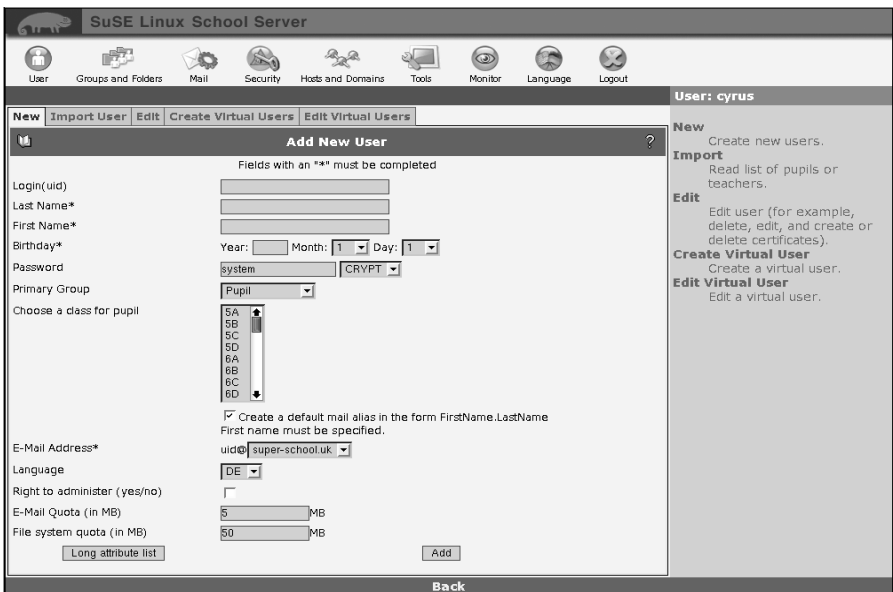
Figure 4.3: Creating a New User

If you want your users to have an intelligible name for their e-mail address on the Internet, simply use the e-mail alias (by default: firstname.lastname@ domain.com) as the address. Additional aliases can later be added by means of the menu item 'Edit'.

The administrator must assign a password to the new user. This does not need to be a secure word, as the user should change it anyway after the first login.

Select a primary group for the new user. Additional groups can later be assigned using the the 'Groups/Folders' menu. If you have not yet created any groups, you can only select the groups `Student`, `Teacher`, and `Administration`.

To assign teachers special rights on the user data, activate the check button 'Right to administer (yes/no)'. This right cannot be assigned to students.

Check the values entered for 'E-Mail Quota (in MB)' and 'File system quota (in MB)'.

These values specify the maximum space assigned to a user for storing e-mail in his folders or files on the server. If the space specified under 'E-Mail Quota (in MB)' is full, no new e-mail can be received until some of the old messages have been deleted. This value can also be changed later.

If the space specified under `File system quota (in MB)` is full, no files can be saved on the server until some of the existing files have been deleted. The calculation of the used hard disk space includes the files in the home directory as well as all other files that the user saves on the system (`/home/all`, `/home/groups/<other_directories>,...`). The default values (`E-Mail Quota (in MB)`,`File system quota (in MB)`) displayed when creating a user can be modified by setting the following variables in the file `/etc/sysconfig/schoolserver`:

`SCHOOL_MAIL_QUOTA` Default value for `E-Mail Quota (in MB)` for newly created students. Default setting: 5 MB.

`SCHOOL_MAIL_TEACHER_QUOTA` Default value for `E-Mail Quota (in MB)` for newly created teachers. Default setting: 25 MB.

`SCHOOL_FILE_QUOTA` Default value for `File system quota (in MB)` for newly created students. Default setting: 50 MB

`SCHOOL_FILE_TEACHER_QUOTA` Default value for `File system quota (in MB)` for new teachers. Default setting: 250 MB

To enter additional personal data such as the address and phone numbers for the user, click 'Long Attribute List' to view and edit all possible attributes.

Now inform the new user of the user name and password. The first thing new users should do when logging in to the web front-end of the server is change their passwords. The administrator does not need to know the user password, as he is able to assign a new password even without knowing the old password.

As stated above, a separate home directory is created for every new user. Teachers have their home directories under `/home/teachers/`, and students have theirs under `/home/<class>` or `/home/users`, depending on what you selected during the installation.

The following directories are created in every new home directory:

Import: Directory for incoming files.

Export: Directory for outgoing files.

public_html: Directory for publishing files. By default, this directory can also be accessed with a web browser under the URL `https://SchoolServer/~<login>`.

Additionally, every user is assigned a directory for his Windows profiles in `/home/profile`.

Importing Users

To avoid having to enter the students and teachers manually every year, you can import the list of students and teachers from a file of the following format:

- Format: Normal ASCII text file. You can use any separator between the individual fields, as long as you use the same separator for the entire file. Usually, all you need to do is export the data from the school administration software to a CVS or text file.

    Brief instructions for a number of school administration applications are available in the annex of the online manual at `http://admin/manual/manualEN.pdf`.

- The columns and the separator are defined in the first line. Currently, the following keywords can be used:

    SURNAME *

    GIVENNAME *

BIRTHDAY*

CLASS *

PASSWORD

LOGIN

PHONENUMBER

FAX

HOMEPHONE

MOBILE

LANGUAGE

DESCRIPTION

STREET

POSTALCODE

STATE

DOMAIN

- The fields marked with '*' are mandatory.

- The user is identified by the LAST NAME, FIRST NAME, and BIRTHDAY fields.

- There are three options for an entry in the user file:

  New User   The user cannot be found in the LDAP database. In this case, a new unique login (see 4 on page 53) will be generated and entered in the LDAP database.
  If the PASSWORD field exists, it will be interpreted as follows:

  'text' =>   'text' will be set as the password.

  '*' =>   If you want to assign some of the users in the text file a fixed password with 'text', but generate a random password for other users, enter '*' for these users.

  'no content' =>   If other users are assigned a password with one of the two said possibilities, but the password field of one (or several) user(s) in the same file is empty, these users will not be assigned a password. Thus, they can log in to the system without a password.

  If the PASSWORD field does not exist in the file, a random password will be generated.

Delete User This function only works if you do *not* import a partial list. If a user is listed in the LDAP database but not in the user list, this means that the user has departed from the school.

The user's data are deleted from the database and the home directory is compressed and saved to the directory `/home/archiv`. As the archiving process consumes a lot of computing power, it is not started immediately, but at 2 a.m. on the next day. However, you can also start the archiving process manually. To do this, log in to the server as `root` and execute the command `/usr/sbin/archiv_ user` on a console.

Note

When preparing a list of teachers, remember that users associated with the primary group `Teachers` are *always* treated as if a partial list were imported. Therefore, you have to manually delete teachers who depart.

Note

Changing old users If a user is listed both in the LDAP database and in the user list, it is an old user.

For old users, the PASSWORD field is not interpreted. The users are merely deleted from the old class and added to the new class, and their home directories are relocated. If the old class and the new class are identical, the data are not changed.

- After the imported file has been processed, the new user list is saved in the file `/root/<date>.<time>.userlist.<CLASS>.txt` in the home directory of the user `root`. As this file contains the password in clear text, it has to be handled securely and with the needed discretion.

Example file for the initial loading of the system with diverse password specifications:

```
BIRTHDAY:SURNAME:GIVENNAME:PASSWORD:CLASS
10-10-1986:Klein:Aladar:system:9A
04-08-1986:Micuc:Emil::9A
11-09-1986:Groß:Evelyn:*:9A
17-04-1986:Müller:Helmuth:*:10A
29-09-1987:Klein:Aladar:*:10A
```

The resulting files `/root/<date>.<time>.userlist.9A.txt` and `/root/ <date>.<time>.userlist.10A.txt` would look as follows:

```
LOGIN:BIRTHDAY:SURNAME:GIVENNAME:PASSWORD:CLASS
```

```
aladklei:11-10-1986:Klein:Aladar:12345:9A
emilmicu:04-08-1986:Micuc:Emil::9A
evelgros:09-11-1986:Groß:Evelyn:*:9A

LOGIN:BIRTHDAY:SURNAME:GIVENNAME:PASSWORD:CLASS
helmmuel:17-04-1986:Müller:Helmuth:*:10A
aladklei1:29-09-987:Klein:Aladar:*:10A
```

Aladar Klein is assigned a specific password (12345). An empty password is
generated for Emil Micuc (thus, he can log in without a password). Random
passwords are generated for all other users in this list, as the respective field
contains an '*'.

Accordingly, if you want to assign random passwords to all users, the file
should not contain a password field (or you have to set an '*' in this field for
every person).

An example file without a password field would look as follows:

```
BIRTHDAY:SURNAME:GIVENNAME:CLASS
11-10-1986:Klein:Aladar:9A
04-08-1986:Micuc:Emil:9A
09-11-1986:Groß:Evelyn:9A
17-04-1986:Müller:Helmuth:10A
29-09-1987:Klein:Aladar:10A
```

Editing User Data

First, click 'Edit'. Select the users to be displayed. If you have a limited num-
ber of users and want to list all users, click 'Apply Filter' without changing the
value '*' in the input field 'Filter'. Select the user to edit with a mouse click.

You can search for users according to the following criteria:

UID or last name or first name   Enter the search string or part of it with the
wild card '*' in the input field 'Filter'. Other wild cards like e. g. '?' do
not work here.

Class or group   Enter the designation of the class or group whose members
you are looking for in the field 'Class'. Here too you can use the wild card
'*'. For instance, all fifth-grade students and teachers can be listed with
the search string '5*'.

The functions

- 'Delete',

- 'Allow/Disable External eMail', and

- 'Edit Access Rights'

can also be executed simultaneously for multiple users. To do this, keep the $\boxed{\text{Ctrl}}$ or $\boxed{\text{Shift}}$ key pressed while selecting several users with the mouse.

The names of the selected users will be highlighted. The button for the individual functions are located to the right (see Figure 4.4).
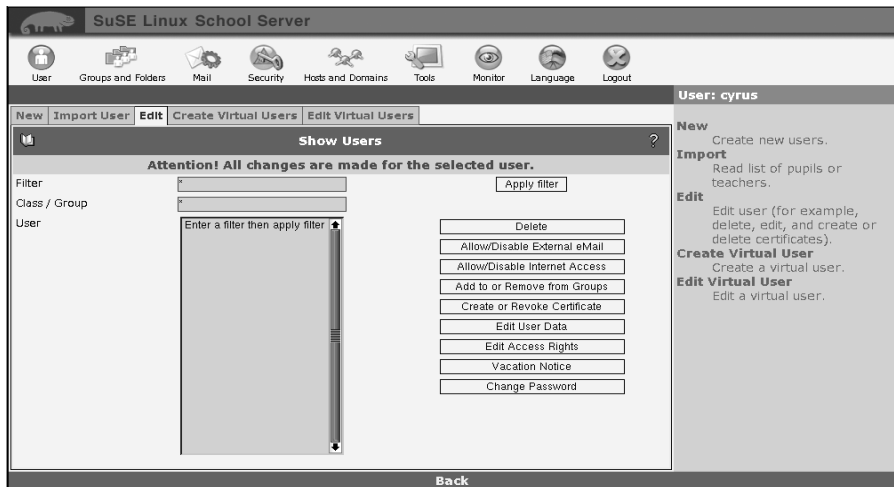
Figure 4.4: Editing User Data

'Delete' Completely removes the selected user from the server. Use this function with caution, as it will permanently delete all e-mail messages and data of the respective user.

'Allow/Disable External eMail' Depending on how you installed SUSE LINUX School Server (keyword: 'Disable external mail transmission for students'), students are allowed or not allowed to send external mail. However, this rule is not associated with the group of the students. Rather, the LDAP attribute mailEnabled is set to OK or locale_only

when the individual users are created. By means of this menu item, you can allow or forbid individual users to send external mail.

To change the default setting, use an editor of your choice to edit the variable SCHOOL_NO_EXTERN_MAIL in the file /etc/sysconfig/ schoolserver. However, the changed setting will only be applied to users created after the modification.

'Allow/Disable Internet Access'   Here you can grant or deny individual users access to the Internet (the LDAP attribute internetDisabled is set to true or false). However, this will only affect Internet surfing; it will not affect other services such as e-mail.

'Create or Revoke Certificate'   Using this item, generate a certificate for this user. This will only work if you created a "CA" (Certification Authority). The generation of a CA is similar to the generation of the server certificate (see 4 on page 75). First, enter the password for the CA. Then enter the password for the new client certificate twice. Confirm the entries with 'Sign'.

'Add to or Remove from Groups'   You can assign users to one or several (secondary) groups. Mark one or more of the available groups with the mouse (keeping the (Shift) or (Ctrl) key pressed) and confirm the changes.

'Edit User Data'   This dialog resembles the one used for creating users. All values can be changed. In addition to their UIDs, users can be assigned aliases. In 'E-Mail Aliases', enter a list of all additional names (separated by blanks) that can be used to reach the user by e-mail.

'Edit Access Rights'   In this dialog, the write access a user has to his personal data can be limited. A list of all available fields is displayed. Select the fields the user is allowed to edit.

'Vacation Notice'   Here you can configure the automatic vacation notification for users (see 8 on page 158).

'Change Password'   In this dialog, you can assign a new password (e.g., if the user forgets his password).

Creating Virtual Users

After you have created at least one virtual domain, click 'New' to create virtual users (see Figure 4.5 on the next page). Click 'Apply Filter' to view a list of all users in the system or limit the search with the input field 'Filter'.

Figure 4.5: Creating a Virtual User

Enter a virtual e-mail address and select one of the virtual domains. Select one or several users and click 'Create'. With immediate effect, the users will receive all e-mail sent to the virtual address.

Editing Virtual Users

To change the address of a virtual user, click 'Edit' and select the address to edit. Assign this address to an address of another (real) recipient or delete it.

Groups and Folders

To facilitate the assignment of access permissions for folders or to create a mailing list, you can assign your users to groups. You can also create shared folders for multiple users or groups. Additionally, the 'Direct Mail Delivery' feature enables the distribution of e-mail to users who use POP instead of IMAP and therefore do not have access to shared folders.

This functionality can also be used to prepare a mailing list.

Creating Groups

To create a new group, go to 'Groups' → 'Create Groups' (see Figure 4.6 on the facing page). Designate a unique name for the group.

┌─ **Caution** ─────────────────────────────────────

Group Names

For group names, use lowercase letters only; do not use special characters
or blank spaces.

─────────────────────────────────────── **Caution** ─┘

Figure 4.6: Creating a Group

Enter a suitable description for the group or use one of the following preconfig-
ured options:

Class   All students of a class should be included here. Using this option, you
can easily create a shared folder and/or a mailing list for an entire class.

User Group   This option distinguishes various groups. By default, the user
groups "Schüler", "teachers", and "administration" are created during
the installation of SUSE LINUX School Server.

Workgroup   This group type can be created and/or edited by teachers who
have the respective administrator permissions.

All these groups are assigned a mailbox and a group directory and are listed in
the groupware (e.g., for arranging appointments or sending e-mail).

To allocate users to the group you want to create, view the list of existing users. Click 'Apply Filter' without changing the value in the field 'Filter' in order to list all existing users, or limit the users to be listed by means of the input field 'Filter'.

Use the mouse to select one or several users to be associated with the group. Selected users will be highlighted. Click 'Add' to create the group with the selected members.

Editing Groups

Existing groups can be edited or deleted and the description of the group can be modified. Select a group and click 'Edit' in order to view or edit the list of members (see Figure 4.7).
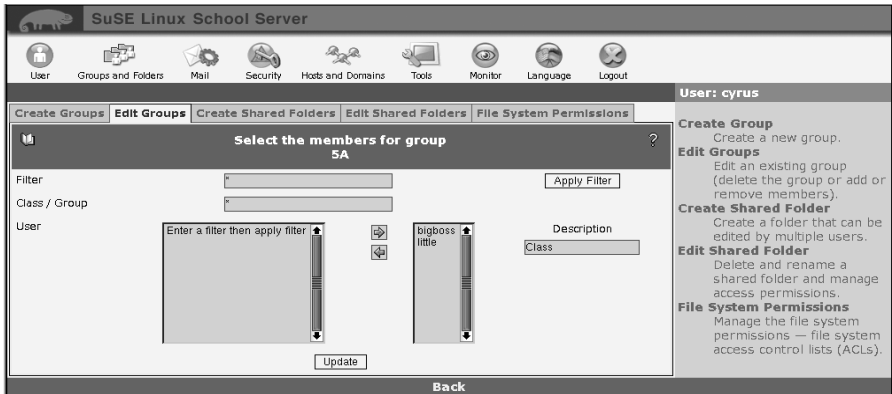

Figure 4.7: Editing a Group

Click 'Apply Filter' to list all existing users in the system. Users that are already affiliated with this group are highlighted. Use the mouse to change the affiliation according to your needs. Click 'Update' to finish the editing and save the changes.

Creating Folders

To create a new folder, select 'Create Shared Folders' and enter a folder name.

> **Caution**
>
> **Folder Names**
>
> For folder names names, use lowercase letters only; do not use special characters or blank spaces.
>
> **Caution**

Enter a suitable description for the folder. If the folder is to be assigned an e-mail address, leave the respective option activated.

Click 'Add'. In the following dialog, you will be prompted to specify the permissions for this folder.

Folder Permissions

Previously set permissions are displayed in the upper part of the dialog. As a general rule, the owner has all permissions for this folder. Do not change these settings. To assign permissions to third parties, view the list of existing users by clicking 'Apply Filter' or limit the users to be listed with the input field 'Filter'. Then select a user.

> **Tip**
>
> **Using Groups**
>
> Permissions can also be set for an entire group. If possible, organize your users in groups and set permissions for the groups. This reduces the administration workload for any changes.
>
> **Tip**

Finish your selection by clicking 'Save'. The set permissions will be added in the upper part of the dialog. Continue setting further permissions or exit the dialog.

The following permissions are available:

(l)ookup   The folder is visible and can be listed.

(r)ead   The folder and e-mail stored in this folder can be read.

(s)tore   The status new and read is retained over several sessions.

(w)rite   Changing of message flags (new, replied, draft) is permitted.

(i)nsert   Inserting of messages is permitted.

(p)ost   Messages can be sent to the recipient address of this folder.

(c)reate   Deleting of subfolders of this folder is possible.

(d)elete   Deleting of messages is possible.

(a)dminister   The folder can be administered (setting permissions).

The following combinations have proved to be practical:

Read (lrs)   Folders can be listed and contents read.

Add (lrsip)   Additionally, new messages can be added.

Write (lrswipcd)   Additionally, subfolders or the folder itself can be created or deleted.

Administer (lrswipcda)   Comprises all permissions including the assignment of access permissions to other users or groups.

Editing Folders and Permissions

Here you can change the attributes of existing folders. Use the mouse to select a folder. The folder will be highlighted. Click 'Edit' to change the description or the folder option "Folder e-mail address?". Select 'Set Permissions' in order to change the permissions. To delete the selected folder and all e-mail messages it contains, click 'Delete'.

Direct Mail Delivery — Mailing Lists via Folders

"Direct mail delivery" is a special feature of folders. Select 'Direct mail delivery for users' to deliver e-mail messages sent to this folder to the inbox of the respective user.

> **Tip**
>
> **Direct Mail Delivery**
>
> This is necessary if the user accesses the server via POP3 (i.e., with an external e-mail program), as POP3 does not support the use of folders.
>
> **Tip**

List all users in the system with 'Apply Filter' or limit the users to be listed with the input field 'Filter'.

Previously selected users are highlighted. Click the names to change the affiliation and complete the input with 'Änderungen speichern'. Click 'Zurücksetzen' to restore the original list status. To select another folder for editing, click 'Zurück zur Ordnerauswahl'.

'Direct mail delivery for groups' works in the same way. All members of the group receive a copy of incoming e-mail messages. With this function, you can easily create a mailing list by placing all list members in a special group and setting up a folder with mail delivery for this group.

File Permissions

Permissions for the folders or files of a user can be set in the same way as for shared mail folders. Click 'Set Permissions' to access the dialog you already used for creating folders.

