

# Deploying Samba on IBM @server BladeCenter

Installing Red Hat 7.3, SuSE 8.1 Linux  
and IBM Director

Installing Samba

Managing Samba using  
SWAT



Rufus Credle  
Eric Butler  
Tim Verhoeven  
David Green





International Technical Support Organization

**Deploying Samba on IBM @server BladeCenter**

November 2003

**Note:** Before using this information and the product it supports, read the information in “Notices” on page v.

**Second Edition (November 2003)**

This edition applies to IBM @server BladeCenter (8677-1xx), IBM @server BladeCenter HS20 (8678-21x and 8678-41x), Red Hat Linux 7.3 and SuSE Linux Enterprise Server 8.

© Copyright International Business Machines Corporation 2002, 2003. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

<b>Notices</b> .....	v
Trademarks .....	vi
<b>Preface</b> .....	vii
The team that wrote this Redpaper .....	vii
Become a published author .....	viii
Comments welcome .....	viii
<b>Summary of changes</b> .....	ix
November 2003, Second Edition .....	ix
<b>Chapter 1. Introduction to IBM eServer BladeCenter technology and its advantages</b> ..	1
1.1 Introduction to blade server technology .....	2
1.1.1 IBM eServer™ BladeCenter and BladeCenter HS20 features .....	2
1.2 Technical overview .....	3
1.2.1 BladeCenter chassis .....	3
1.2.2 IBM eServer BladeCenter HS20 .....	5
1.2.3 BladeCenter Management Module .....	8
1.2.4 BladeCenter 1200W Power Supply Module .....	9
1.2.5 BladeCenter blowers .....	11
1.2.6 BladeCenter 4-Port Ethernet Switch Module .....	12
1.2.7 BladeCenter Layer 2-7 GbE Switch Module .....	13
1.2.8 BladeCenter 2-Port Fibre Channel Switch Module .....	14
1.2.9 BladeCenter Acoustic Attenuation Module .....	15
1.3 The advantages of IBM eServer BladeCenter .....	16
1.3.1 Systems management .....	16
1.3.2 High density computing .....	18
1.3.3 Redundancy .....	20
<b>Chapter 2. Samba</b> .....	25
2.1 What is Samba? .....	26
2.2 What can you do with Samba? .....	26
<b>Chapter 3. Installation of Red Hat Linux 7.3 and IBM Director Agent</b> .....	29
3.1 Installation of Red Hat Linux 7.3 .....	30
3.2 CD installation .....	30
3.2.1 Creating the boot disk .....	30
3.2.2 Installing Red Hat 7.3 .....	30
3.2.3 Applying updates and installing the latest kernel .....	35
3.3 Network installation .....	36
3.3.1 Setting up the NFS install server .....	36
3.3.2 Setting up the FTP install server .....	37
3.3.3 Creating the network boot diskette .....	38
3.3.4 Installing from the NFS server .....	40
3.3.5 Installing a Linux operating system from the FTP server .....	41
3.4 PXE Boot installation .....	42
3.4.1 Configuration of the PXE Boot server .....	42
3.4.2 Starting the installation .....	44
3.5 Installation of SuSE Linux Enterprise Server 8 .....	46

3.6 Installation of IBM Director Agent .....	52
3.6.1 Overview of IBM Director V4. ....	52
3.6.2 Installation of IBM Director Agent on Linux. ....	54
<b>Chapter 4. Installing and configuring Samba. ....</b>	<b>57</b>
4.1 Installing Samba .....	58
4.2 Configuring the Samba server .....	58
4.2.1 Samba configuration file .....	58
4.2.2 Using SWAT .....	64
4.3 Encrypted password file .....	76
4.4 Starting and stopping the Samba server. ....	77
4.5 Starting Samba as part of the boot process .....	77
4.6 Sources and additional information. ....	78
<b>Chapter 5. Samba management and troubleshooting .....</b>	<b>79</b>
5.1 Checking the server status .....	80
5.1.1 Checking the status .....	80
5.1.2 Checking resources .....	80
5.1.3 Checking WINS. ....	82
5.2 Testing the configuration file .....	83
5.3 Closing connections .....	85
5.3.1 Command line .....	85
5.3.2 SWAT .....	87
5.4 Configuring log files. ....	87
5.5 Sending Winpopup messages .....	89
5.6 Viewing NetBIOS network traffic. ....	90
5.6.1 Installing ethereal .....	90
5.6.2 Using ethereal. ....	90
5.7 Sources of additional information .....	94
<b>Chapter 6. A brief introduction to Layer 4-7 Switching .....</b>	<b>95</b>
6.1 Layer 4-7 Switching. ....	96
<b>Appendix A. Samba configuration file .....</b>	<b>99</b>
Sample smb.conf with comments .....	100
<b>Related publications .....</b>	<b>111</b>
IBM Redbooks .....	111
Referenced Web sites .....	111
How to get IBM Redbooks .....	112
IBM Redbooks collections. ....	112