As the owner of the folder, you have virtually all permissions for the respective folder. Do not change this setting. A detailed description of setting permissions is provided in *Folder Permissions* on page 65. The only difference is that by default, the user who creates a folder has all permissions for the folder, not the school admin. Newly created subfolders inherit the permissions of the parent folder.

Mail

The entire mail system can be configured under 'MAIL'. Important data for the operation of the server can be modified here. Do not change anything unless you are sure about the result of your actions.

Postfix: Basic Configuration

Using the Postfix interface, you can configure the following functions (see Figure 4.8 on the next page):

Name of Relay Host Enter the mail relay supplied by your provider. This is usually necessary if the server is not connected to the Internet over a dedicated line.

Dial on Demand If you use a dial-up line (such as ISDN), specify whether the server is permitted to initiate a dial-up automatically when needed.

SMTP_AUTH   Activate this field if users should be permitted to log in with "authenticated SMTP".

TLS   This option is only visible if you created a "CA". Activate this option to use encrypted e-mail transmission and certificate-based relaying.

SPAM Filter   Activate this option to screen mail arriving via SMTP for SPAM. Mail identified as SPAM is tagged, which means that some information is added to the e-mail headers. Nothing else is done at this stage. Subsequently, every user can decide what to do with e-mail marked as SPAM.

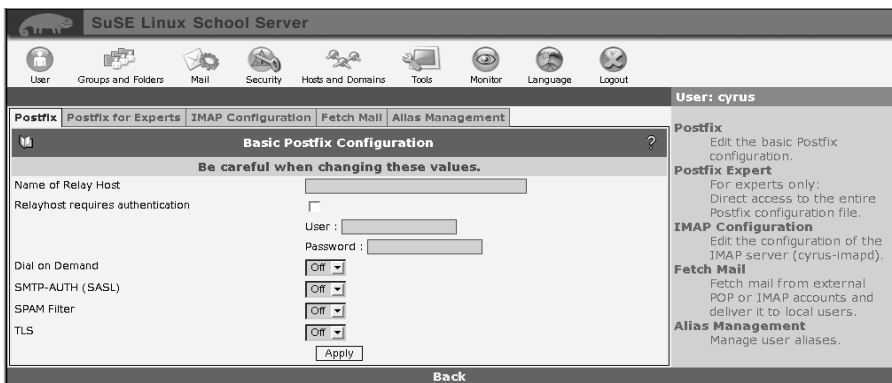*Figure 4.8: Postfix: Basic Configuration*

Postfix: Advanced Configuration

Allmost all Postfix parameters can be edited, removed, or added in this dialog (see Figure 4.9 on the facing page).

> **Caution** ─────────────
>
> Unsuitable changes in this dialog can render your server inoperable. Do not change anything unless you have detailed knowledge of the configuration of Postfix.
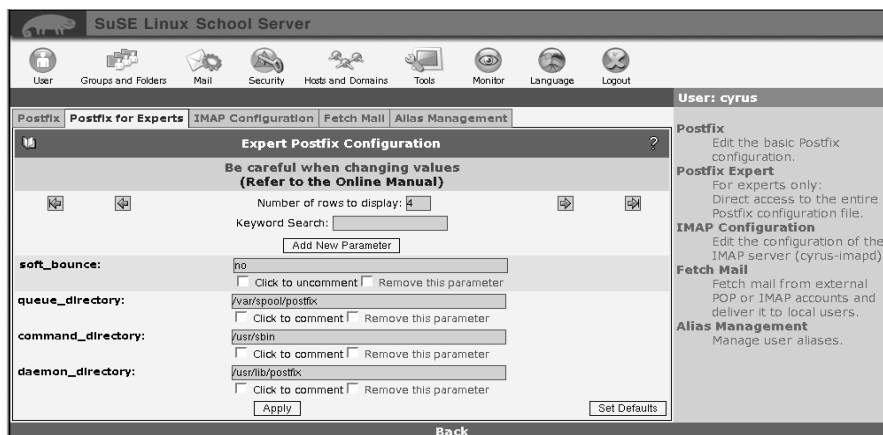>
> ─────────── **Caution** ─

Figure 4.9: Postfix: Advanced Configuration

IMAP Configuration

Here you can specify basic settings that determine how the server handles clients. Under 'Set Default Quota Size', set the quota value suggested when creating new users. With 'After the expiration of this time, idle IMAP users will automatically be logged out', specify the idle time after which a user is logged out automatically. For example, users who forget to log out before leaving will be logged out automatically. The value for 'After the expiration of this time, idle POP3 users will be logged out automatically' specifies the idle time after which POP3 users are logged out automatically. Thus, open connections to the server are closed. Usually, POP3 clients send their authentication data to the server every time they fetch e-mail.

Furthermore, you can specify the procedure for e-mail addressed to users whose quota limit is reached. By default, incoming mail is accepted. If the `postfix` parameter `maximal_queue_lifetime` is not changed, the server will repeatedly try to deliver the e-mail for a period of five days. Then the e-mail will be discarded and the sender will be notified by e-mail If the switch 'Mail will be rejected immediately when the quota limit is exceeded' is set to "yes", the e-mail will be discarded immediately and the sender will be notified.

You can also specify a local user for undeliverable e-mail. Normally, e-mail to nonexistent local users is rejected and the sender is notified by e-mail. If you enter an existing local user in this field, e-mail addressed to nonexistent addresses will be delivered to this user. In this case, the sender will not receive any notification.

If the parameter `drop_undeliverable_mail` in the menu 'Tools' → 'Edit Global Configuration' is set to `true`, undeliverable e-mail will be discarded without any further action.

> **Note**
>
> You can only enter local users like `mailadmin`. Do not enter the e-mail domain.
>
> **Note**

Fetching Mail

If you use a static, official IP address for your server and your mail server is "responsible" for your domain (meaning that an "mx record" exists on an official name server), you do not need this functionality.

'Fetch Mail' can be used to fetch e-mail from a provider and deliver it to a local user. Select 'New' to add an entry or 'Edit' to edit an existing entry (see Figure 4.10).

Figure 4.10: *Fetching Mail*

Enter the required data for the login on the remote mail server. Under 'Delivery Address', enter the complete e-mail address of one of your local users. This user will receive all e-mail fetched from this account.

Under "Protocol", you can select POP3 or IMAP. Providers usually offer POP3. Ask your provider whether IMAP is supported. If your account is a ☞*multidrop* account (e-mail messages to multiple users with the same domain are stored

in one account), activate the respective option. In this case, you do not need to specify a delivery address, as the delivery will automatically be handled by the server.

This is where the "QMail prefix" comes into play. If your provider uses QMail on his system, the delivery addresses have a special format. For example, someone may send an e-mail to `user@school.com` in your school. The provider's QMail server will write something like "Delivered-To: multidrop-user@school.com" in the mail header. In this example, the QMail prefix is "multidrop-". The prefix depends on the settings your provider configured on his system. If necessary, ask your provider for details.

With 'On the following days', you can limit the fetching process to certain days. Specify "Mon Tue Wed Thu Fri, From 8 To 18, Every 15 Minutes" to limit the fetching process to your office hours. The interval for fetching mail is especially important for dial-on-demand connections (such as ISDN). To save costs, extend the intervals, as the e-mail server must dial up the provider every time mail fetched.

Receiving E-Mail via UUCP

Preconditions:

- User name for uucp
- Password for uucp
- Address of the e-mail server

Tip

If you applied for a normal WinShuttle account, you need to negotiate a separate password for UUCP over the WinShuttle phone hotline (not the same as the normal WinShuttle access password). Subsequently, WinShuttle will set up the uucp access, which will usually be active and ready for use on the following day. The address of the e-mail server for WinShuttle accounts is usually mail.KFZ.shuttle.de.

Tip

As far as possible, all preliminary steps for the configuration have been taken. The needed RPM packages are installed, and the Postfix configuration does not need to be modified. You merely need to adapt four configuration files and automate the mail exchange.

Adapting the Configuration Files   The following files have to be set up in the
directory `/etc/uucp` with the respective contents:

```
shuttle           <winshuttle-username>  <password>
```

File 1: Content of the file call

```
nodename    <winshuttle-username>
```

File 2: Content of the file config

```
port    TCP
type    tcp
```

File 3: Content of the file port

```
system          shuttle
call-login      *
call-password   *
time            any
address         <winshuttle-emailserver>
commands        rmail #rnews
port            TCP
```

File 4: Content of the file sys

Setting the Permissions   Use the command

```
chown uucp.root *
```

to assign all files to the user `uucp`. Then enter

```
chmod o-r *
```

in order to cancel the read permissions for all other users.

Testing the E-Mail Reception   Now it should be possible to activate the recep-
tion of e-mail via WinShuttle with the command:

```
uucico -S shuttle
```

E-mail addressed to users existing on the system will be fetched and de-
livered.

Following the first mail exchange, the log files will be located in `/var/log/uucp`:

`Stats` contains general information on the transmitted amount of data. `Log` – which is more important in the event of an error – contains information on the (successful) login and mail exchange.

Automating the E-Mail Exchange   Activate the following line in the file `/etc/crontab.in`

`#30 * * * * root /bin/bash /usr/sbin/uucico -S shuttle`

by removing the # at the beginning. The e-mail exchange will be activated every half hour.

Alias Management

This front-end facilitates the management of "mail aliases". Each mail recipient can be assigned an unlimited number of aliases. The dialog features the assigned aliases to the left and the associated user names next to them. The alias fields can be edited directly. To complete the procedure, click 'Save'.

To remove an alias or add additional users to an alias, click 'Add or Remove' to the right. You will be taken to another dialog in which existing users can be added to or removed from the alias with the help of the arrow keys. If you remove all users, the selected alias will also be removed.

In this dialog, you cannot create any new aliases. To do this, go to 'User' → 'Edit'. Select the user to whom to assign a new alias and click 'Edit user data'. Enter one or several e-mail addresses (separated by spaces) and click 'Update'. When you return to the 'Alias Management', this user will be listed together with his alias.

Security

┌─ **Note** ──────────────────────────────

Secure Default Configuration

Here you can modify some settings affecting the security of the server services. Normally, nothing needs to be changed, as the services are started with a secure default configuration.

─────────────────────────────── **Note** ─┘

SSL Configuration

The dialog for the SSL configuration consists of three sections for SSL for Apache, SSL for Cyrus IMAPD, and SSL for OpenLDAP (see Figure 4.11).
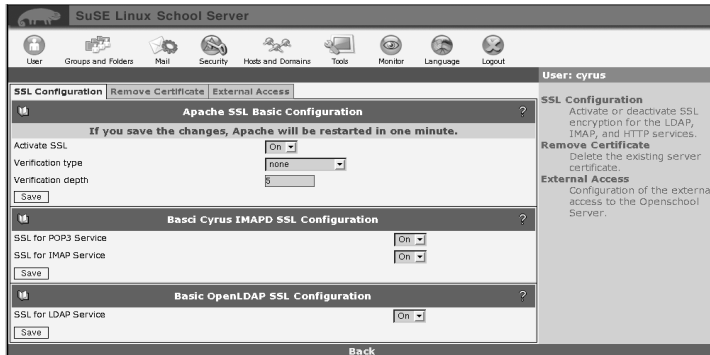
Figure 4.11: SSL Configuration

Basic Configuration of SSL for Apache

Click 'Activate SSL' to enable a secure client-to-server connection. The button is only available if you created a CA (Certification Authority) and a server certificate. If this is the case, select a verification method:

none   No verification for a valid certificate.

optional   The presence of a certificate is checked, but access is granted even without a certificate.

require   Access is only possible with a valid certificate.

optional_no_ca   Verification for an existing certificate. However, the certificate does not have to be valid.

CAs can be organized hierarchically. This means that a CA can be validated by another CA. In turn, the validity of the latter can be confirmed by a "superior" CA. The 'verification depth' specifies the number of steps the Apache web server traces the validity of CAs until they are rejected. The default value is '10'.

Basic Configuration of SSL for Cyrus IMAPD

Activate SSL for IMAP and POP3. The POP3 or IMAP server must be restarted after every activation or deactivation. All mail clients currently connected to the server will be disconnected.

Basic Configuration of SSL for OpenLDAP

Activate SSL for the LDAP service. The LDAP server also must be restarted after every change.

Certificate Management

In the certificate management dialog, you can delete your existing server certificate. For this purpose, you need the CA password, which corresponds to your admin password. Once the certificate is deleted, you can generate or import a new certificate. Use the existing CA or create a new CA for generating a server certificate.

┌─ Note ──────────────────────────────────

If you delete your CA or create a new CA, existing client certificates will no longer be valid.

────────────────────────────── Note ─┘

Create your own CA or import a certificate signed by a trust center. The latter is subject to a fee and is not mandatory for the smooth operation of your mail server.

Create your own certificate to use your server as CA. Fill in the required fields. You will need the CA password for generating certificates for your clients. The password cannot be changed posteriorly.

In the following dialog, generate the server certificate that is signed by the CA. If possible, use a different password. 'Host name of the web server' refers to the name of your server. If the name stored in the server certificate does not correspond to this name, some browsers (like Netscape) will question the certificate each time a secure connection is established to the server. After generating the server certificate, you can generate certificates for individual users. Additionally, you can now activate the SSL function of Apache and Postfix.

External Access

Normally, the server's firewall blocks all access from the external interface. However, you can configure the server in such a way that some services can be accessed from the Internet.

Allow SSH access

This button enables remote administration of the server by way of an SSH con-
nection. For this purpose, the port 22 in the firewall is opened for external ac-
cess.

If you activate X-forwarding, the remote administration of the server will be
like sitting in front of the actual machine. In this way, even YaST can be started
with the graphical interface. On a Linux client, all you have to do is enter the
command `ssh -X -l admin <ip-address>`.

Allow access to the admin GUI

If you want quick access to the web interface for the server administration,
activate this button. In this case, you will be able to administer the server
from the Internet with any web browser by entering the URL `https://
<ip-address>:444/` in the location field of the browser. Important: Be sure
to enter port 444 correctly at the end of the address.

Allow access to the mail/groupware

Activate this button if you want your students to be able to access the mail and
groupware interface of your server in their free time.

In this case, every user existing on the server (except for `admin`) will be able to
log in to the server and perform actions like reading e-mail, provided he knows
the URL of the server. The mail and groupware interface can be accessed by
entering the URL `https://<ip-address>/` in the browser.

┌─ **Note** ──

  Remember that this makes the server accessible for all users from the
  Internet. If a student uses a weak password for his account, others may
  be able to use this account for malicious purposes ...

  ─── **Note** ─┘

Hosts and Domains

Registering New Clients

Regardless of the operating system of the client host, clients have to be registered with the server in order to associate the workstations with a room and enter the respective DNS and DHCP services.

Prior to the actual registration, clients usually have to be configured correctly. The following section provides a brief overview of the individual client types. Refer to Chapter 5 on page 101 for more details.

SuSE Linux clients with autoinstallation

- Install the clients with the autoinstallation function of SUSE LINUX School Server as described in Chapter 6 on page 125.
- Start a web browser and register the client as described further below in this chapter.
- To be on the safe side, restart the network services of the client (with `rcnetwork restart` or reboot the client.

Connecting existing Linux clients

- Configure the network card of the client in such a way that it receives its IP address and its host name via `DHCP` and restart the network services if necessary.
- Use YaST to configure the client as `LDAP client`.
- Use YaST to configure the client as `NFS client`.
- Start a web browser and register the client as described further below in this chapter.
- To be on the safe side, restart the network services of the client (with `rcnetwork restart` or reboot the client.

Windows clients

- Configure the network card of the client in such a way that it receives its IP address via `DHCP` and reboot the machine.
- Start a web browser and register the client as described further below in this chapter.
- Subsequently, change the name of the client in the network properties in such a way that it corresponds with the name assigned via `DHCP` and reboot the machine.

- If necessary, include the client in the domain as described in 5 on page 104 and reboot the machine.

Mac clients

- First, activate and start the `Netatalk` service on the server's administration pages under 'Monitor' → 'Service Monitoring'.

- Configure the network card of the client in such a way that it receives its IP address via `DHCP`.

- Start a web browser and register the client as described further below in this chapter.

- Integrate the needed server drives on the client by means of the 'Selection' menu.

To register a client with the server, start a browser (Konqueror, Netscape, Opera, or Internet Explorer) and go to the SUSE LINUX School Server administration pages: `https://admin`. Log in as `admin` and select 'Hosts and Domains' → 'New' (see Figure 4.12).

Figure 4.12: Registering Clients with the Server

Now select the desired room under 'List of the registered classrooms' or associate the machine with a new room under 'Name of the new classroom'. Following the successful registration of the client, the new room will be included in the 'List of the registered classrooms'.

Note

The host name is derived from the room name as follows:
`<room>-pc<NN>` (e.g., `music1-pc01`). Due to the DNS conventions, the name of a room may only consist of the letters of the English alphabet, numerals, and the `'-'` sign. As Windows operating systems only support host names consisting of no more than 15 characters, room names to be used for Windows clients should not exceed 10 characters.

Note

Figure 4.13: Adding a Client

If you configured one or several virtual domains for the server, you can select the domain name under 'Choose a Domain'.

To add a Windows machine to the school network, select the menu item 'Should the workstation join the Windows domain?'. Then click 'Execute Admission'. The result of the integration – the IP address, host name, hardware address, and possibly the Netbios name – will be displayed (see Figure 4.13). During the registration, the system creates a new user whose name and password corresponds to the host name of the registered machine (workstation user).

In this way, examinations can be realized in a protected environment. For this purpose, students will not log in to the system with their own login (UID), but with the login of the host. Thus, they have a standard environment and no access to their own data. For more information, refer to 8 on page 162.

Now the client machine is integrated in the school network. The next step for a Windows machine is the registration with the domain (see 5 on page 104).

For MAC OS 9.X clients, nothing else needs to be done.

Autoinstalled Linux clients do not require any further configuration. For other Linux clients, refer to 5 on page 102.

> **Tip** ┐
>
> **Changing the Client Information**
>
> If the hardware address of a client changes (e.g., due to a new network
> card), delete the respective client entry and create it anew.
>
> └ **Tip**

Deleting a Client Entry from the Server

To delete a client entry on the server, the respective entry must be removed from
the DHCP server.

To do this, select the menu item 'DHCP Configuration' under 'Hosts and Do-
mains' and click (Manage Hosts). Then search the respective group for the host
name and click (Delete). To activate the change, click (Export) at the bottom of the
page.

Setting Access Rights
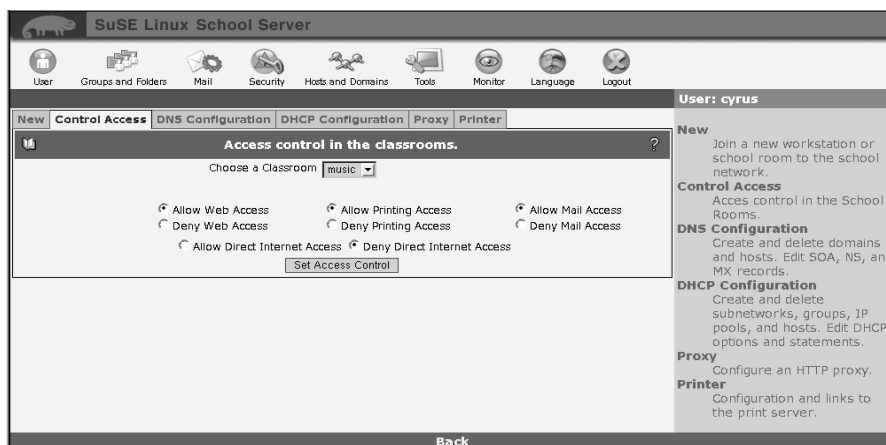
Figure 4.14: Access Administration of the Hosts in the Rooms

Once the machines of the school have been registered with the server and as-
signed to rooms, certain services (Internet access, access to the mail and group-
ware server, access to the print server) can be enabled or disabled for the ma-
chines of a room. However, the access to the main server (`https://admin`)

cannot be disabled, as this server offers a number of indispensable services (`DNS`, `DHCP`, `nfs`, `samba`).

Teachers can set these services for the current classroom. The main administrator `admin` has control over all registered rooms.

DNS Configuration

Here you can create virtual domains, assign and delete host names, and edit the values for `SOA`, `NS`, and `MX` in the zone files.

> **Note**
>
> Changes in this menu item will only be applied if you click 'Export'.
>
> **Note**

To avoid errors in the configuration of the DHCP server, clients integrated by means of the menu item `New` will not be listed in the DNS configuration. Nevertheless, you can view the clients registered on your server under the menu item 'Manage Hosts' in the DHCP configuration.

Creating and Editing Virtual Domains

Many schools use several domains, such as the main domain `school.com` and the virtual domains `school.net` and `my-school.com`. Frequently, the additional domains merely serve a functional purpose, such as publishing the web presence in multiple languages. SUSE LINUX School Server supports the use of an unlimited number of virtual domains and users and is able to distinguish between the users in the various domains on the basis of this extension. E-mail messages to a virtual user in a virtual domain (e.g., `principal@physics-school.com`) are forwarded to a real user in the main domain (e.g., `principal@school.com`).

The same component of an e-mail address (`principal` in this example) can be used for the main domain and for the virtual domain. SUSE LINUX School Server distinguishes these on the basis of the domain. If necessary, give the real recipient the virtual e-mail address as sender address. This enables the implementation of domain-specific users for external use.

Before you can create a virtual user, you have to create the respective virtual domain. Click 'Hosts and Domains' → 'DNS Configuration'. To create a new domain, enter the name of the domain in the field behind 'New Domain' and confirm with 'Add' (see Figure 4.15 on the next page). In this way, you can add an unlimited number of virtual domains.

Figure 4.15: *Creating and Editing Virtual Domains*

To add existing domains in the name service configuration, click 'Export'. The new domains should appear in the list at the top left.

To add your own zone databases in addition to the automatically generated configuration for the server domain and the virtual domains, simply use names that do not correspond to those generated by the server. Zone files are designated according to the following scheme:

For "forward mapping": `/var/named/school.com.zone`. For "reverse mapping", the "IN-ADDR.ARPA" address is added to the file names.

To delete an existing domain, select it from the top left frame and click `Delete`. However, you can only delete a domain if no virtual e-mail addresses are defined for this domain.

Domain Types

SUSE LINUX School Server supports two types of virtual domains. The characteristics of these domains depend on how these are mapped by LDAP queries and implemented on "virtual tables" of Postfix. Check the file `/etc/postfix/virtual` for details.

Type S (default) All local users can receive e-mail under this domain. Moreover, additional "virtual" addresses can be configured for specific local users. This virtual domain type was already used by SuSE Linux Openexchange Server 4. In the Postfix documentation, it is referred to as `SENDMAIL-STYLE VIRTUAL DOMAIN`.

Type P   In this virtual domain type, no e-mail address exists unless you configure a virtual address. Local users can *not* receive mail under this domain. If a message is sent to a nonexistent address within this domain, the MTA (Postfix) will reject it as nonexistent. In the Postfix documentation, this type is referred to as `POSTFIX-STYLE VIRTUAL DOMAIN`.

We recommend using type `P`. You can recognize this from the `[P]` preceding the domain name.

Manage Hosts

To add or delete a DNS entry, select 'Manage Hosts'. On the following page, all hosts are listed in the left frame.

> **Tip**
>
> **Hosts Entered in the DHCP**
>
> Remember that clients added with the menu item 'New' are not displayed in this list. You can only see and delete these hosts in the DHCP configuration.
>
> This prevents malfunction of the DHCP server due to an orphaned entry (if a client was deleted in the DNS configuration but not on the DHCP server).
>
> **Tip**

Click 'Add Host', enter the host name and IP number of the new host, and confirm with 'Create'.

Subsequently, you can specify additional host names and IP numbers or exit the dialog by clicking a different menu.

To remove a client from the local network, select the entry in the left frame and click 'Delete Host'.

> **Caution**
>
> If the IP number of a client changes, remove the entry and create a new entry.
>
> **Caution**

DHCP Configuration

The dialog for the DHCP configuration can be accessed under 'Hosts and Domains'. You can create and remove subnets, groups, and hosts and edit DHCP entries.

Configuration of the DHCP Server
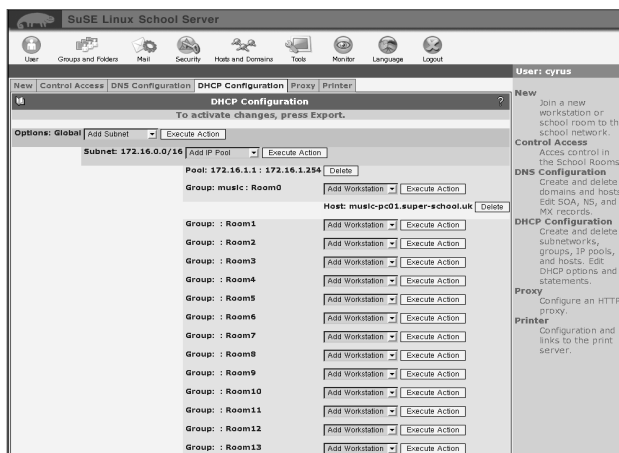
Figure 4.16: DHCP Configuration

To add a new entry (subnet, group, or host) to the configuration, click the respective button (see Figure 4.16).

Existing subnets, groups, hosts, and IP pools that were created during the installation of SUSE LINUX School Server are listed in this dialog. Select an action for the respective entry from the selection box and click 'Action'.

No entries can be added to pools and hosts. They can only be deleted.

Caution

When an entry is deleted, all subentries will also be deleted.

Caution

To edit or add the DHCP options or statements in an entry, click 'Edit'. The following DHCP entries can be created:

DHCP Subnet This is the basic entry for the DHCP server. This entry specifies for which subnets with which IP address mask the DHCP server is responsible. All additional DHCP objects can be added in a subnet.

Group Hosts (host names) handled by the DHCP server with the same DHCP parameters (options, statements) are combined in a group. Only host objects can be added to a group. However, a group can be part of the global configuration and of a subnet.

IP Pool An address pool defines an IP address space that is treated differently than the other IP addresses. When a DHCP pool is created, the IP addresses in the IP pool are registered with the name server and host names are generated for these IP addresses.

Host To add a host to the DHCP configuration, it first must be entered in the DNS configuration. A host can be added to the basic configuration, to a DHCP subnet, or to a group.

> **Note**
>
> To be able to start the DHCP server, at least one subnet must be defined.
>
> **Note**

Changes to the DHCP configuration are saved by the LDAP server. Click 'Export' to generate and reload the configuration of the DHCP server.

Adding a Group to the DHCP Configuration

In this dialog, you can add a new DHCP group. Hosts (host names) handled by the DHCP server with the same DHCP parameters (options, statements) are combined in a group. Only host objects can be added to a group. However, a group can be part of the global configuration and of a subnet.

If you create a group in the 'Global DHCP Configuration', the hosts of this group can get their IP addresses from various subnets. In this case, all subnets must be configured. If you create a group in a DHCP subnet, make sure that the hosts of this group get their IP addresses from this subnet.

The group designation can be selected freely. Click 'Confirm' to add the new group to the DHCP configuration. If necessary, the automatically generated DHCP options and statements for the newly created group can be modified under 'Expert Options'.

Adding a Host to the DHCP Configuration

Click 'Add Workstation' to enter the dialog. Select a domain and click 'Next'. Select a host from the list, enter the hardware address of the network card (MAC), and click 'Confirm'. If the host is not listed, it must be created in a DNS domain with 'Create Host' in the 'DNS Configuration' dialog. If the selected domain does not contain any hosts that are included in the DHCP configuration, you will automatically be taken to the 'DNS Configuration' dialog.

Once the host has been added, DHCP options and statements can be defined for the newly added host. To do this, click 'Expert Options'.

> **Note** ─────────────────────────────────
>
> A host that is added to the DHCP configuration cannot be removed from
> the name server. It is not listed under 'DNS Configuration' → 'Manage
> Hosts' → 'Delete Host', as the unintentional deletion of this entry can
> impair the functionality of the DHCP server. To remove a host entered
> in the DHCP configuration from the name server, delete the DHCP host
> entry first.
>
> ──────────────────────────────────── **Note** ─┘

Adding a Subnet to the DHCP Configuration

Click 'Add Subnet'. Define the network address in the dialog and the netmask
of the subnet in 'Netmask'. The netmask can be entered in bitmask form (e.g.,
24) or in decimal form (255.255.255.0).

This entry specifies for which subnets with which IP address mask the DHCP
server is responsible. All additional DHCP objects can be added in a subnet.

Click 'Confirm' to enter the new subnet in the DHCP configuration. If necessary,
the DHCP options and statements for the newly created subnet can be modified
under 'Expert Options'.

Options and Statements of a DHCP Entry

Modify the options and statements of a DHCP entry in 'Expert Options'. The
dialog displays the current values of the entry. Some parameters (such as object
classes, cn) are only readable. To change the value of an option or statement,
edit the respective text field and click 'Save Changes'.

To delete an option or statement, click the 'Delete' checkbox to the right of the
value then click 'Save Changes'. To include a new option or statement in the
DHCP entry, enter it in 'New' and click 'Save Changes'.

> **Note** ─────────────────────────────────
>
> Do not enter the word option for DHCP options.
>
> ──────────────────────────────────── **Note** ─┘

Click the question mark next to 'New' to open a window with a list of DHCP
options and statements. Select the desired item and click 'Choose a DHCP pa-
rameter'. Then click 'Close'. The entry will be adopted in 'New' and can be ex-
panded if necessary.

To restore the previous values, click 'Reset Selection'. Click 'Export' to generate
and reload the configuration of the DHCP server.

Dynamic DNS

Dynamic DNS is a service for allocating one or several host names to your dynamic IP address. As soon as you dial up the Internet and get a new dynamic IP address, the new IP address will be entered for the name. In this way, other users can contact you under this host name.

To use this service, register with a provider who offers these services. You will receive a login and a password for administering one or several host names. The service scope and fee varies from provider to provider. Depending on the provider, select a name from a list of domains or register your own domain (e.g., custom DNS service at `www.dyndns.org`).

Some providers or services support additional settings, such as the use of wild cards or the specification of a mail server or backup mail server. These additional settings are only displayed for providers who support these settings.

Login: Enter your registered user name.

Password: Enter your registered password.

Host Name: Enter the host name or comma-separated list of host names registered with the dynamic DNS provider. The provider `www.dslreports.com` provides unique numbers instead of host names. Enter these in the field for host names.

Wild Card: This switch enables the use of the dynamic DNS host name like a subdomain. If your host name is `myhostname.dyndns.org`, the names `www.myhostname.dyndns.org` and `ftp.myhostname.dyndns.org` also point to `myhostname.dyndns.org`.

Mail Server: Here you can specify the host name of a mail server that should receive e-mail for your host (such as the mail server of your provider). In this case, e-mail will not be delivered directly to your host.

> **Note**
>
> This mail server must be configured correctly and accept e-mail for your host name.
>
> **Note**

Backup Mail Server If 'Backup Mail Server' is activated, the host specified as mail server will be used as backup mail server. Your host name using a dynamic IP address will be used as primary mail server. In this case, e-mail will first be delivered to the host name using a dynamic IP. If this host cannot be reached, the mail will be delivered to the secondary server.

If you do not specify any mail server, the host name should be created as virtual domain in the 'DNS Configuration' for the purpose of receiving e-mail. This is not necessary if the host name is not used to receive mail.

> **Caution**
>
> With dynamic IP addresses, the name will continue to point to the IP address even when the machine is offline. If the provider allocates this IP address to another customer, your e-mail will go there!
>
> **Caution**

Update Type: DynDNS.org offers three types of dynamic DNS. Select the type that is suitable for the host name type.

dyndns: Dynamic DNS is the default setting.

static: Static DNS is similar to dynamic DNS, but the IP address is valid for a longer time. This is useful if your provider usually gives you the same IP address and the address does not change frequently.

custom: Custom DNS enables updates for your own domains and subdomains run at DynDNS.org.

Proxy

By default, the IP address of the proxy server (e.g., `192.168.0.5`) and the port `8080` are already entered in the proxy dialog.

The cache size is preset to 500 MB, but can be adapted as required. The check box 'Use Web Filter' is activated, but can be deactivated if you do not want to use SquidGuard.

More information on SquidGuard is available in the annex of the online manual (`http://admin/manual/manualEN.pdf`).
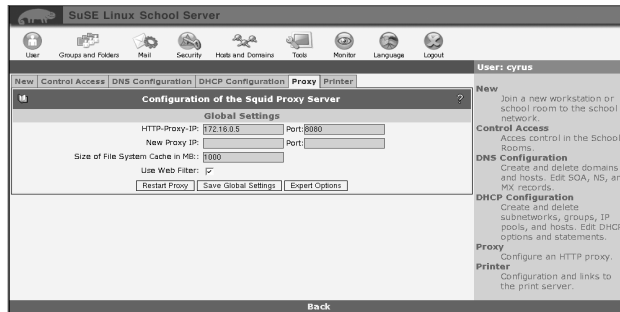
Figure 4.17: Proxy Configuration

Click 'Expert Options' to access the ACL dialog in which you can define new ACLs (Access Control Lists) or edit existing ones.

After you have defined ACLs, click 'Order ACLs' to set the processing sequence. The rules are processed from the top down until a rule matches. Click 'Global Settings' to return to the proxy dialog.

Defining ACLs

Figure 4.18 on the next page shows the ACL dialog. First, enter a name for the new list. Then select a 'Type' for your ACL. The following types are available:

browser Specification of browsers.

dst (destination) Specification of target addresses.

dstdomain Specification of the target domain.

dstdom_regex Specification of the target domain using regular expressions.

ident User authentication over the ident daemon. Specify one or several user names or REQUIRED, which includes all valid user names.

maxconn Maximum number of connections.
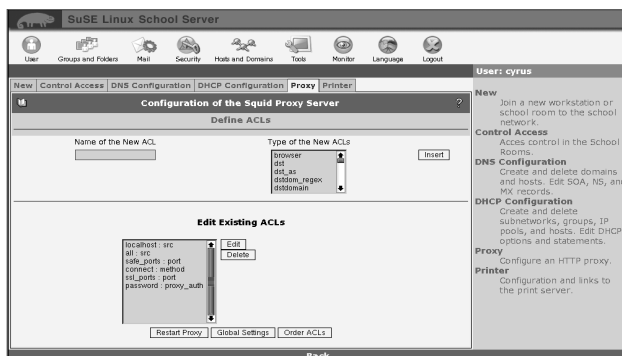
Figure 4.18: Defining ACLs

method   Specification of the method (CONNECT, POST, or GET).

port   Port specification.

proto (protocol)   Specification of the protocols.

proxy_auth   User authentication over squid_ldapauth

snmp_community   Specification of the SNMP community (Simple Network Management Protocol). Can be used to grant certain SNMP agents access to Squid. The default setting for community is public. However, this value can be changed as needed and serves the authentication of the agents, which can query information such as the version, memory, and hard disk usage from the running Squid.

src (source)   Specification of the source addresses.

srcdomain   Specification of the source domain.

srcdom_regex   Specification of the source domain, using regular expressions.

time   Time specification.

url_regex   Specification of URL addresses, using regular expressions.

urlpath_regex   Specification of URL paths, using regular expressions.

Detailed documentation for the Squid proxy is available at `http://squid.visolve.com/squid24sl/contents.htm`. For more details for the various

ACLs, see `http://squid.visolve.com/squid24s1/access_controls.htm`.

Click 'Add' to add a new ACL to the list of existing ACLs. Click 'Edit' to open a window in which to enter or edit values for a selected ACL. In the input field, add new values or edit or delete existing values. To remove entire ACLs, click 'Delete'. Click 'Save' to save your changes. 'Back' returns to the proxy configuration. Click 'Order ACLs' to access the dialog for setting the sequence of the ACLs.

Order ACLs

The settings in 'Defined ACLs' and in 'Defined ACLs Negated' are linked with "AND". With the 'Action' field, you can 'allow' or 'deny' Internet access.

Apply your settings to an existing list under 'Defined ACLs' or select an ACL to negate from 'Defined ACLs Negated'. For example, you can permit access to Internet pages (selection from 'Defined ACLs'), except for those using SSL ports (selection from 'Defined ACLs Negate').

Click 'Add' to add a new rule. The rule will be listed under the defined ACLs. To delete a rule, select it from the list and click 'Delete'. Use 'Up' and 'Down' to move a selected rule up or down in the list.

> **Caution**
>
> The sequence of the rules in the list is very important, as the list will be processed from the top down. Depending on which rule applies first, access to the required URL will be granted or blocked.
>
> **Caution**

After you have performed all changes, click 'Global Settings' to return to the proxy dialog. The changes will be effective after you have restarted the proxy.

Printers

The printer dialog, shown in Figure 4.19 on the facing page, features a number of links for the print server. By means of these links, view a list of printers and print jobs or administer the print server. If you click 'Administration', you will be required to log in as the user `root` with the administrator password (same as the `admin` password). Click 'Help' to access detailed instructions for all configuration options.

Configure the local print server in the lower part of the printer dialog. Specify the IP addresses or broadcast IPs for an entire network to which the print server
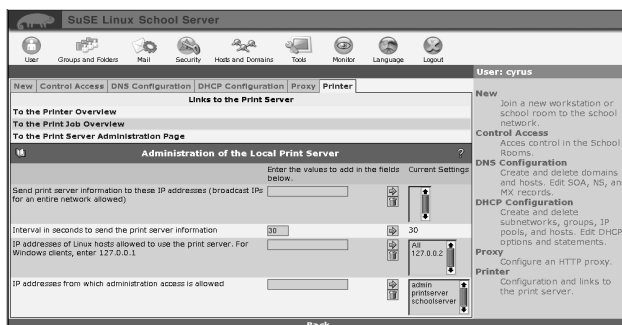
Figure 4.19: *Printer Administration*

information should be broadcasted. Click (Enter) or the arrow symbol to adopt the entry in the current settings. Then set the broadcasting interval for the information. In the next field, enter the IP addresses of all hosts that should be granted access to the print server. In the last field, enter the IP addresses of certain hosts that should be granted administrative access to the print server.

Tools: Additional Functions

LDAP Browser: Editing the LDAP Database
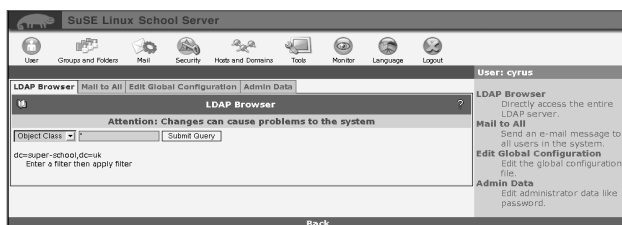
Figure 4.20: *Tree Structure of the LDAP Browser*

SUSE LINUX School Server uses the LDAP directory service for its internal group and user management (also for Samba), address management, mail routing, DNS, and DHCP. In addition to the configuration dialogs of these services, the LDAP browser can be used for editing, deleting, and adding attribute values to existing entries. See Figure 4.21 on the next page.

> **Caution**
>
> Do not change any settings unless you are sure about what you are doing,
> as incorrect settings can render the server inoperable.
>
> **Caution**
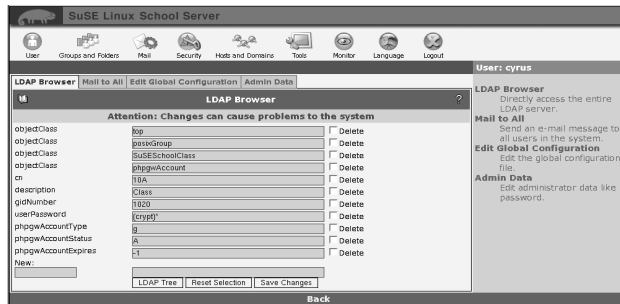
Figure 4.21: Editing LDAP Settings

LDAP directories have a tree-like structure. All entries (called objects) in the
directory have a defined position in this hierarchy. This hierarchy is referred to
as the *Directory Information Tree* or DIT. The complete path identifying a specific
entry is referred to as the *Distinguished Name*. The individual nodes on the way
to this entry are called *Relative Distinguished Names* or RDN. Basically, there are
two types of objects:

Containers   These objects can contain other objects. Object classes are `root`
(virtual root element of the directory tree), `c` (country), `ou` (organization-
alUnit), and `dc` (domainComponent). This model is similar to directories
(folders) in a file system.