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.*

*The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:* INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

## COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

# Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

@server™  
@server™  
Redbooks (logo) ™  
eServer™  
ibm.com®  
pSeries®  
xSeries®  
zSeries®  
AIX®

BladeCenter™  
Chipkill™  
Domino®  
DB2®  
DFS™  
Home Director™  
IBM®  
Lotus Notes®  
Lotus®

Netfinity®  
Notes®  
Predictive Failure Analysis®  
PS/2®  
Redbooks™  
ServerProven®  
Tivoli Enterprise™  
Tivoli®  
WebSphere®

The following terms are trademarks of International Business Machines Corporation and Rational Software Corporation, in the United States, other countries or both:

Rational Software Corporation®      Rational®

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.



# Preface

As data centers have grown with the proliferation of Intel®-based servers over recent years, it is important to note that rack space and floor space can be more efficiently used with the use of the IBM® IBM @server BladeCenter™ HS20 servers. Attractive cost savings are also possible where a large number of rack installed servers are required, since the equivalent number of 1U servers would be much more expensive.

This IBM Redpaper describes how to set up and configure Linux and Samba on the IBM IBM @server BladeCenter and provides some pointers on managing the installation. It also describes the functionality of the IBM IBM @server BladeCenter in this type of environment.

## The team that wrote this Redpaper

This Redpaper was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

**Rufus Credle** is a Senior I/T Specialist and certified Professional Server Specialist at the International Technical Support Organization, Raleigh Center. He conducts residencies and develops Redbooks™ about network operating systems, ERP solutions, voice technology, high availability and clustering solutions, Web application servers, pervasive computing, and IBM and OEM e-business applications, all running IBM @server xSeries® systems. Rufus's various positions during his IBM career have included assignments in administration and asset management, systems engineering, sales and marketing, and IT services. He holds a BS degree in business management from Saint Augustine's College. Rufus has been employed at IBM for 22 years.

**Eric Butler** is a Network Engineer in United States of America. He has three years of experience with Linux and Open Source software. He holds a degree in Electrical Engineering. He has worked at IBM for seven years. His areas of expertise include network monitoring, administration of Lotus® Domino®, AIX®, and Linux systems, DCE/DFS™, Apache, Samba, MRTG, Cricket, and xSeries and pSeries® hardware. Eric participated extensively in the writing of *Deploying Samba on IBM @server BladeCenter*, REDP3595.

**Tim Verhoeven** is an IT Professional in Belgium. He has four years of experience in Linux and Open Source software. He has worked at IBM for one year. He holds a degree in Electronics and Computer Science. His areas of expertise include Linux, Apache, Samba, WebSphere® Application Server, Java™ and J2EE, xSeries and zSeries® hardware and clustering. Tim participated extensively in the writing of *Deploying Apache on IBM @server BladeCenter*, REDP3588.

**David Green** is a Staff Engineer at IBM in Research Triangle Park, North Carolina and works in BladeCenter ecosystem development. He worked on the development of the Layer 2-7 GbE Switch Module and the Optical Passthrough Module for BladeCenter. He has a Bachelor of Science degree in Information Systems from UNC-Greensboro. His areas of expertise include IBM IBM @server BladeCenter, Fibre Channel, SANS and networking.

Thanks to the following people for their contributions to this project:

Tamikia Barrow, Diane O'Shea, Gail Christensen, Cecilia Bardy, Jeanne Tucker  
International Technical Support Organization, Raleigh Center

Stephen Hochstetler  
International Technical Support Organization, Austin Center

Rob Sauerwalt, Global Brand Manager and Team Lead - IBM IBM @server Marketing  
IBM Raleigh

Amy Freeman, Manager, Brand and ISV Communications, xSeries Linux Marketing  
IBM Raleigh

ITSO PC-5009 project team: David Robertson, David L Brown, Lowell Davis, Thomas Ternau  
IBM Raleigh

## Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this Redpaper or other Redbooks in one of the following ways:

- ▶ Use the online **Contact us** review redbook form found at:

[ibm.com/redbooks](http://ibm.com/redbooks)

- ▶ Send your comments in an Internet note to:

[redbook@us.ibm.com](mailto:redbook@us.ibm.com)

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization  
Dept. HQ7 Building 662  
P.O. Box 12195  
Research Triangle Park, NC 27709-2195

# Summary of changes

This section describes the technical changes made in this edition of the paper and in previous editions. This edition may also include minor corrections and editorial changes that are not identified.

Summary of Changes  
for Deploying Samba on IBM @server BladeCenter  
as created or updated on November 20, 2003.

## November 2003, Second Edition

This revision reflects the addition, deletion, or modification of new and changed information described below.

### **New information**

- ▶ Added 1.2.7, “BladeCenter Layer 2-7 GbE Switch Module” on page 13
- ▶ Added Chapter 6, “A brief introduction to Layer 4-7 Switching” on page 95
- ▶ Added information to 1.2.4 “BladeCenter 1200W Power Supply Module”
- ▶ Added URLs to the bibliography

### **Changed information**

- ▶ None at this time





# **Introduction to IBM eServer BladeCenter technology and its advantages**

In this chapter, we will introduce the IBM *@server* BladeCenter. This introduction includes an overview of the BladeCenter technology and hardware for the chassis and the blades; we also look at blade management and the options that are currently available. We will also discuss the advantages of blade servers over other servers in the market, where the blade servers fit into the market and why the market is driven towards blade servers.

## 1.1 Introduction to blade server technology

Blade servers are a relatively new technology that has captured industry focus because of its modular design, which can reduce cost with a more efficient use of valuable floor space, and its simplified management, which can help to speed up such tasks as deploying, reprovisioning, updating and troubleshooting hundreds of blade servers. All this can be done remotely with one graphical console using IBM Director systems management tools. In addition, blade servers provide improved performance by doubling current rack density. By integrating your resources and sharing key components, you will not only reduce cost but also increase availability.

### 1.1.1 IBM eServer™ BladeCenter and BladeCenter HS20 features

- ▶ The IBM @server BladeCenter has the following features:
  - Rack-optimized, 7U modular design enclosure: holds up to 14 hot-swap BladeCenter HS20 blades with up to six enclosures in a 42U rack.
  - Contains a high availability MidPlane supporting the hot-swap of individual blades.
  - Two 1200-watt, hot-swap power modules and support for two optional 1200-watt power modules: provides redundancy and power for robust configurations. See the guidelines in 1.2.4, “BladeCenter 1200W Power Supply Module” on page 9.
  - Two hot-swap 325 CFM blowers and thermal sensors throughout to monitor and alert you to over-temperature conditions.
  - Management module: lets you manage and control components in the enclosure.
  - Optional hot-swap redundant Ethernet and Fibre Channel switch modules (supports up to four network switch modules).
  - Control panel : contains USB port and status LEDs.
- ▶ The IBM @server BladeCenter HS20 features are as follows:
  - Choose between 2.0 or 2.4 GHz(1) Xeon processors with quad-pumped 400 MHz front-side bus (FSB) and full-speed 512 KB ECC L2 caches.
  - Standard 512 MB system memory with Chipkill ECC support: supports 8GB maximum, when 2GB memory module becomes available.
  - Dual Broadcom Gigabit Ethernet controllers with teaming and failover support.
  - Integrated service processor: monitors critical components on each blade for remote and local systems management.
  - ATA-100 IDE controller: economical interface for up to two optional 40 GB IDE HDDs.
  - SCSI expansion connector: supports optional storage unit containing an Ultra320 RAID 1 SCSI controller and backplane support for two hot-swap HDDs.

Each of these features will be discussed in greater detail later in the paper, as well as a few other important points.

## 1.2 Technical overview

In this section, we will look at each of the key components individually and explain their function within the IBM eServer BladeCenter and the BladeCenter HS20.