Forms   These objects are located at the tip of a branch. They do not have
any subordinate objects. Examples: `person`, `InetOrgPerson`,
`groupOfNames`.

For more information on `LDAP`, refer to the annex of the online manual (`http:
//admin/manual/manualEN.pdf`).

Mail to All: Message from the Administrator

Sometimes the mail administrator (`mailadmin`) may want to send an e-mail
message to all users. For example, the server may need to go offline due to

maintenance tasks. To do this, enter the subject and the message body. See Figure 4.22. The e-mail message will be sent to all existing users, regardless of their quota.

Figure 4.22: A Message from the Administrator

Global Configuration

These settings affect the web-based configuration and some of the components of your server. The configuration file is located on the server in the file `/etc/imap/globals.conf`.

GENERAL

> **EnableUserSpamFrontend**   Enables or disables the SPAM filter front-end in the filter settings for users.

> **EnableSieveEditor**   Enables or disables the SIEVE filter editor in the filter settings for users.

> **EnableDynDns**   Enables dynamic DNS.

> **MonitorResolveAddr**   Resolution of IP addresses to host names in the online monitor.

> **NewUserChangePassword**   If you activate this function, the user will be prompted to change the password assigned by the administrator after the first login.

> **UserJpegPhotoMaxHeight**   Specifies the maximum height of user photographs. The proportions are retained if the photograph is scaled.

UserJpegPhotoMaxWidth Specifies the maximum width of user photographs. The proportions are retained if the photograph is scaled.

MonitorServices Specify the services to be displayed in the menu 'Monitor' → 'Service Monitoring'. Basically, you can specify every service that has an "rc" start file.

SESSIOND

SessionTimeout

SessionTimeout Here you can set the time-out after which a user is automatically logged out from the web front-end.

SessionHost; SessionPort; SSL_key_file; SSL_cert_file and SSL_ca_file Currently these options are not needed. They are intended for a possible relocation of the administrative web front-end to another host.

SECURITY

UseCookie The options 'UseCookie' and 'CheckClientIP' prevent a user's session from being stolen if an attacker gets access to the session ID of the respective user. 'UseCookie' is more secure than 'CheckClientIP', as it saves an additional ID in a cookie in the browser of the respective user.

CheckClientIP To prevent a session from being stolen, 'CheckClientIP' checks whether the web front-end is accessed by only one host per user. As IP addresses can be faked and a user may access the front-end by way of a proxy cluster using varying IP addresses, this option is not as efficient as the method using cookies.

DefaultPasswordHash Here you can specify the default encryption method for user passwords.

FETCHD

debug If you set this option to a value greater than 0 and restart "fetchd" by entering `rcfetchd restart`, you will receive debug information.

keeponserver If you activate this option, e-mail messages will not be deleted from the server after they are fetched. Normally, you should not activate this function, as all e-mail would be fetched from the server repeatedly.

unixsocket This socket is used for the communication between the web client and `fetchd`.

ldaphost Here, specify the host name or IP address of the LDAP server on which fetchd should store the data of the user mailboxes.

ldap_reconnect_interval fetchd maintains a permanent connection to the LDAP server. If this connection is terminated or becomes invalid, a new connection is established after the interval (in seconds) specified here.

ldap_max_reconnect The maximum number of attempts fetchd should make to reestablish the connection to the LDAP server.

mailadmin The name of the local folder for saving administrative messages.

append_fetch_header Use this option to append a special header to every e-mail messages fetched with fetchd.

drop_undeliverable_mail If you set this option to `true`, undeliverable mail will be discarded without comment.

thread_max Maximum number of concurrent processes started by the fetchd scheduler. This value should not be too high, as such a process might use a lot of memory.

priority_granularity This value should be at least twice the value of 'thread_max'.

SQUID

squid_conf_file Here, specify the configuration file for Squid.

Edit Administrator Data

Under the menu item 'Admin Data' you can edit the data and the password of the main administrator `admin`.

To change the password, click 'Set Password'. You will be taken to another dialog. Enter the old password once and the new password twice (see Figure 4.23 on the next page).

Note

Do not forget the password. The server cannot be administered without the password.
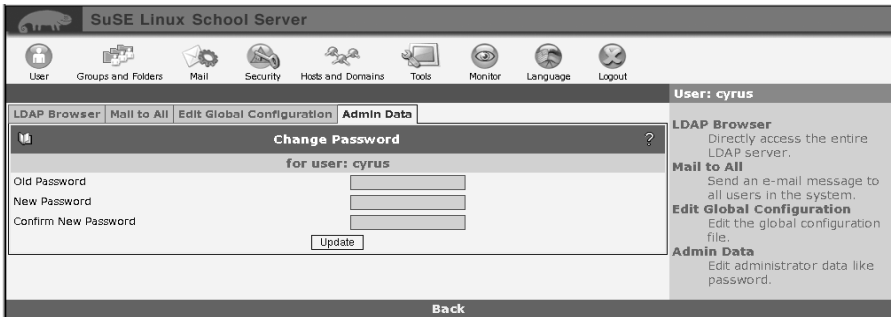
Note

Figure 4.23: *Changing the Administrator Password*

System Monitoring

Online Users

This item provides an overview of the users currently online using the web front-end. Only internal server sessions are listed. POP3 and IMAP connections are not listed. Click a user ID to delete the respective user session. You cannot delete your own session.

Figure 4.24: *Online Users*

Mail Queue

This dialog shows the e-mail messages currently processed by Postfix. Enter the refresh rate in seconds (e.g., 5 seconds) and press (Enter). The dialog will be updated at this interval. To disable this function, select the menu item 'Mail Queue' anew. Usually, no messages are listed permanently. If the Postfix system is stopped or e-mail cannot be delivered for any reason, messages that still need to be delivered will be listed here.

Click 'Flush Queue' to prompt Postfix to process accumulated messages immediately. You can also delete accumulated mail. To do this, click the queue ID of the respective message. However, this will delete the message permanently.

Mail Statistics

Click 'Mail Statistics' to view a chart of the mail processed during any period between the past 24 hours and last year. The error statistics and data volume are displayed in other charts.

System Statistics

This item provides an overview of your server load.

> **Note**
>
> Following a hardware modification, such as the repartitioning of a hard disk, you must reinitialize the system monitor. To do this, enter the following commands:
>
> ```
> /usr/lib/sysMonitor/clearall CLEAR_GRAPHS
> ```
> ```
> /usr/lib/sysMonitor/clearall CLEAR_DATABASES
> ```
> ```
> /usr/lib/sysMonitor/SETUP.pl
> ```
> ```
> /usr/lib/sysMonitor/rrdtimer gv
> ```
>
> **Note**

Service Monitoring

This menu item provides an overview of important system services and their current statuses. See Figure 4.25 on the following page. All services currently listed after the parameter `MonitorServices` in `/etc/imap/globals.conf` will be displayed.
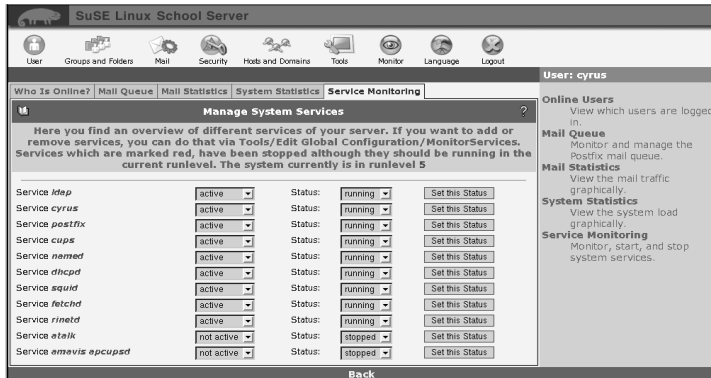
Figure 4.25: Service Status

A service can be active or inactive. Active services are started automatically when the system is booted.

Furthermore, you can start, stop, reload, and restart services. When you restart a service, it is stopped then started again. When you reload a system, it is not stopped, but its configuration will usually be reloaded and some features initialized. This function is not supported by all services. Click 'Set Status' after you have changed the status of a service.

Language

Select the preferred language for the web front-end and click `Set Language`.

Client Configuration

SUSE LINUX School Server is preconfigured for the communication with Linux clients and Windows clients. This chapter shows what you need to watch and how to configure heterogeneous networks.

Configuration of Linux Clients

To enable SuSE Linux users to log on to the server and get their home directories from the server via "automounter", the hosts must be configured as LDAP clients.

If the clients were installed with the included autoinstallation tool, no additional configuration is needed.

Tip

Perhaps you may have to install a number of RPM packages on the clients. This can be done by means of the YaST module 'Install and Remove Software'. In this module, change the filter to "Package Groups" and select the following packages under `Productivity/Network/LDAP/Client`:

- `nss_ldap`
- `pam_ldap`
- `openldap2-client`

Select the following package under `System/YaST`:

- `yast2-ldap-client`

Tip

Start the YaST module 'LDAP Client' (see Figure 5.1 on the next page).

Activate the check box 'Use LDAP' and enter the 'LDAP base DN'. In the second field, specify the SUSE LINUX School Server as the LDAP server. If SSL for LDAP is activated on the SUSE LINUX School Server, activate TLS/SSL encryption for the communication with the server on the client side. Confirm your input with 'Finish'.

Under 'Network Devices' → 'Network Card', configure the network adapter as follows:

- Select "Automatic address setup (via DHCP)".

- Under 'Host name and name server', activate the check boxes "Change host name via DHCP" and "Update name servers and search list via DHCP".

This will facilitate the administration of the network, provided the client is logged on to the server with the correct name (see 4 on page 77).
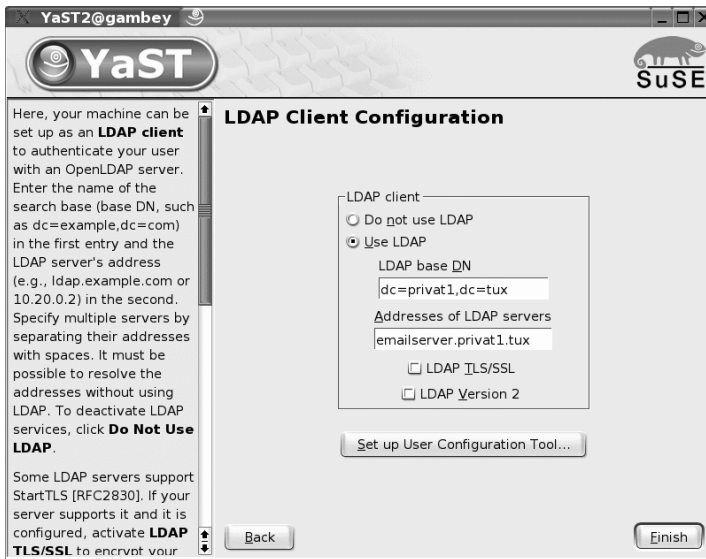
Figure 5.1: LDAP Client Configuration

This is all that is needed to configure SuSE Linux desktops as clients for SUSE LINUX School Server. The following overview lists all values you may need for the configuration:

- NFS client (normally handled automatically by the automounter):

  Host name of the NFS server: `nfs`
  Remote file system: `/home`
  Mount point (local): `/home`
  Options: `defaults,rsize=8192,wsize=8192,soft`

- LDAP client

  Do not use LDAP `Off`
  Use LDAP `On`
  LDAP base DN Your "ldapbase" is located in the file `/etc/openldap/ldap.conf` on the server.
  LDAP server addresses `ldap`
  LDAP TLS/SSL `Off`
  LDAP version 2 `Off`

Configuring Windows Clients

To use the server as PDC, integrate your Microsoft Windows system in the domain operated by the server in order to benefit from the advantages of a central user management. This will facilitate the users' access to the data and printers administered by the server, as no additional authentication is needed once a user has logged on to the PDC.

To use SUSE LINUX School Server as PDC for your existing Microsoft Windows clients, the respective hosts must be registered with the system. For this purpose, the server automatically creates a machine account for every workstation. No additional steps are required on the server. The following sections briefly describe the configuration procedure for various Microsoft Windows clients.

Microsoft Windows 9x/ME

First, make sure that all software components Windows needs for accessing the server are available. In the Control Panel, select the item 'Network'. A window with three tabs and an overview of the installed network components will appear (see Figure 5.2 on the next page).

Configuring a Network Connection to the Server

Apart from the network adapter installed in the machine, the "Client for Microsoft Networks" and the "TCP/IP Protocol" should be listed.

These components are already available on many machines; if not, you have to install them as follows: Select 'Add' and double-click 'Client'. In the ensuing dialog, select `Microsoft` and "Client for Microsoft Networks" and confirm your entries with 'OK'. "TCP/IP" is listed in 'Protocol' under the vendor `Microsoft`.

Usually, a Windows CD is required for this procedure. Following the installation, the system normally has to be rebooted. Other settings are not required, as these will automatically be retrieved from the server via DHCP. Following the configuration of the identification data, Windows must be rebooted.

If Windows cannot get these data automatically due to special system settings, make sure that the IP number of the server is entered for the WINS server, DNS server, and gateway. By default, `192.168.0.1` is proposed.

Test the settings by right-clicking the 'Network Neighborhood' icon and selecting the item 'Properties'. The following settings should be displayed:

IP Address 'Obtain an IP address automatically'
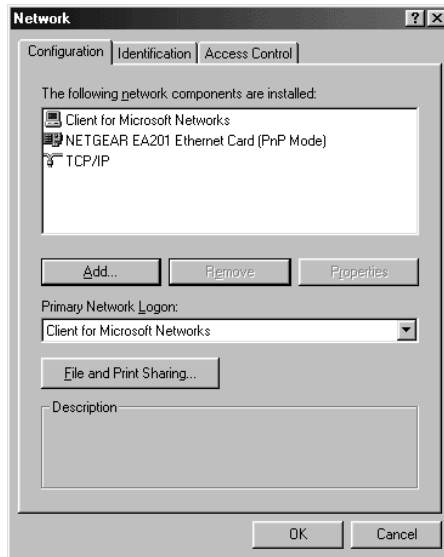
Figure 5.2: Network Configuration in Windows 9x/ME

WINS Configuration 'Use DHCP for WINS Resolution'

Gateway Empty

DNS Configuration 'Disable DNS'

After the client is rebooted, the installed protocols and services should be available. If you want to gain access to a private user directory, you have to specify some additional settings.

Domain Logon

In the Control Panel, double-click 'Network'. Make sure that the "Primary Network Logon" is set to "Client for Microsoft Networks". Then select the 'Identification' tab for some more settings. The computer name and description can be selected freely. However, the computer name should consist of no more than 15 characters and may not contain any blanks.

If the server is configured as PDC, you have to switch from 'Share-level access control' to 'User-level access control' under the 'Access Control' tab and enter the domain name specified during the installation in 'Obtain list of users and groups from'.

For your Windows client to operate correctly, it needs an NT domain. In Windows, enter the NT domain specified by the Samba configuration in 'Client for Microsoft Networks' → 'Properties' → 'Windows NT Domain'. Activate the check box 'Log on to Windows NT Domain'. If the server was configured as Primary Domain Controller, the entire user management will take place on this server. In this case, the Windows clients will be able to see all created users.

If you run an early version of Windows 95 that does not yet support the transmission of encrypted passwords to Samba, download an update from `ftp: //ftp.microsoft.com/softlib/mslfiles/vrdrupd.exe` and install it in order to enable the authentication with encrypted passwords.

Microsoft Windows NT 4

Right-click the 'Network Neighborhood' icon on the desktop. If this icon does not exist, open the Control Panel with 'Start' → 'Settings' → 'Control Panel' and double-click the 'Network' icon.

Select the 'Identification' tab and click 'Change...'. Under 'Member of', select 'Domain' and enter the name of the Microsoft Windows domain operated by SUSE LINUX School Server.

Activate the check box 'Create a Computer Account in the Domain' and enter the user name `Administrator` and the password of the SUSE LINUX School Server administrator. Click 'OK' to apply the changes.

Windows 2000

On your desktop, right-click 'My Computer' and select 'System Properties'. Activate the 'Network Identification' tab and click '' (see Figure 5.3).
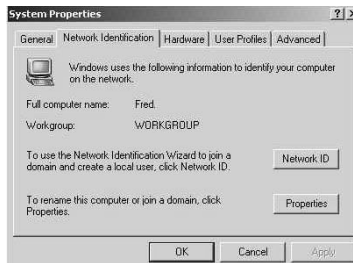
Figure 5.3: Network Properties in Windows 2000

In the new window, activate 'Domain' under 'Member of' and enter the name of your Windows domain in uppercase letters in the input field (see Figure 5.4).

Figure 5.4: Changing the Domain Name in Windows 2000

Click 'OK'. You will be prompted to enter a user who is authorized to add an account to your domain. Enter `Administrator` and the password that you specified for the administrator `admin` during the installation. Following a reboot, you should be able to log in as one of the users created on the server.

Windows XP

In Windows XP, you have to be logged in as the administrator or a user of the "Administrators" group in order to be able to perform changes in the network configuration. For the first login, you need the root account and the root password of the server. To connect an XP client with the server, proceed as follows.

Before you proceed, make sure there are no open connections between the Windows XP client and the server. If necessary, open a command line and enter the command `net use * /delete` in order to delete all open network connections.

Open the 'Start' menu and right-click 'My Computer'. Select 'System Properties' (see Figure 5.5 on the following page).

In the next window, activate the 'Computer Name' tab and click 'Change...'.

In the new window, activate 'Domain' under 'Member of' and enter the name of your Windows domain (see Figure 5.6 on the next page).

Figure 5.5: *Windows XP Start Menu*

Figure 5.6: *Changing the Domain Name in Windows XP*

Click 'OK'. You will be prompted to enter a user who is authorized to add an account to your domain. Enter `Administrator` and the password that you used for the administrator `admin` during the installation. Following a reboot, you should be able to log in as one of the users created on the server.

Server-based Profiles with Windows Clients

In contrast to Linux clients, which simply mount the respective home directory of a user and place all relevant data in this home directory (which can be made available network-wide), Windows clients require some more effort in order to enjoy the same comfort.

This chapter covers the configuration of server-based profiles for Windows clients. Profiles contain all relevant settings of a Windows environment.

Remember that there are many ways of achieving the same goal and this is not a Windows manual. Therefore, do not expect a perfect guideline for administering Windows-based hosts. If you encounter difficulties with the configuration, contact your Windows vendor.

A combination of various Windows clients in one network is very difficult to administer. Therefore, the following instructions presume that you use identical versions in your network.

Server-based Profiles with Microsoft Windows 9x/ME

Originally, the older Windows versions were not designed for deployment in networks. Therefore, the configuration is a bit more complicated than in later versions.

Remember that these older versions do not have any effective protective mechanisms. Therefore, we recommend the use of "safety cards" which reset the hosts to a defined state every time they are rebooted.

Requirements

In order to be able to use server-based profiles, the clients have to log on to the server. In this connection, refer to 5 on page 104.

Activating User Profiles

In order to be able to use user profiles in Windows 9x/ME, these have to be activated.