### 1.2.1 BladeCenter chassis

The IBM eServer BladeCenter is a 7U modular chassis capable of housing up to 14 blade servers. The BladeCenter chassis allows individual blades to share resources such as power, switch, management and blower modules. The front view of the BladeCenter chassis is shown below in Figure 1-1. We can see the fourteen slots which, in this example, has been populated by one blade server and thirteen Processor Blade Fillers. These Processor Blade Fillers are required if a slot is not populated by a blade server or the HS20 SCSI Expansion Option, which will be discussed later, to provide proper airflow and system cooling. The BladeCenter Media Tray is also shown; it is located at the top of the chassis above the blade slots. This is shown in greater detail in Figure 1-2 on page 4.



Figure 1-1 Front view of BladeCenter chassis

The Media Tray is a hot-pluggable unit that contains an interface card, CD-ROM and diskette drive. Mounted on the interface card is a USB 1.1 port and system information LEDs which provide status information for your IBM eServer BladeCenter and BladeCenter HS20s.

There are five LEDs on the front panel. Figure 1-2 on page 4 illustrates the location of these LEDs. The five LEDs are:

- |                 |   |
|-----------------|---|
| <b>Power</b>    | This is a green LED which indicates the presence of power in the BladeCenter chassis. If this LED is not on, it could indicate one of the following conditions: <ul style="list-style-type: none"><li>• There is no power to the chassis.</li><li>• The management module is not present or has failed.</li><li>• The LED has failed.</li></ul> |
| <b>Location</b> | This LED is used to locate or identify the particular IBM eServer BladeCenter. When on, this LED is bright blue and can be set to blink or remain constant. This LED will be on as a result of a request from the systems administrator via the Management Module or if a component requires maintenance.                                       |

- Over- temperature** This is an amber LED which will report any over-temperature conditions that occur either in the BladeCenter chassis or the blade servers. If an over-temperature condition occurs, the IBM @server BladeCenter may increase the speed of the blower to correct this, in which case the LED will automatically be turned off.
- Information** The information LED is also amber; this LED reports non-critical events. These events are recorded in the Error log. This LED must be manually switched off via the management module.
- System Error** Again, this is an amber LED which reports when a system error occurs. This LED reports errors such as a failure of a power, blower or switch modules. It will also be on if a system error occurs on a blade. The failed component's LED will also be on to help isolate the error.

These system LEDs are also located on the rear of the BladeCenter chassis under blower module 2.

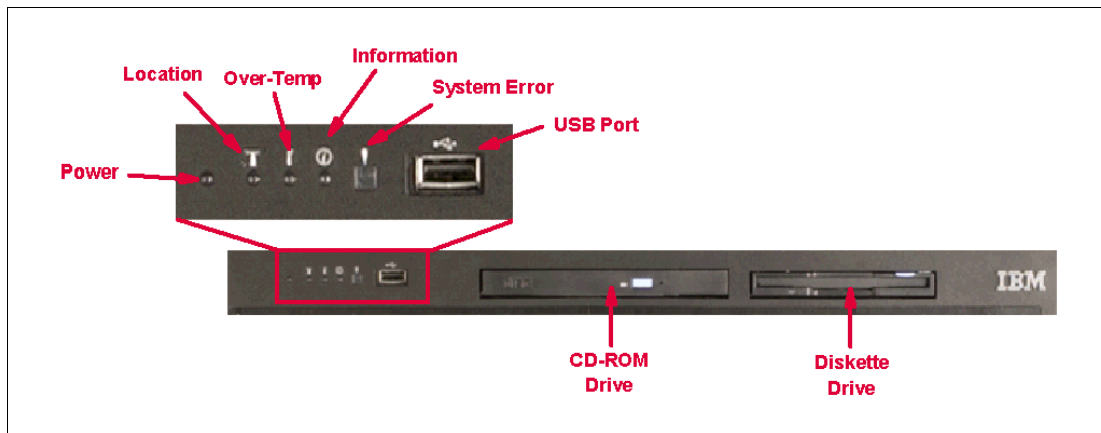


Figure 1-2 Media tray front view

As we discussed earlier, the BladeCenter chassis is capable of housing several hot swap and redundant components, such as:

- ▶ Power supply modules
- ▶ Switch modules
- ▶ Management modules
- ▶ Blower modules

In Figure 1-3 on page 5, you can see where each of these components should be located in the rear of the IBM @server BladeCenter.