In Windows 95, do this by selecting 'Start' → 'Settings' → 'Control Panel' → 'Passwords' and activating 'User profiles'.
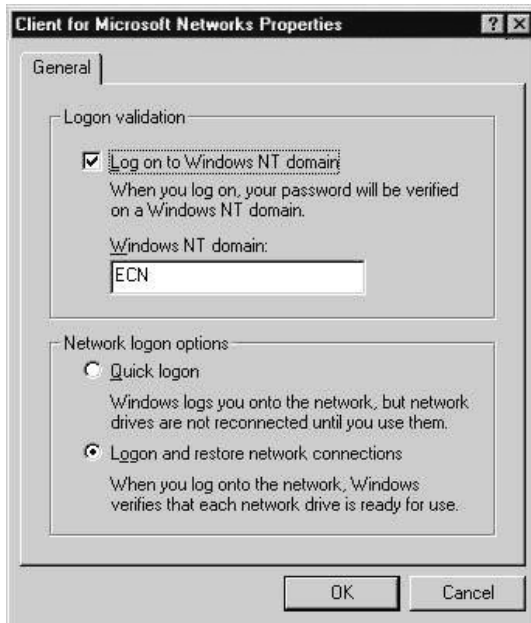
Figure 5.7: *Activating the Server Logon*

Two options are available at the top. Select "Users can customize their preferences and desktop settings ..." (see Figure 5.8 on the next page). Then exit the menu and reboot the machine.

In Windows 98 and Windows ME, select 'Start' → 'Settings' → 'Control Panel' → 'Users'. A wizard will guide you through the individual steps. Then reboot the machine.

Mandatory Profiles

After you activate the user profiles, Windows will save the user-specific settings in the file "user.dat" in the profile directory of the user. (The system-specific data are saved in the file system.dat and, in Windows ME, in the file classes.dat.)

┌─ **Note** ───

Every user can be assigned a mandatory profile by renaming the file user.dat to user.man.

─── **Note** ─┘
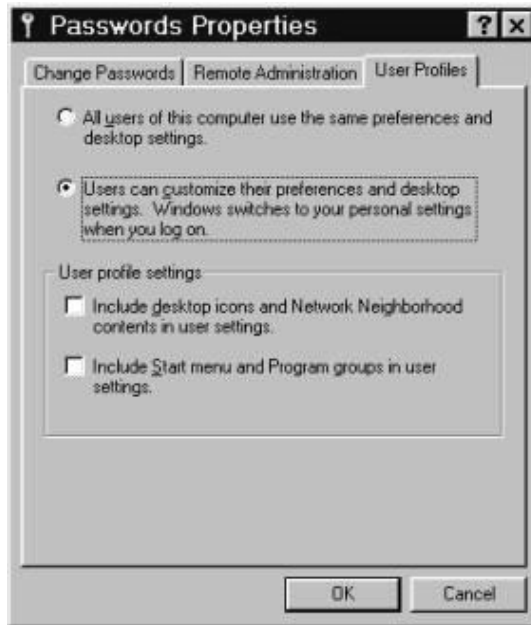
Figure 5.8: Activating User Profiles

In this way, the user profile is protected from being overwritten when the user logs out. This mandatory profile will be loaded next time the user logs in.

Accordingly, create a sample user with all needed settings, distribute this profile to all other users, and make it mandatory by renaming it to `user.man`.

This should be sufficient for smaller networks. However, if you want more comfort or have a large number of users and machines with different permissions and installed software, use system and group policies.

Poledit

Almost all important information of the Windows operating system is saved in the registry. The registry is the central location for saving and querying settings of a Windows computer and its components.

Note

As the administrator, you have to edit the registry directly. Proceed with caution, as you can endanger the system by entering incorrect values or delete or modify needed values.

Note

The application Poledit is a convenient tool for editing the registry and performing other tasks such as moving part of the registry to the directory Netlogon on the server in server-based networks, from where it is downloaded to the local host when a user logs in. In this way, the administrator will be able to do everything on a Windows workstation, but a normal user will not. Furthermore, the data of the users can be stored on the server and do not need to be made available on the local host.

The system policy editor Poledit.exe is available on your Windows CD (in the directory admin/apptool/poledit in Windows 95 or in the directory \tools\reskit\netadmin\poledit in Windows 98). The latest version for your operating system can also be downloaded from the Internet.

Tip

A special template file for Poledit adapted to the needs of schools is available under ftp://ftp.suse.com/pub/people/lrupp/ schoolserver/win/ (with the name of the respective operating system).

Tip
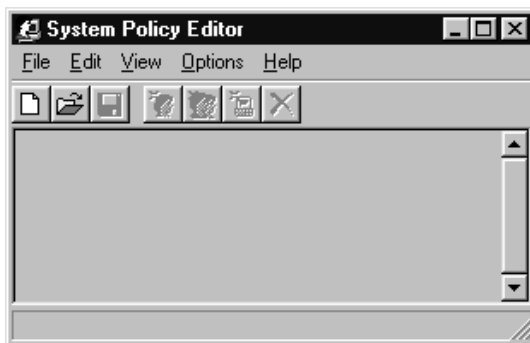
Figure 5.9: Poledit

> **Caution**
>
> Due to its capabilities, Poledit.exe should only be available to the system administrator.
>
> **Caution**

The application (including all files in the folder) can be installed in the home directory of the admin. To do this, copy the respective directory (usually `C:\\ProgramFiles\Ork\Poledit`) containing the application to this location.

Poledit.exe can be used on three levels:

Editing the local registry   'File' → 'Open Registry' – This option enables editing the registry of the local host.

Editing and modifying the policy file   'File' → 'New' or 'File' → 'Open' – This item is covered in the following paragraphs.

Remote access   In case remote access is enabled on the respective client, the registry can be edited from a remote host.

The First Start-up

Start Poledit (if you are prompted to specify a template file, use the proposed file `admin.adm` or use a downloaded template file).

At first, the window is empty. Select 'File' → 'New'. Two new icons will appear in the dialog.

Figure 5.10: Creating a New Policy File

One icon represents the default user, and the other the default machine. Every user for whom no separate icon is available here is considered a default user.

System Guidelines for the Administrator

Use the menu item 'Edit' → 'Add User' to add the user `admin`.

Assign this user all permissions in the system by double-clicking its icon and deactivating all check boxes in the new window.

Explanation:

- If the check box is blank, the respective function is not active.

- If the check box has a check mark, the function or restriction is active.

- If the check box is gray, the local setting is retained. This setting is not recommended, as a normal user would have extended permissions if the user who logged in to the machine before him had more permissions.

Save your settings by clicking (OK).

If you create additional users in Poledit, these will first be assigned all settings of the default user. To configure a second administrator user, simply copy the profile by clicking the icon and selecting 'Edit' → 'Copy'. Then select the new user and assign him the new permissions with 'Edit' → 'Paste'.

Figure 5.11: Creating a New User

System Policies for the Default User

Suitable restrictions should be imposed for the default user.

Of course, the restrictions depend on your specific needs. Here are some proposals that you can adapt to your circumstances:

Control Panel Activate all restrictions.

Desktop If, for example, "none" is set as wallpaper, no wallpaper will be loaded, since this file does not exist. If the user generates a wallpaper image with the option 'Save as Wallpaper' in an application, it will not be displayed at the next login.

Network Activate all restrictions.

Shell Adapt the restrictions for 'Custom Folders'. More details are provided below.

System Prohibit all applications for editing the registry. If necessary, block the MS-DOS prompt. However, if you do this, some MS-DOS programs will not work.

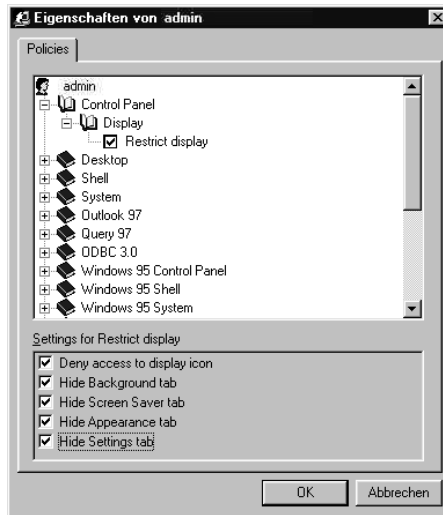If you want to save the data of the users on the server, some adaptions must be made in 'Shell' → 'Custom Folders'.

Figure 5.12: Setting Administrator Permissions

┌ Caution ───────────────────────────────

To avoid a system crash, create the respective subdirectories before you specify them in Poledit.

─────────────────────────────── Caution ┘

For example, you can store the start menu and the desktop icons on a server drive to which only teachers have write access. In this way, the students cannot change anything, and the desktop and the start menu will always look the same on all hosts.

Or you can place the paths for these folders into the home directory in order to enable all users to configure their desktop environments as they wish – which is often very motivating for students.

The paths for the folder `My Documents` should point to the home directory of the user. It would be practical to specify the entire path (`\\<server>\<homes>\profile\My Documents`). However, as this is not accepted by all programs, you should use a subdirectory in the drive `H:`.

Following the login, the server will create additional drives for server-based software (`S:`), group directories (`M:`), and for the exchange among each other (`P:`).
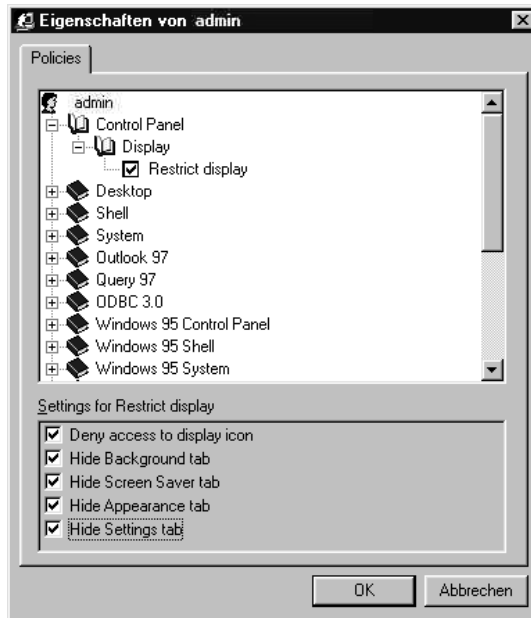
Figure 5.13: Setting User Permissions

Thus, the storage locations of the custom folders can be defined freely. However, make sure that the respective folders really exist and that they may have to contain the respective data!

System Policies for the Default Computer

With this option, you can add a specific computer and define it as a special teacher workstation. The NetBIOS name of the host is used as the basis for the definition.

For example, you can specify the hosts in another, smaller room and assign them different settings than the rest.

If you use several computer rooms, use a different procedure that enables you to entrust the rooms to other administrators. Simply use policy files with different names for the various rooms and specify them once for every host.

Subsequently, administrators of rooms merely need to take care of the `default computer`.

Some example settings:
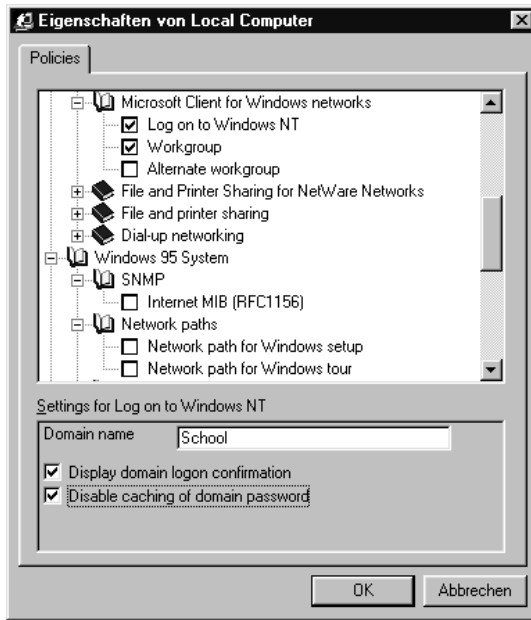
Figure 5.14: Configuring a Default Computer

Access control Deactivate this option in order to disable shares. This should be done for examination environments.

Logon If you want the users to be sent a message following the logon, activate 'Logon banner' and enter the respective message in the window below.

If you activate 'Require validation from network for Windows access', only users who log on to the server will be granted access; clicking 'Cancel' during the logon will no longer be possible. This also applies if the client cannot establish a network connection to the server.

To use the client as a stand-alone PC, create and assign a local policy file such as config.pol.

⌐ Caution ────────────────────────────────────

The option 'Remote update' under 'Network' is very important: the policy will only be interpreted by the server if this option is activated.

──────────────────────────────────── **Caution** ⌐

The default settings in the lower part can be left as they are or adapted in case you want to use several policy files.

Under 'Path for manual update:', enter the IP number of the server and the path `netlogon` together with the full file name (watch lowercase and uppercase spelling). Example:

```
\\192.168.0.2\netlogon\room1.pol
```

Exit the window with (OK), save the policy file, and move it to the directory

```
/var/lib/samba/netlogon
```

on the server. Enter

```
chmod 644/var/lib/samba/netlogon/room1.pol
```

to set the correct permissions for the file.

Activating System Policies

After you finish these preliminary steps and save the policy file on the server, configure the clients to get their settings from the server.

To do this, run the following file (available on our FTP server in the directory `ftp://ftp.suse.com/pub/people/lrupp/schoolserver/win/` `<version>` under the name `remote_update_aktivieren.reg`), thereby entering it in the registry.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Update]
"NetworkPath"=""
"UpdateMode"=dword:00000001
"Verbose"=dword:00000001
"LoadBalance"=dword:00000001
```

File 6: The file remote_update_aktivieren.reg

If you assigned a file name other than the default value (for Windows 9x: `config.pol`; for Windows NT, 2000, and XP: `ntconfig.pol`), set the correct path to the file after `NetworkPath`.

Server-based Profiles with Microsoft Windows 2000 and XP

In contrast to Windows 9x and ME, the professional versions of Windows 2000 and Windows XP as well as Windows NT support multiuser operation by default.

> **Note**
>
> The Home Edition of Microsoft Windows XP is not suitable for network operation. The workstation cannot be integrated in the domain.
>
> Though a default user for domain operation can be defined with the tool *TweakUI* (can be downloaded from the Internet), real multiuser operation is not possible.
>
> **Note**

Basic Information on the Use of Profiles

In Windows 2000 and Windows XP, every user has a separate profile. All data and settings concerning this user are stored there. On a workstation, the default location for these profiles is `C:\DocumentsandSettings\<username>`.

Stand-alone Operation

If a user does not yet exist on a client, and if the client is not yet integrated in a domain, a profile will be generated at the first successful login of the user.

For this purpose, the "Default User" profile will be used as a template. Subsequently, the access permissions will be changed for the newly created profile.

> **Note**
>
> As the access permissions vary, profiles cannot simply be copied for other users. This has to be done in 'My Computer' → 'Properties' → 'User Profiles'.
>
> **Note**

There is another profile called `All Users`. The general settings that apply to all users are stored in this profile. When the administrator installs an application that is to be made available to all users on this workstation, the respective links are created in this profile.

Network Operation

If the client is integrated in a domain, the login procedure for a new user is
somewhat different than on a stand-alone system, unless the administrator
changes the configuration:

- First, the client checks if the share `netlogon` (located on the server un-
  der `/var/lib/samba/netlogon`) contains a directory `Default User`
  which it can use as template.

- If such a directory exists, the client creates the personal user directory on
  the local host and copies the `Default User` profile from the network
  there.

- If this directory does not exist on the server, the local `Default User` pro-
  file is used as template.

Following the logout, the local user profile is copied to the server. The next time
the user logs in to the client, the local profile is synchronized with the profile on
the server and any old files are replaced by new files.

Policies or Group Policies?

Microsoft provides administrators with two different mechanisms for adminis-
tering network clients:

Policy editor Poledit can be used to set user-specific permissions in the net-
work. However, this is very time-consuming if there are many different
profiles and computers.

Group policies Group policies can be used to configure an individual computer in the network. The settings made here apply to *all* users of this computer. If incorrect settings are made, even the administrator himself can be hindered from performing administrative operations on a machine.

Note

Choose one of the two systems for administering your clients. Mixed operation is possible, but this may render the administration of the overall system more complicated.

Note

By default, the group policy editor is installed on all Windows versions starting from Windows 2000. It can be started by entering the command `gpedit.msc` on a command line (or with 'Start' → 'Run' → 'gpedit.msc'). Poledit still needs to be installed.

Despite the disadvantages mentioned above, we recommend using Poledit, as it enables the comfortable remote administration of all computers, the definition of custom policies for every user, and concurrent loading and combining of multiple template files.

Refer to 5 on page 112 for information on the installation and use of Poledit.

Autoinstallation and Network Booting

During the installation of SUSE LINUX School Server, an installation server is configured for the installation of the latest version of SuSE Linux. Moreover, a TFTP server is configured in order to enable network booting with the PXE protocol. Using these two tools, you can install SuSE Linux automatically or manually.

Schools often receive donations of free hardware from companies, or the school itself may have old unused hardware.

By offering a terminal server/ThinClient solution, SUSE LINUX School Server enables you to utilize this old hardware in a meaningful way in your school.

Preparation for the Installation

The root directory of the TFTP server is `/srv/tftpboot`. A number of files must be copied to this directory from CD 1 or the DVD of the latest SuSE Linux distribution. The following instructions assume that a DVD is mounted in the file system under `/media/dvd`:

linux The Linux kernel to load; must be copied from the latest SuSE Linux DVD:
> `cp /media/dvd/boot/loader/linux /srv/tftpboot`

initrd The file system to start; must be copied from the latest SuSE Linux DVD:
> `cp /media/dvd/boot/loader/initrd /srv/tftpboot`

menu.lst This file contains the boot menu.

pxegrub PXE boot image for the boot loader GRUB.

pxes This directory contains special kernel images and file system images for starting Linux X terminals.

Furthermore, the CDs or DVD of the latest SuSE Linux distribution have to be copied to the directory `/var/SuSE/akt/` with the following commands (assuming you are using the DVD):
```
mount /media/dvd
cd /media/dvd
cp -va .  /var/SuSE/akt
umount /media/dvd
```
If necessary, repeat these commands for all CDs or DVDs.

Tip

Using the DVD Directly

The DVD of the latest SuSE Linux distribution can also be mounted directly under `/var/SuSE/akt/` (`mount /dev/dvd/ /var/SuSE/akt/`). In this case, remove the comment mark "#" preceding the entry `/var/SuSE/akt/` in the file `/etc/exports` and update the NFS server with the command `rcnfsserver reload`. However, for performance reasons this procedure is only suitable for test purposes.

Tip

If you boot a host from the network using PXE, a boot menu with the following options will be displayed:

(xterm) Linux X Terminal   Starts a diskless Linux X terminal. The Terminalserver is used as X server.

(linux1)SuSE Workstation autoinstallation   Starts the automatic installation of a SuSE Linux workstation.

(linux2) SuSE Workstation autoinstallation with Windows partitions   Starts the automatic installation of a SuSE Linux workstation with two additional Windows partitions.

(manual) Manual installation   Starts the manual installation of a SuSE Linux workstation.

(thin) SuSE ThinClient autoinstallation   Starts the automatic installation of a SuSE Linux ThinClient.

(term) SuSE Terminal server autoinstallation   Starts the manual installation of a SuSE Linux terminal server.

The configuration files std+win.xml, std.xml, thin_client.xml, and terminalserver.xml for the autoinstallation are located in the directory /var/SuSE. If necessary, these files can be edited with an XML editor or with the YaST module autoyast on an existing client. Additional information about AutoYaST is available in the directory docu on the SUSE LINUX School Server installation CD . The settings for the automatic installation are as follows:.

⌐ Caution ─────────────────────────────────

Remember that *all* automatic installation modes delete the previous data and partitions on the hard disks of the clients.

Moreover, the administrator password entered during the installation for the user root is set on all systems, and a password-free SSH connection is configured for the user root of the server.

───────────────────────────────── Caution ⌐

The Configuration Files std+win.xml and std.xml

These configuration files control the automatic installation of a workstation. As the file names imply, std+win.xml is used for installing a workstation with additional Windows partitions; std.xml is used for preparing the entire hard disk for a Linux installation.

Partitioning   The entire hard disk space is utilized and partitioned as follows: For a client with std+win.xml:

	std+win.xml	
Mount point	Size	File system type
/boot	30 MB	Linux
swap	Determined automatically	Linux swap
	4 GB	Win95 FAT32
	4 GB	Win95 FAT32
/	4 GB	Linux

For a client with std.xml:

	std.xml	
Mount point	Size	File system type
/boot	30 MB	Linux
swap	Determined automatically	Linux swap
/	Rest of the hard disk	Linux

The boot manager is written to the MBR. The two `Win95 FAT32` partitions can later be used for installing Windows. Depending on the Windows version, you may need to reinstall the boot manager after the installation. Look for the keyword "Windows" in our Support Database at `http://portal.suse.com/PM/page/search.pm?`.

Package selection Selected package groups:

- default
- Kde
- Kde-Desktop
- Office

Network The first network card is configured as DHCP client.

NFS client `nfs:/home` is mounted under `/home` with the default options.

LDAP client The server is integrated in the LDAP authentication.

Printing CUPS is installed as printer daemon; the CUPS server is the host `printserver`.

X If possible, 3-D hardware is activated; the resolution is 1024 x 768 @ 75 Hz.

The Configuration File thin_client.xml

This configuration file handles the configuration of a server for ThinClients.

Hardware requirements   Older clients with a 2 MB graphics card, about 32 MB RAM, a bootable network card with PXE ROM or a CD-ROM drive and a hard disk with more than 600 MB. To reduce the network load generated by exclusive terminal operation (see annex [1]), a swap partition and a small operating system for starting an X server are configured on the hard disk.

Partitioning   The entire hard disk space is utilized and partitioned as follows:

Mount point	Size	File system type
swap	Determined automatically	Linux swap
/	Rest of the hard disk	Linux

The boot manager is written to the MBR.

Package selection   Basic selection: minimum + X11
Additional packages:

- xdmsc
- nfsserver
- mozilla

Network   The first network card is configured as DHCP client.

X   If possible, 3-D hardware is activated; the resolution is 1024 x 768 @ 75 Hz.

sysconfig xdmsc   By default, the DNS name `terminalserver` is used as terminal server.

Note

The ThinClients should also be registered. However, the registration tool cannot detect the hardware address (MAC address) of the ThinClients, as the actual operation takes place on the terminal server. Therefore, the hardware address has to be entered manually. You can determine the hardware address by changing to the ThinClient console with (Alt)–(Ctrl)–(F1), logging in as `root`, and entering the command `ip link show eth0`.

Note

---

[1]The annex is available in the online manual at `http://admin/manual/manualEN.pdf`

The Configuration File terminalserver.xml

The file serves the configuration of a terminal server.

Hardware requirements   This should be a modern machine with sufficient RAM (about 64 MB for each client and 128 MB for the server system).

Partitioning   The entire hard disk space is utilized and partitioned as follows:

Mount point	Size	File system type
/boot	30 MB	Linux
swap	Determined automatically	Linux swap
/	Rest of the hard disk	Linux

The boot manager is written to the MBR.

Package selection   Selected package groups:

- default
- Basis-Devel
- Basis-Sound
- Kde-Desktop
- Kde-Devel
- Kde
- LAMP
- Network
- Office
- SuSE-Documentation
- Tcl-Development
- X11

Additional packages:

- a2ps
- cvs
- emacs
- emacs-x11
- gv

- html2txt
- mozilla
- mutt
- phpMyAdmin

Network   The first network card is configured as DHCP client. Following the installation, register the terminal server with SUSE LINUX School Server as a client as described under 4 on page 77. Make a note of the IP address, as you will need it.

Additionally, enter the name `terminalserver` in the DNS server, as the autoinstalled ThinClients will contact the `terminalserver`. For this purpose, enter the new IP address (received during the registration) under the menu item 'DNS: Add Host' as described under 4 on page 82 [2].

NFS client   `nfs:/home` is mounted under `/home` with the default options.

LDAP client   The server is integrated in the LDAP authentication.

Printing   CUPS is installed as printer daemon; the CUPS server is the host `printserver`.

X   If possible, 3-D hardware is activated; the resolution is 1024 x 768 @ 75 Hz.

Tip

Multiple Terminal Servers

Several terminal servers (for instance, one terminal server for each classroom) can be installed. To do this, proceed as follows for every terminal server:

- Install and register a terminal server, but do not enter its IP address as `terminalserver` in the DNS.
- In the autoinstallation configuration file of the ThinClients `/var/SuSE/thin_client.xml`, Replace `terminalserver` with the name of the registered terminal server.
- Now you can install and register the desired number of ThinClients. Newly installed ThinClients will contact the terminal server you last installed.

Tip

---

[2] The new entry is not included automatically in the configuration files. To write the configuration files, select 'DNS Configuration' → 'Export'.

Network Installation

If you have network cards with PXE ROM, all you need to do is boot the hosts by means of the network card.

If you want to install a SuSE Linux client by way of SUSE LINUX School Server or check if older hardware is suitable for installation as ThinClient or diskless client, you can create a bootable CD that automatically establishes a connection to the server after booting and displays the selection menu. The ISO image is located at `http://admin/bootcd.iso`.

Groupware

Apart from the administration interface, SUSE LINUX School Server includes a groupware component that features mail and calendar functionalities and enables access to the central address book and student and teacher forums, thus providing the basis for efficient teamwork. The following chapter explains how you can use the groupware component of SUSE LINUX School Server as effectively as possible.

Overview of the Groupware Interface

To access the groupware function, click the icon 'Web Mail, Groupware, Forum' in the SUSE LINUX School Server menu or enter the URL `https://SchoolServer` ("https" stands for the encrypted connection) in a browser on a host in the school network.

> **Tip**
>
> **External Login**
>
> From outside the school network, you may be able to access the groupware interface by means of an encrypted connection (port 443). For example, if your school is registered under www.school.com, enter the following address in the browser: `https://www.school.com`
>
> **Tip**

Log in to the server with your user data. The SUSE LINUX School Server groupware interface (see 7.1 on the next page) will be displayed with your personal calendar.

The groupware interface features the following menu items for students:

- Home
- EMail
- Calendar
- Addressbook
- Forum

These items can be accessed by clicking the respective icon. Additionally, teachers have access to a 'tforum' (Teacher Forum) and an 'Administration' menu. The following sections describe the individual components of the groupware interface in detail.

The Calendar

View Modes

By default, the calendar displays the current month (large, at the center), the past month, and the coming month (small, to the left and right). Under the calendar, there is a button for the search function and three pull-down menus with the following functions:

Figure 7.1: *The Calendar View of the SUSE LINUX School Server User Interface*

Category: This pull-down menu enables you to allocate events and appoint-
ments in the calendar to specific categories. By default, no categories are
available; therefore, the menu only contains the item 'All'. If you select a
category, the calendar will only display the appointments associated with
the respective category. Section 7 on page 138 shows how categories can
be created and edited.

Filter: Appointments and events can be either private or public. Here you can
determine whether to display all appointments and events or only the
private ones.

User: Here you can choose whether you want to view only your own calen-
dar or the class calendar too (the calendars of the other students or teach-
ers). If an appointment is not marked as private, appointments of students
will apply to the entire class and appointments of teachers will apply to
the entire body of teachers. This means that teachers have read access to
the calendars of the other teachers and the calendars of their own classes.
Similarly, students have read access to the calendars of all fellow students.
These settings can be modified under 'settings' → 'Calendar Preferences'
'Preselected Group for entering the planner'. For confidential appoint-
ments and events, select the check box 'Private only'.

The calendar view (day, month, etc.) can be toggled with the six little icons at
the top left. The following views are available (from left to right):

- Today → Shows only the current day. Useful if several appointments are
  due on one day and for creating a new appointment at a specific time.

- This week → Shows the current week or a selected week. Apart from the
  week, the three months preceding, during, and following the respective
  week are also displayed.

- This month → The default view of the calendar.

- This year → Overview of all twelve months.

- Planner → Here you can view several weeks on a timeline. For example,
  if you select 'User:' → 'Students', you can check the appointments of the
  individual students for any conflicts.

- Daily Matrix View → The view described under 'Planner' can also be set
  for a specific day. To do this, click this icon.

If you get lost in a maze of events and appointments, use the search function at
the top right of the calendar. Enter the keyword you are looking for in the input
field and click 'Search'.

Creating and Managing Calendar Entries

As a general rule, you can only create calendar entries in your own calendar,
unless someone explicitly gives you write access to this calendar. Therefore,
select your own entry under 'User:' before you try to make an appointment.

The creation of new entries takes place by means of a uniform dialog. Depend-
ing on the view mode, various steps are required to access the input dialog.
From the *week* view and the default *month* view, click the plus symbol next to
the calendar day in order to access the input dialog for a new appointment. This
procedure is mainly suitable for full-day events, as the event is not associated
with a specific time. However, the time can be specified later on.

From the *day* view, simply click a time at the end of the shaded field to access the input dialog for the new appointment. In the dialog, the time you selected is entered as the 'Start Time' and 'End Time'. If no dialog is opened, check if the color of the time entry changes to orange when you move the mouse pointer over it. If this does not happen, you most likely do not have write access to the calendar. In this case, select a different user from the pull-down menu 'User:'.

The procedure is the same for the *month* view. However, you first have to select the respective day in order to access the *day* view.

New appointments can also be created from the *Planner-* and *Matrix* views. From the *Planner* view, click the respective day to access the input dialog. From the *Matrix* view, click the respective time.

Adding a calendar entry

If everthing was done correctly, the dialog 'Add Calendar Entry' should be displayed (see 7.2 on the next page). Enter the 'Title' and a 'Full Description' for the event. Select an item from 'Category:' (read the following section for more information). 'Location' can be a conference room or a detailed address. When the appointment is created, the 'Start Date' and the 'End Date' are automatically set to the selected day. Depending on how you created the appointment, the 'Start Time' and 'End Time' entries are either empty (i.e., 0000 hours) or set to a specific time.

The check box 'Private' allows you to mark the appointment as private or make it readable for others. Private appointments can be queried by other users; however, others will merely be able to see that you have a private appointment on the respective day. This prevents others from making an appointment with you on a day on which you already planned a private appointment.

Under 'Participants', you can invite others for an appointment and notify them accordingly. You can select individual students or teachers (u=users) or groups and classes (g=group). To add several entries, keep Ctrl pressed while you click the individual entries with the mouse. All selected participants will be notified about the appointment by e-mail and will see the appointment entry in their own calendars. By default, you will automatically be invited for all appointments you create. If you do not want to be invited automatically (perhaps you work in the secretariat and frequently have to plan appointments for the school administration), click the check box '<login> Last name, First name participates:' once to remove the selection.

In the lower part of the input dialog, you can specify 'Repeating Event Information' such as extracurricular lessons or holidays. Select the frequency of the event under 'Repeat Type' and use the check boxes to specify the days on which

Figure 7.2: The Calendar View of the SUSE LINUX School Server User Interface

the event will be repeated (for weekly events) and until when ('Repeat End Date').