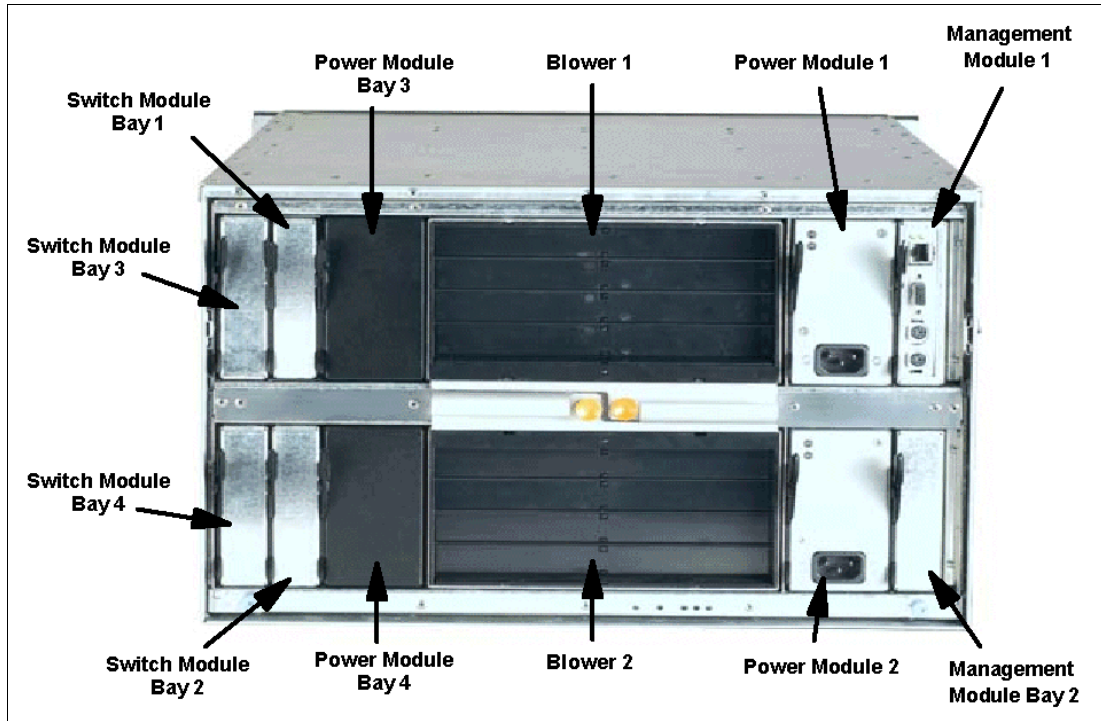


Figure 1-3 Rear view of BladeCenter chassis

The IBM @server BladeCenter automatically detects all blades and modules that are installed.

## 1.2.2 IBM eServer BladeCenter HS20

The IBM @server BladeCenter HS20 blades are high-throughput, two-way SMP-capable Xeon-based blade servers, highly scalable by adding memory and a second processor. Two Intel Xeon connectors are standard on the blade board to support installation of a second processor. High-speed, PC2100 DDR SDRAM is synchronized for up to 400 MHz processor-to-memory subsystem performance with current processors. There are four memory DIMM connectors; due to two-way interleaving, installation of memory options in pairs is required. Current memory options available are 256 MB, 512 MB and 1 GB size DIMMs, which support a minimum of 512 MB and a maximum of 4 GB of system memory. In the future, IBM will release a 2 GB memory option which will see the maximum system memory double from 4 GB to 8 GB.

Figure 1-4 on page 6 shows the BladeCenter HS20 with its top cover removed.