Click 'Submit' to create the appointment. To delete an existing appointment, click 'Delete Single' or 'Delete Series'. If you decide not to create the appointment, click 'Cancel'. The system will save the entry in your calendar (and the other selected calendars) and send an e-mail to all participants (see 7 on page 146).

Categories

In order to avoid getting lost in a full calendar, the individual appointments can be allocated to various categories. To create a new category, select 'Settings' at the top (next to 'Log out'). Then select 'Calendar' → 'Edit Categories'. Teachers can also select the item 'Administration' → 'Global Categories'.
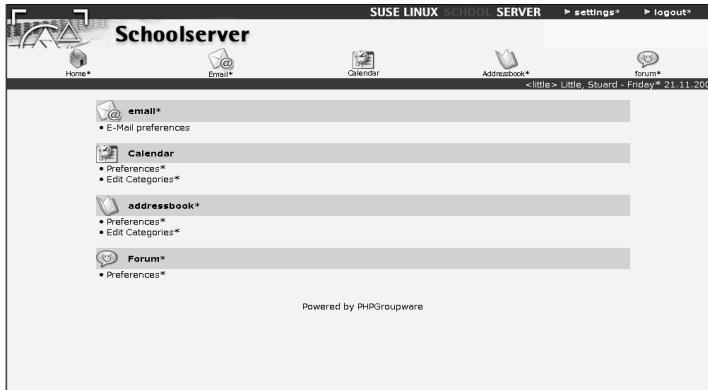
Figure 7.3: Settings for Students

Select the respective item and click 'Add' to create a new category. Previously
created categories will be listed. Click 'Add subcategory' to create a new subcat-
egory. After you click 'Add', select the respective category from the pull-down
menu 'Category' (see Figure 7.4 on the next page). Designate a suitable name
for the category and a precise description which will facilitate the use of the cat-
egory. If you do not want the category to be visible for others, mark the check
box 'Private' (when creating new appointments, you still have to mark the check
box 'Private' in order to make sure that the appointment remains private).

Click 'Save' to create the category. The message *Category XY was saved!* will be
displayed. If you wish, you can create additional categories. When you are fin-
ished, click 'Done' (do not forget to save the settings before you click this but-
ton). The newly created categories will be displayed and can be used in the cal-
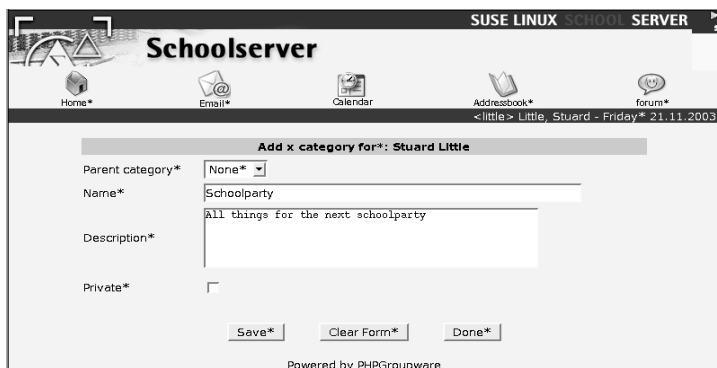endar when creating new appointments.

Figure 7.4: Creating a New Calendar Category

E-Mail

Overview of the E-Mail Component

The SUSE LINUX School Server web mail client can be accessed by means of the e-mail icon. For security reasons, the program can only be accessed from inside the school network. To access your mail account from your home, use an e-mail client such as KMail, Evolution, or Outlook.

By default, the SUSE LINUX School Server mail client displays the existing folders and the number of new and read messages in the individual folders. Click the 'Folder' icon to return to the folder view. To create a new message, click 'Compose'.

Composing E-Mail Messages

Click 'Compose' to access the input dialog for composing a new message (see Figure 7.6 on the facing page). First, specify a recipient under 'To:'. This can be done manually or by means of the address book icon (see following section). You can also send a message as a 'Copy (cc)' or 'Blind Copy (bcc)'. If you send a 'cc', the recipient will be able to see who else received the message. If sent as a 'bcc' the other recipients will not be visible. Specify the subject or purpose of the e-mail message under 'subject'. Be sure to fill in this field, as the subject line helps to organize messages.

If you want to be notified when the recipient receives the message, mark the check box 'Notify on delivery'. (this function is not supported by all mail pro-

Figure 7.5: *The SUSE LINUX School Server Mail Program*

grams). To append files to your message, click 'Attach file' → 'Search...'. Select a file and click 'Attach File' to move the file to the server. Depending on the browser you use, a message may be displayed, indicating that the files are moved from your machine to another machine. As SUSE LINUX School Server makes use of the `https` protocol, this procedure is secure. Proceed in the same way to attach any further files. Before you close the dialog with 'Done', mark the check box of every file you want to append.

Use the large text field at the bottom to compose the message text. When the message is ready, click 'Send'. SUSE LINUX School Server will transmit your e-mail to the respective recipient(s).

Caution ⌐

By default, e-mail can only be sent to internal addresses.

Caution ⌐

Using the Address Book

Nobody can memorize 1,000 e-mail addresses. For this reason, SUSE LINUX School Server has a central address book that contains all e-mail addresses. By default, all teachers and students have read access to the central address book. To view the individual entries, click the main menu item 'Address Book' in the web interface. The address book overview will be displayed (see Figure 7.7).

Use the arrow keys to browse the address book or employ the search function in order to search for a specific entry. To do this, type the search string in the
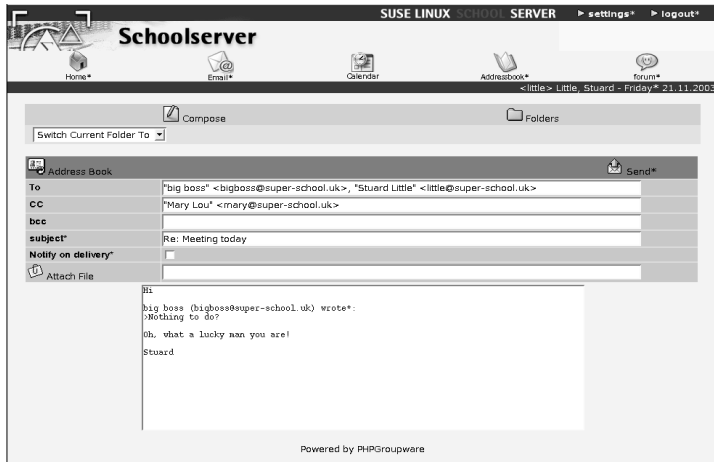
Figure 7.6: Composing E-Mail Messages

input field and click 'Search'. To limit the search to specific categories, use the pull-down list 'Select Category'. For example, to view all student entries of the class 5B, select the (preset) category 'Pupils', type 5B in the input field (case-sensitive), and click 'Search'.

To add a new entry to your address book, click 'Add'. An extensive dialog consisting of the sections personal, business, and private (home) will be displayed. The fields 'Last Name' and 'First Name' are mandatory, all other fields are optional. To facilitate the search for the entry, fill in the items 'Private' and 'Category'. Then click 'OK'. An overview will be displayed, enabling you to edit or
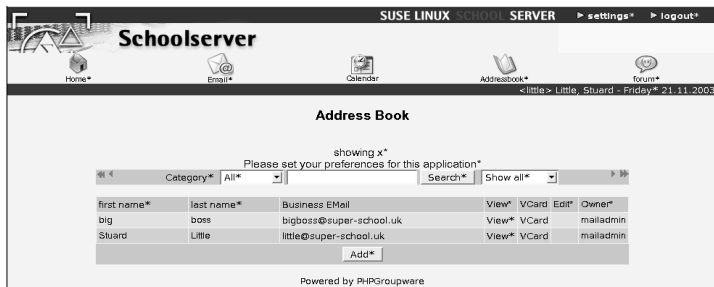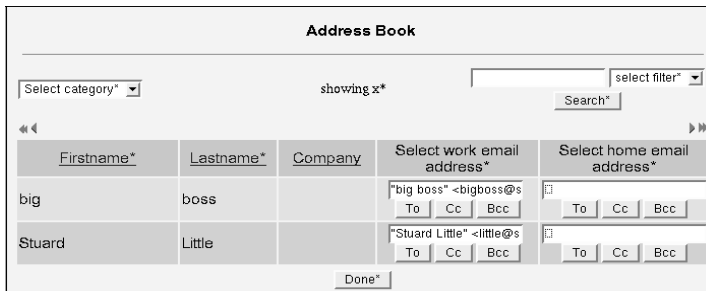

Figure 7.7: Address Book Overview

copy the entry or export it as VCard. Click 'Done' to finish the entry and return to the address book view.

Selecting Existing Entries in the Mail Component

To access address book entries, click 'Address Book' when you compose a message. The dialog shown in Figure 7.8 on the facing page will be displayed.

Figure 7.8: Inserting Addresses from the Address Book

Depending on the setting, you will see 10-20 entries. For more than 20 entries, use the green arrow keys at the top right and top left for navigating. To add an address, click the 'To', 'Cc', or 'Bcc' buttons under the entries:

To: The recipient of the message. In contrast to conventional letters, an e-mail message can be sent to multiple recipients at the same time. To do this, simply click the 'To' button associated with the individual entries.

Cc: The individuals selected with this button will receive the message in the form of a copy. For example, you may want to send parents a copy of a message from students.

Bcc: The addresses selected with the button receive a blind copy of the message. Thus, the recipient will not be able to see the other recipients. For reasons of politeness, use of blind copies should be avoided if possible.

When you click the individual buttons, the mail program will automatically insert the addresses at the correct position in the new message. After you have inserted all addresses, click 'Done'. In the input dialog, the individual addresses are separated with commas. Additional addresses can be entered manually.

Reading E-Mail

E-mail can be read in two different ways:

- Click the respective folder name in the list of folders. This is the fastest approach when you start the mail component. To return to the folder overview, click 'Folder'.

- Select the respective folder from the pull-down list 'switch current folder to'. With this approach, you can change to the respective folder without returning to the folder overview.

The INBOX

If you have not configured any mail filters (see 8 on page 155), all incoming messages will be stored in the 'INBOX' folder. When you click this folder, a dialog similar to the one shown in Figure 7.9 will appear.

Figure 7.9: The INBOX Overview of Berta Beck

Over the INBOX, you will see the same controls as in the folder overview. Below, there are two arrow icons to the left and two to the right. These arrow symbols can be used to browse the INBOX in case your messages cover more than one page. The green bar below provides important information on the INBOX, such as the number of new and unread messages. The INBOX itself consists of six columns.

The first column features check boxes for selecting the messages. Selected messages can be moved, deleted, or moved to the trash. To select all messages on the page, click the blue check mark under the check boxes. To move the selected message(s) to the trash, click 'Delete'. The message(s) will be moved to the folder 'INBOX/Trash'. To delete the message(s) permanently, change to this folder and delete the respective message(s). To move mail to a different folder, select the message(s), click the pull-down menu 'move selected messages into', and select the respective folder.

In the next column, you can see if a message only contains text or if it has a file attachment. If the message has an attachment, this is indicated by a paper clip in this column.

The third column ('From') specifies the sender. If the sender is highlighted with bold letters, this means that you have not yet read the message. To sort incoming messages by the sender, click the header 'From'. The header will be marked with two asterisks. By default, incoming messages are sorted by the date of receipt.

The next column ('Subject') displays the subject of the message. Subjects beginning with 'Re:' are usually replies. Click the subject to access the actual message. To sort the messages by the subject, click the header 'Subject'.

The next column ('Date') shows the date on which the message was sent or the time if the message was received on the same day.

The size of the message is displayed in the last column. Messages that only consist text are usually just a few KB. Messages that exceed 50 KB in size usually have attachments.

Replying to and Forwarding Messages

Click the subject to read the message. The navigation elements are located at the top of the view. Below, a green bar features arrow icons for scrolling (to the right) and the following four icons:

Envelope with red arrow pointing to the left – reply to message   Click this icon to reply to the message. A new window containing the recipient and the original message (without attachments) will appear, enabling you to compose the reply and add an attachment.

Envelope with two red arrows pointing to the left – reply to all   The function is the same as the above function. However, the reply will be sent to all recipients. This function is helpful if you want to discuss a matter with three or four persons.

Envelope with blue arrow pointing to the right – forward message   To forward the message to someone else, click this icon. The dialog for composing a message will be displayed, enabling you to select the recipient(s) and add a comment.

Trash – delete message   If you click this icon, the message will be moved to the trash without any confirmation query. Mail deleted in this way can still be accessed in the folder 'INBOX/Trash'. To delete a message permanently, change to this folder and delete it there.

Figure 7.10: *Reading and Replying to a Message*

The actual message is located under 'message:'. Attachments are located under 'section: 2'. Depending on the file type, the attachment may be displayed (e.g., images) or can be saved with a mouse click.

Creating New Folders

New subfolders cannot be created from the groupware interface. To create a new mail folder, log in to the administration interface and select 'Folder' → 'New'. Then log in to the groupware interface anew.

Editing Calendar Messages

Among the incoming messages, Internal messages of the calendar have a special status. These can be identified from the subject 'Calendar Event ()' (see Figure 7.9 on page 144). Such messages usually represent an invitation for a joint appointment. You have several options for responding to the invitation (see Figure 7.11 on the facing page).

This message provides an overview of the day on which the appointment takes place. If you have other appointments on the same day, these also appear on the timeline. In this way, you can check if the planned time is suitable. The title and description of the appointment and other important parameters such as the location, duration, participants, and the person who organizes the appointment are specified under the timeline.
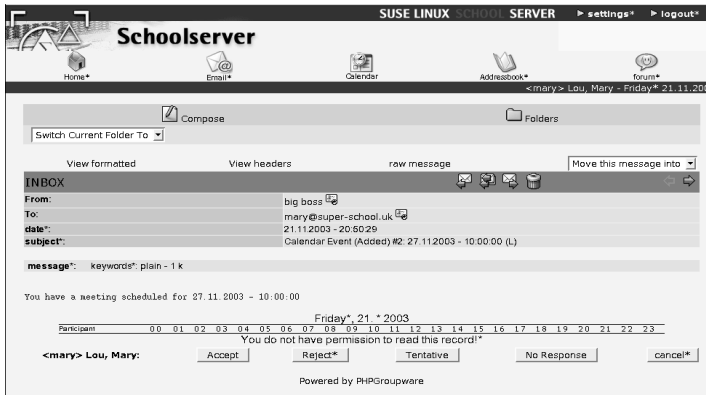
Figure 7.11: Organizing Appointments by Mail

Using the five buttons at the bottom, you can decide what to do. To participate in the appointment, click 'Accept'. If you are not able to participate, click 'Reject'. If you are not sure whether you will be able to participate but plan to do so, click 'Tentative'. If you cannot make a decision immediately, click 'No Response'. In this way, you can return to this message later on. Click 'Cancel' to access your calendar, where you can make a counter-proposal or reorganize an appointment that takes place at the same time.

As soon as you make your decision by clicking one of the buttons, a message sent by way of the server will automatically update the calendar entries of the other participants. For example, if you confirmed the appointment, you will automatically be taken to your calendar. In the calendar, select the appointment. Your name should be marked as '(Accepted)'.

Forums

Configuring Forums

To be able to utilize the SUSE LINUX School Server forums, these have to be configured by a teacher. Log in to the web-based user interface and select the menu item 'Administration' → '(Teacher) Forum Administration'. in order to access the dialog shown in Figure 7.12 on the next page. As the general forum and the teacher forum are configured in the same way, this chapter merely describes the configuration of the general forum.
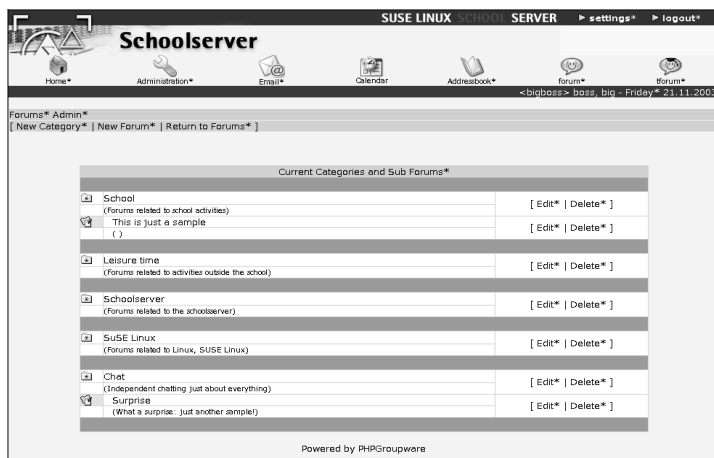
Figure 7.12: Initial Configuration of the Student and Teacher Forums

Configured example categories and the associated forums are listed under 'Current Categories and Sub Forums'. The easiest approach is to edit these. Click 'Edit' behind 'Just a sample' and enter a new name and a brief description for the category in the dialog that opens up. To save the changes and exit the dialog, click 'Update Category'. For example, you can create a category called "Linux".

At this stage, the forums (folder icon with note paper and pin) are still called 'Sample' and 'This is another sample'. Repeat the steps described above for these two entries and create forums such as "SUSE" and "Novell". Then change the entries under 'Another sample category' as described above. To create further categories, click the menu item 'New Category'. To create a new forum, click the entry 'New Forum'. When creating a forum, you have to select an existing category. Therefore, the needed categories have to be created in advance. When you are finished, your screen should look similar to Figure 7.13 on the facing page.

Repeat the same steps for the teacher forums. If you are not satisfied with the appearance, edit the file `default.theme` in `/srv/phpwg/phpgwapi/themes` or replace it by one of the theme files in this directory (as the user `root`).
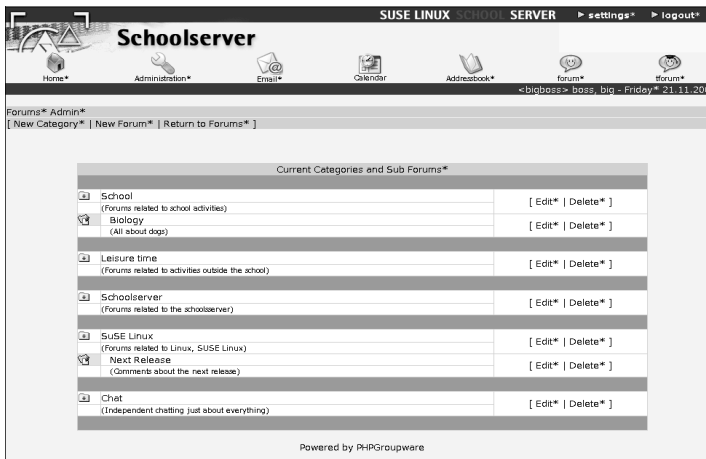
Figure 7.13: Following the Creation of the Forum

Caution

Changes in the theme file affect the entire web-based user interface, not only the forums. Therefore, you should make a backup copy of the existing `default.theme` file before you make any changes.

Caution

Using the Teacher Forum and Student Forum

Following the configuration of the forums, these can be used by the students and teachers. Teachers have access to both forums. Students can only read and write on the student forum. The configured categories, the brief description, the date of creation, and the number of messages are displayed on the start page (see Figure 7.14 on the next page).

If you select the name of the respective category, the associated forum will appear with the information listed above. Click the respective name again in order to access the subject overview. You can start a new thread ('New Topic') Topic or add a message to an existing thread. If you decide to start a new thread, you can write your first message. Think carefully before you start a thread, as created threads cannot be deleted. To participate in an existing thread, click the respective subject. Depending on how extensive the thread is, you may have to read a
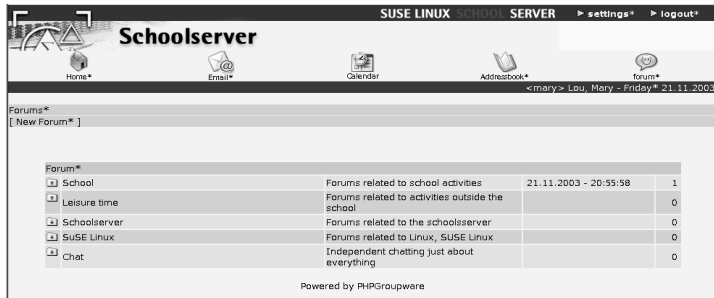
Figure 7.14: Start Page for a Student Forum

number of messages before you reach the input field for your own message at the end of the page.

To avoid this, click the item 'View Threads' next to 'New Topic' in the overview. In this way you can directly access the message you want to reply to. Replies are automatically marked as Re:. If you do not want to reply to a message but provide additional information, you can enter a more suitable subject.

Caution

Teachers can create and delete forums and categories, but they cannot moderate individual messages.

Caution

Administration as a User

The 'Setup' link in the groupware dialog takes users to a configuration zone in which they can specify personal settings. The individual menu items are explained in the following sections.

Settings

This menu offers options for changing your personal data, such as the address and phone number, and your password. It also has an option for downloading a personal certificate.

Entering and Changing Personal Data

Depending on your write access, you can change your personal data stored in the system's address book (see Figure 8.1 on the following page). If you do not have write access to some fields, they cannot be edited. To save your changes, click 'Save'.

> **Note**
>
> Students are not allowed to change their personal data. They only have access to their passwords.
>
> **Note**

Changing the Password

For security reasons, change your password from time to time. To do so, first enter your old password and then your new password twice in the designated
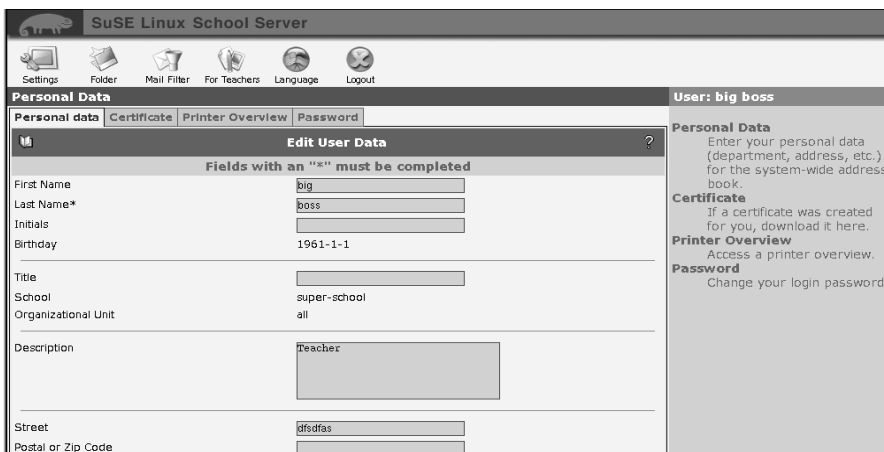
Figure 8.1: Personal Data

fields (see Figure 8.2 on page 153). You can also determine the way the new password is saved. The following options are available:

CRYPT: When using the CRYPT mechanism, the maximum length of the password is limited to eight characters. This is the standard mechanism for most Unix systems. Longer passwords are truncated.

SMD5: The SMD5 mechanism enables much longer passwords than the CRYPT algorithm – up to 255 characters. Moreover, security experts consider the encryption used for this mechanism to be superior to the method used for the CRYPT mechanism.

By default, the mechanism that was used for saving the old password will be applied.

If you forget your password, contact your administrator. The administrator can create a new password for you without knowing your old one.

Downloading a Certificate

If your administrator generated a certificate for you, download it with 'Certificate' and import it with your browser. For information about how to import a certificate with your browser, refer to the documentation of your browser.
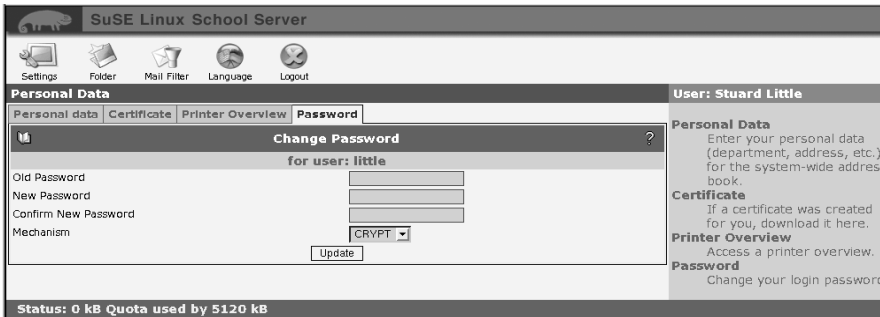
Figure 8.2: *Changing the Password of the User*

Folders

SUSE LINUX School Server places e-mail in folders. Under the menu item 'Folder', you can create, rename, and delete folders and administer the access permissions other users have to your folders. This is one of the advantages of the IMAP protocol. This is not possible when using POP.

SUSE LINUX School Server implements a hierarchical folder structure. The folder INBOX is located at the top of this hierarchy. All other folders are sub-folders of INBOX. By default, the following folders are created for every user:

INBOX: If no mail filters are defined, all incoming messages are stored here.

INBOX.drafts: In this folder, you can store unsent message drafts.

INBOX.sent-mail: All sent e-mail is stored here.

INBOX.spam: This folder is used if the SPAM filter is active on your system. All mail identified as SPAM can automatically be moved to this folder (for details about the SPAM filter, see 8 on page 158).

INBOX.trash: By default, the web mail program saves backup copies of deleted e-mail in this folder.

These folders are needed by the system and should not be deleted. The entire INBOX cannot be deleted.

Creating a New Folder

Click 'New' to create new folders. A list of all folders in which you can store e-mail is displayed to the left. To add a new folder, use the mouse to select an existing folder (such as INBOX) under which you want to create a new folder. Enter the name of the new folder (see Figure 8.3).
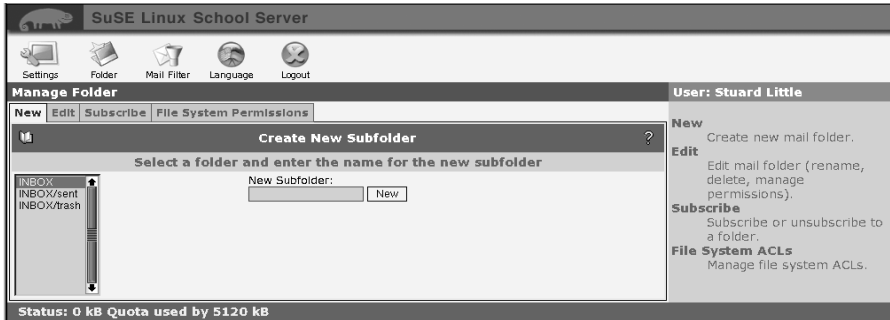

Figure 8.3: Creating a New Folder

Click 'New' to create the folder. The name of the new folder is, for example, INBOX.subfolder. Other subfolders, such as another_folder, can be created in this folder. In this case, the name of the folder will be INBOX.subfolder.another_folder.

> **Note**
>
> The dot in folder names has a special meaning. A dot is used as a hierarchy separator, similar to the "/" (slash) in the directory structure. For example, creating the folder teacher.maths is comparable to creating the directory teacher containing the file maths. If you create a second folder called teacher.music, you will have a directory with two files.
>
> If the folder teacher was not created, no e-mail can be stored in this folder.
>
> **Note**

Editing Folder Properties and Permissions

In the submenu 'Edit', you can rename and delete existing folders and edit the access permissions of other users for these folders. To delete a folder, select it from the list to the left and click 'Delete'.

Caution

When deleting a folder, all mail it contains is lost. All its subfolders and their contents are also deleted.

Caution

To rename an existing folder, select it from the list, enter the new name, and click 'Rename' (see Figure 8.4).

Figure 8.4: Editing Folders

Apart from the shared folders, you can also assign permissions to the user folders. Click 'Set Permissions' to access a dialog like the one used for creating shared folders. As the owner of the folder, you have all permissions for this folder. This setting should not be changed.

SIEVE: The Mail Filter

Using the SIEVE-based mail filter system, you can automate the handling of incoming mail. A detailed description of SIEVE is provided in RFC 3028:

```
http://www.ietf.org/rfc/rfc3028.txt
```

Mail filter

In 'Mail Filter', you can define the rules for handling incoming mail. For example, you can automatically sort e-mail messages in certain folders or forward them to another e-mail address.

When you select 'Mail Filter', you will first see an overview of all existing mail filters. Initially, this list is empty.

Creating Filter Rules

To create a new rule for a filter, click 'Enter filter rule'. Creating a new rule for a filter is divided into several few steps. The first step is to define the filter conditions. The following properties of an e-mail can be evaluated:

Size: Checks whether the size of a message is larger or smaller than the specified value.

Header/envelope fields: Checks the content of header and envelope fields, which contain information such as the sender, recipient, and subject of an e-mail message.

The second step is to define an action that is executed if the filter conditions match. If several filter conditions are entered, you can determine how the individual conditions are linked.

`AND` means that all filter conditions must apply in order for the action to be executed. `OR` means that only one condition must apply (see Figure 8.5).
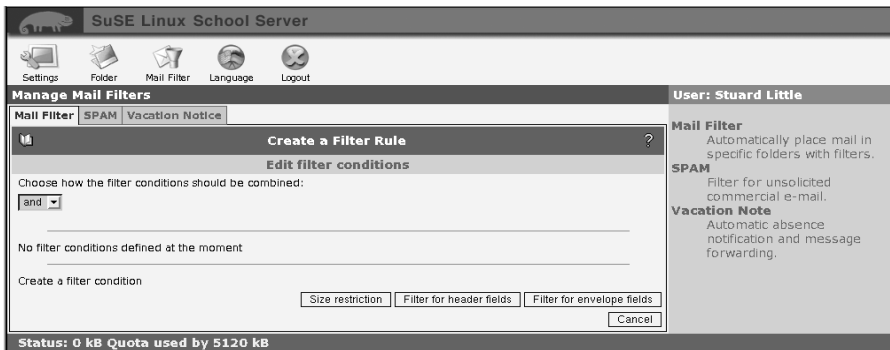

Figure 8.5: Mail Filter

The following simple example demonstrates the configuration of the mail filter. A friend regularly sends you e-mail. However, you do not want to receive all messages. You want to sort out all messages sent by `friend@domain.com` that are larger than one MB. These messages are to be rejected and the sender is to be notified accordingly.

Select 'insert filter rule'. Click 'Size limit'. Insert the desired value (see Figure 8.6 on the facing page). For our example, use 'larger than 5 Megabytes'. Confirm with 'OK'. Then select 'Filter of header fields'. Enter 'From contains friend@domain.com' and confirm with 'OK'. Click 'Next' to access the dialog for selecting a suitable action.
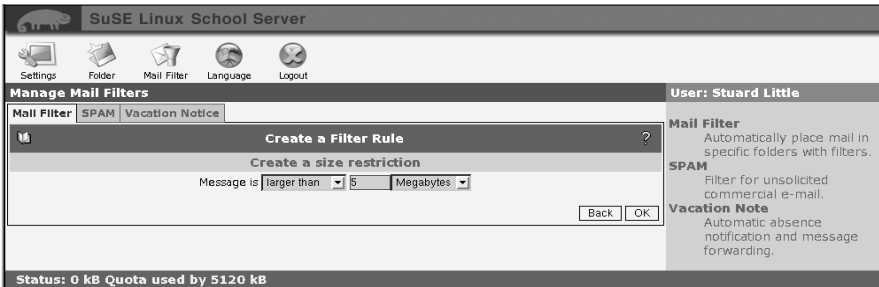
Figure 8.6: Define a Size Limit

Select 'reject message with the explanation' and enter a meaningful text, such
as "Your mail is too large. Please do not send me such large messages!" (see
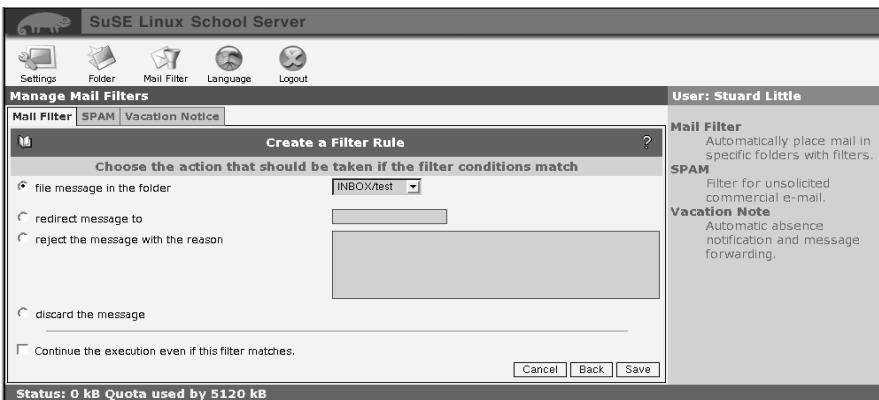Figure 8.7).

Figure 8.7: Setting Mail Filter Actions

To apply another filter to this mail – which is rather unlikely in this example – click 'Continue processing this mail'. Save the changes. If you open the sub-menu 'Mail Filter' anew, you will see the new rule in form of a sentence. If you wish, you can edit this filter (the icon with the paper and pen), disable or enable it without modifying the data (the red X or green check mark), or delete the filter (waste bin icon). To create another filter, click 'Insert new filter'. Unless you change the field 'in position', the filter will be placed after existing filters. In some cases, the order of the filters is important.

SPAM: Filter for Unsolicited Commercial E-Mail

If the system is configured for recognizing and marking SPAM, you can determine what to do with messages marked as SPAM. The following options are available:

Save to a folder: If this item is activated, you can select a folder for storing all messages marked as SPAM.

Delete: All messages marked as SPAM are deleted immediately.

> ┌─ **Caution** ─────────────────────────────
>
> Use this setting with caution. Possibly, non-SPAM mail may be taken for SPAM due to SPAM-typical characteristics.
>
> ──────────────────────────── **Caution** ─┘

Nothing: No special handling of mail recognized as SPAM.

Vacation Notice: Automatic Reply During Absence

Using the vacation notice, you can configure the server to reply automatically to incoming e-mail messages. Click 'Create' to configure a vacation notice. In the following dialog, enter a subject and text for the automatic reply (see Figure 8.8 on the facing page).

To use the subject of the incoming message, leave the 'Subject' field empty. If someone sends you an e-mail message while the vacation notice is activated, the sender will receive your standard reply. The sender will be stored in a database. If the sender sends another message within the time frame specified in 'Repeat after', the automatic reply will not be sent again. In 'Forward to', you can specify an e-mail address to which incoming mail will be forwarded. E-mail can be
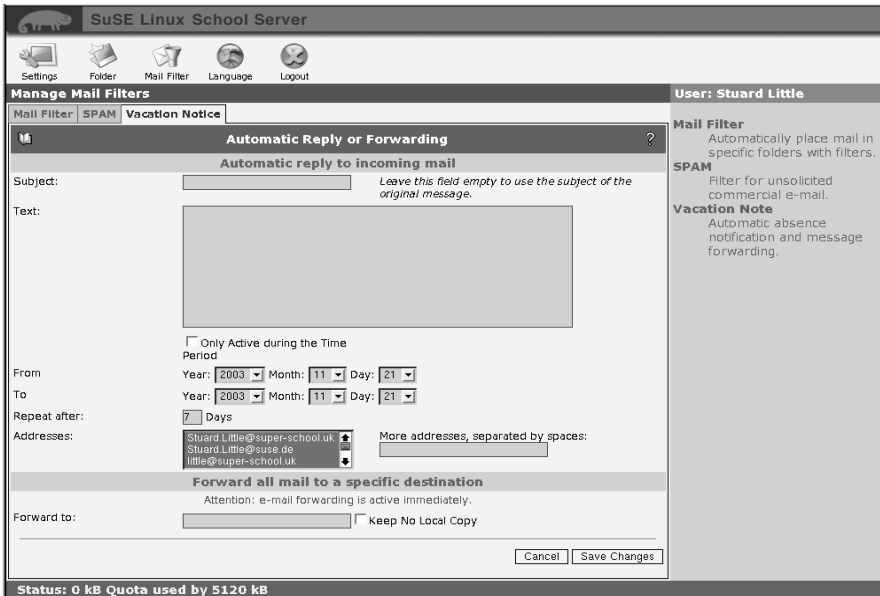
Figure 8.8: Creating a Vacation Notice

forwarded to an internal address (e.g., if a colleague takes over your responsibilities) or external e-mail addresses (e.g., a mail account you can access from home).

If you created a vacation notice, it will be shown when you select this submenu. You can activate or deactivate this function without changing the settings by clicking the green check mark or the red X.

For Teachers

Control Access

Like the main administrator `admin`, teachers can also block or allow the access of the hosts in a room to certain services (access to the Internet, mail and groupware server, print server) (see 4 on page 81). However, teachers can only control the access in the room they are currently in.

In order to prevent the host on which the action is executed from being blocked, mark the check box 'Den eigenen Rechner nicht aussperren' (default setting).
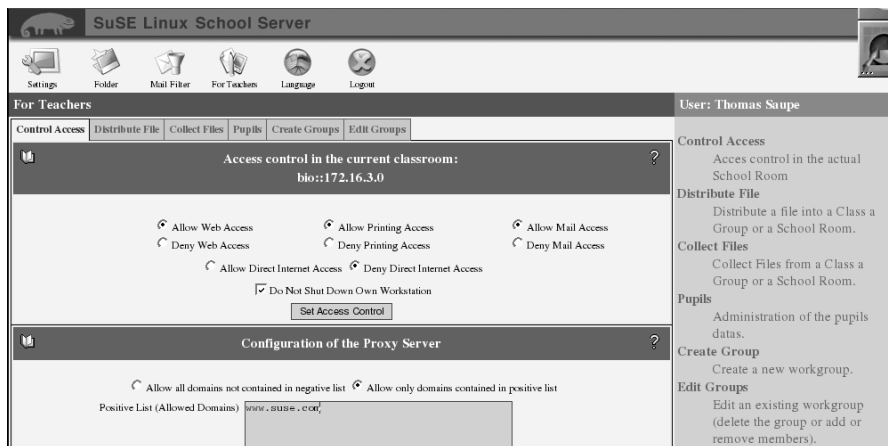

Figure 8.9: Access Control for Teachers

Allow or Deny Web Access

Activate this button to allow registered clients to access the proxy server, thus enabling students to surf the Internet.

The permission or prohibition to use the Internet is implemented on the basis of rooms, provided the clients are registered with the server. For example, if a teacher in the Computer Room 1 allows his students to use the Internet, this will not affect the hosts in the other rooms.

From the long waiting time and the subsequent error message (indicating that the page cannot be accessed) in the browser, students will notice that Internet access is not possible. Clients are not sent any special notification.

Allow or Deny Printing Access

If the printers of the school are managed by means of the print server of SUSE LINUX School Server, this item can be used to block access to all available print-

ers from the respective room. In this way, you can prevent undesired printing.

Allow or Deny Mail Access

With this item you can permit or block access to the groupware page under `https://SchoolServer`.

Allow or Deny Direct Internet Access

With this item you can activate masquerading for the hosts in the respective room.

This is necessary for directly exchanging data with servers on the Internet by way of `ftp`, `smtp`, `imap` or `pop`. For instance, if the school's home page is hosted by a provider and you want to update it via `ftp` or you want to edit e-mail from another provider with an e-mail client, you have to activate masquerading.

Tip

Masquerading

If masquerading is implemented, SUSE LINUX School Server generates a table of the internal IP addresses of the clients which are not forwarded on the Internet. When a client submits a query, the server enters its IP address (and the respective port) in its table and replaces the sender address of the query packet with its own public IP address (using a different port which it can assign later on). When the server receives the reply from a server on the Internet (on the respective port), it checks the packet, allocates it to the correct client on the basis of the table, enters the correct receiver address, and forwards it to the client.

Normally, neither the clients nor the servers on the Internet will notice this backstage substitution – both will think they are directly connected to each other. However, this procedure may not work with some applications.

Tip

As the server sends the clients their IP address together with some other data via `DHCP`, usually no further configuration is needed on the clients.

For FTP programs, enable the "passive" transmission mode. If set to "active" FTP, the clients will submit a query to the respective FTP server and request to be called back on a free port. In this case, the FTP server will select a free port and try to establish a connection on this port.

However, as SUSE LINUX School Server does not know where to forward the respective external query, it will reject the connection attempt of the FTP server. If set to "passive" FTP, the clients will repeatedly try to establish a data connection to the FTP server until they find a free port on the server. This takes a few fractions of a second longer, but in this way the connections are established by the clients and SUSE LINUX School Server is able to allocate the respective responses correctly.

> ┌─ **Caution** ─────────────────────────────
>
> If masquerading is enabled, the clients will have a "direct" connection to the Internet. In this case, protective functions of SUSE LINUX School Server (such as the Internet filter) are no longer effective!
>
> ────────────────────────────── **Caution** ─┘

Configuration of the Proxy Server

Here you can "fine-tune" the Internet access for the clients. You can permit `Everything which is not contained in the negative list` of the proxy server (see annex of the online manual at `http://admin/manual/manualEN.pdf`) or create your own "positive list".

To limit your students' access during lessons to certain domains, enter the respective URLs in the dialog (see Figure 8.9 on page 160 and activate `Allow only domains contained in positive list`.

For example, to limit the access to the domain `http://www.suse.com`, enter this domain here, activate `Allow only domains contained in positive list`, and click `Set Access Control` (after having activated `Allow Web Access`).

Distributing and Collecting Files

SUSE LINUX School Server enables teachers to distribute files to the students of a class. To do this, go to the menu item 'For Teachers' → 'Distribute File' (see Figure 8.10 on the preceding page) and select the desired file and class. The file will be placed in the personal `Import` directories of the students of the selected class.

Select the menu item 'For Teachers' → 'Collect Files' to place the contents of the `Export` directories of the students of a class in the `Import` directory of the teacher. If necessary, separate directories will be created for every student: `/home/teacher/<teacherlogin>/Import/<teacher~loginname>/<files>`.
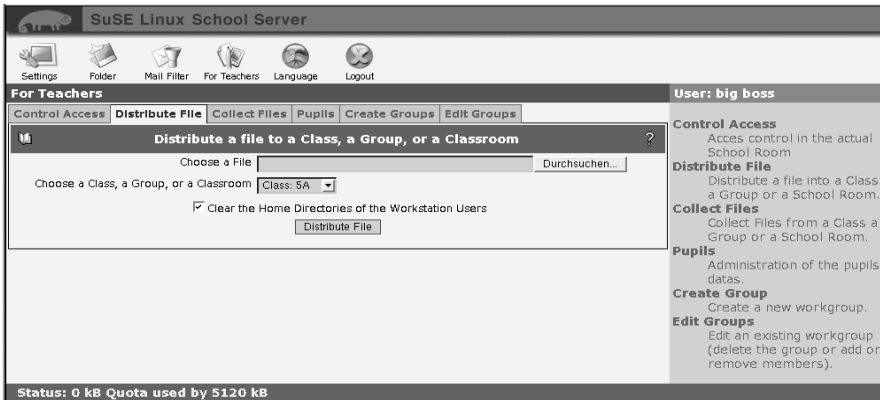
Figure 8.10: Distributing Files

Workstation User - Examination Environment

If the client machines are registered according to rooms, examinations can be conducted in a protected environment. For this purpose, select a room instead of a class under 'For Teachers' → 'Distribute File'.

Click 'Clear the Home Directories of the Workstation Users' to set the home directories of the workstation users to a default state before you distribute the file. In this case, the students should log in after the file has been distributed.

> **Tip**
>
> For examinations, do not forget to set the access permissions for the class room accordingly (see 8 on page 159).
>
> Workstation accounts do not have access to the Internet, groupware, and e-mail.
>
> **Tip**

Students should log in with the workstation accounts, not with their own user accounts. The access data are as follows:

- Login = name of the workstation
- Password = name of the workstation

Following the login, the students will find the distributed files in the subdirectory `Import` in the home directory. At the end of the lesson, the students can save the edited files in the `Export` directory, from where they can be collected by the teacher.

Administration through Teachers

If a teacher was assigned administration rights during the installation or later, the teacher is able to change the passwords and access permissions of the students and create new user groups.

> **Note**
>
> When teachers are imported from a list, they are not assigned administration rights. In this case, the administrator has to set the respective rights manually.
>
> **Note**

Students

In the menu 'Students', select which users to display. If you have a limited number of users and want to list all users, click 'Apply Filter' without changing the value '*' in the input field 'Filter'. Select the user to edit with a mouse click.

> **Note**
>
> A teacher with administration rights can only change the passwords of his "own" students (the students in his classes.
>
> **Note**

Select the user to edit with a mouse click.

You can search for users according to the following criteria:

UID or last name or first name Enter the search string or part of it with the wild card '*' in the input field 'Filter'. Other wild cards like e. g. '?' do not work here.

Class or group Enter the designation of the class or group whose members you are looking for in the field 'Class'. Here too you can use the wild card '*'. For instance, all fifth-grade students and teachers can be listed with the search string '5*'.

The functions

Allow/Disable External eMail Here you can permit the students to send e-mail to external addresses. Normally, students are only permitted to send e-mail within the school domain. E-mail to external addresses are not forwarded.

Allow/Disable Internet Access   If a student misuses the Internet, you can block his access to the Internet as a "disciplinary measure". In this case, the student will be able to log in to a client as usual and use all other SUSE LINUX School Server functions. However, if he attempts to log in to the proxy server, he will be denied access to the Internet.

Add or remove from Groups   If you created your own groups, you can add the student(s) to these groups.

can also be executed simultaneously for multiple users. To do this, keep the (Ctrl) or (Shift) key pressed while selecting several users with the mouse.

The names of the selected users will be highlighted. The button for the individual functions are located to the right (see Figure 8.11).
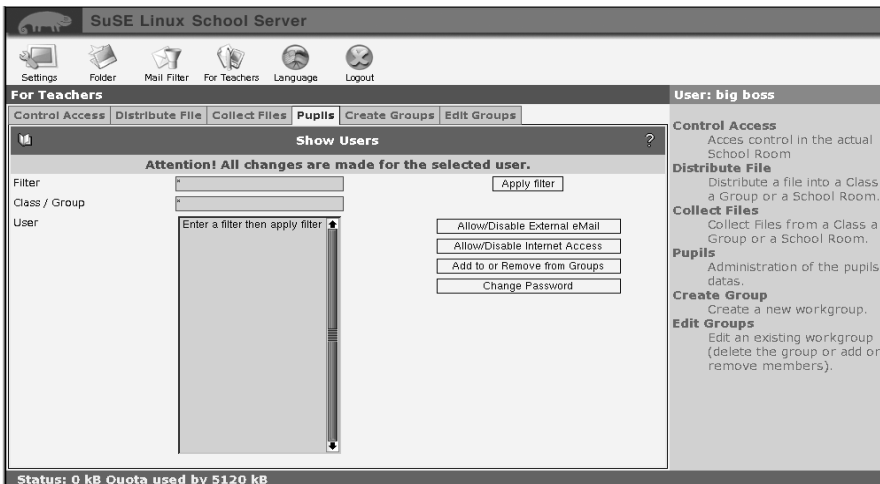
Figure 8.11: *Administration through Teachers: Editing User Data*

Under 'Change Password', you can change the password of students who forgot their passwords. To do this, you do not need to know the old password.

Under the menu item 'Mechanism', you can select the password encryption mechanism. The older CRYPT encryption allows a maximum password length of eight characters, longer passwords are simply truncated.

SMD5 enables the use of passwords consisting of up to 255 characters.

If you want the student to change the password after the first login (recommended), activate the respective check box before you click 'Update'.

Create/Edit Groups

Here you can create your own workgroups with shared folders for joint tasks and a separate e-mail address for the workgroup name.

Note

Workgroup names may not contain any blank spaces or special characters.

Note

You can first create workgroups without any members and later add students or teachers.

All members of the workgroup automatically receive e-mail messages addressed to the workgroup name in a subfolder called `workgroups/` `<workgroupname>`.

The shared folder is located in the subdirectory `/home/groups/` `<workgroupname>`. All members have full access to this folder

Change Language

Select a language under the menu item 'Language' and click 'Set Language'.

Memo

Support Information

All information you need when you contact our support desk is listed in this section. In order to be able to solve problems quickly, you should be close to the server and a client.

FIRST NAME:	
LAST NAME:	
COMPANY:	
STREET:	
COUNTRY:	
POSTAL CODE:	
CITY:	
REG CODE: (product registration code)	
E-MAIL:	

Hardware Information

Try to collect as much information as possible about the server hardware.

CPU(s)/clock frequency:		Graphics card:	
Main board:		RAM:	
SCSI or RAID controller	Manufacturer, model	Driver	
Hard disk(s)	Manufacturer, model		
CD-ROM drive	Manufacturer, model:		
Network adapter eth0	Manufacturer, driver	Subnet or DSL	MAC address
Network adapter eth1	Manufacturer, driver	Subnet or DSL	MAC address
Network adapter eth2	Manufacturer, driver	Subnet or DSL	MAC address
ISDN card	Manufacturer, driver		

Hard Disk Partitioning Data

In the event of a failure or accidental destruction of the partition table, the data specified here may be useful. Simply enter the values displayed in the YaST partitioning tool.

Device	Size	Type	Mount point	Start cylinder	End cylinder	RAID

Passwords

For security reasons, making a note of the server passwords is a bad idea. However, if the administrator is absent, such a note may represent the last resort, provided it is kept under lock and key.

┌─ **Caution** ──

Keep the password memo in a sealed, non-transparent envelope and keep it in a safe place.

The administrator should be notified before the envelope is opened.

── **Caution** ─┘

Department	Account	Password	Note
Internet			Provider data
Server BIOS			
Server root	root		
School admin	admin		
Mail server	mailadmin		

Index