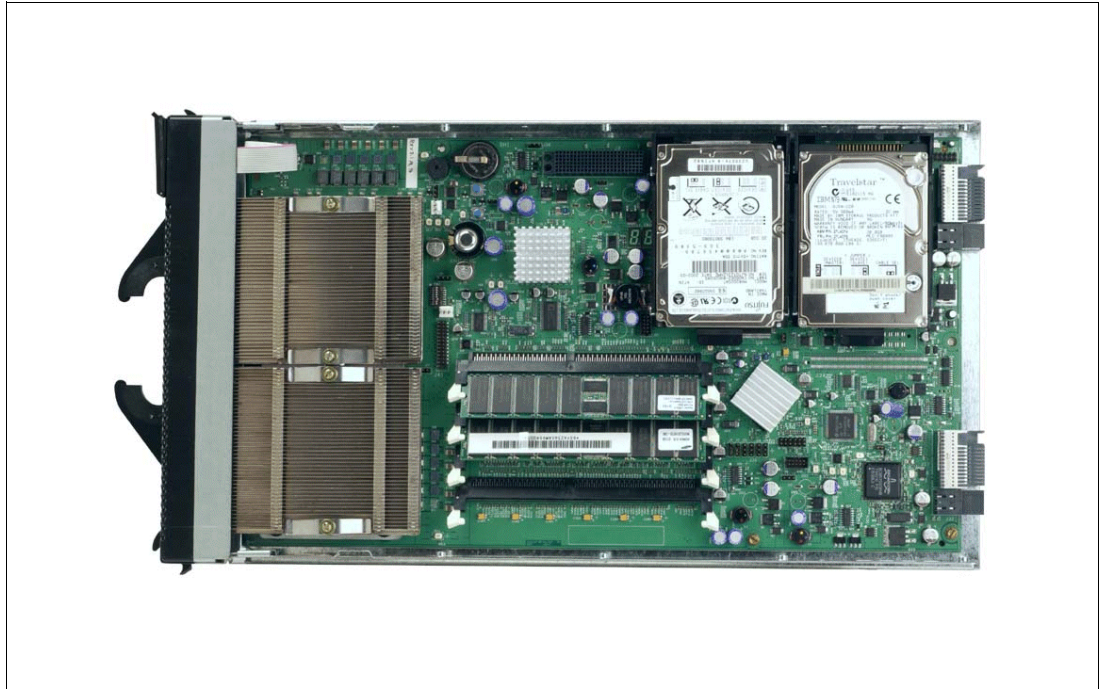


Figure 1-4 BladeCenter HS20 with top cover removed

Each BladeCenter HS20 has an integrated service processor on-board that communicates with the BladeCenter Management Module to enable blade server management remotely (see 1.2.3, “BladeCenter Management Module” on page 8 for more details on the management module). The service processor provides the following functions:

- ▶ Loader and OS Watch Timer
- ▶ Remote soft shutdown
- ▶ POST Watchdog Timer
- ▶ Light Path support
- ▶ VPD support
- ▶ PFA for VRM/CPU/Memory/HD
- ▶ Numeric based Error log
- ▶ ASM interconnect support (RS485)
- ▶ Environmental querying and alerts (TEMP/Voltages)
- ▶ Automatic Server Restart
- ▶ Remote Power On/Off
- ▶ In-band support for UMS/Director
- ▶ I2C interface to core logic (CSB5 chip)
- ▶ Local Environmental Monitoring
- ▶ Local LED control
- ▶ RS-485 interface to the Management Modules

The BladeCenter HS20 also has two integrated Ethernet controllers for redundancy. If redundancy is required, you must install Ethernet switch modules in switch module bays 1 and 2 (see 1.2.6, “BladeCenter 4-Port Ethernet Switch Module” on page 12 for more details).

Each controller is auto-sensing and will connect at the appropriate rate, even if the transfer rate is 10 Mbps, 100 Mbps or 1000 Mbps. The controller will also set the appropriate duplex state.

The Ethernet controller is capable of providing several teaming options that increase throughput and fault tolerance. In your blade server, a team consists of the two Ethernet controllers to utilize the options below:

- Adapter fault tolerance (AFT)** Provides automatic redundancy for your Ethernet controllers. You can configure either one of the integrated Ethernet controllers as the primary Ethernet controller. If the primary link fails, the secondary controller takes over. When the primary link is restored to an operational state, the Ethernet traffic switches back to the primary Ethernet controller.
- Adaptive load balancing (ALB)** Enables you to balance the transmission data flow among the two controllers. ALB also includes the AFT option. You can use ALB with any 100BASE-TX/1000BASE-T switch.
- Cisco Fast EtherChannel (FEC)** Creates a team of two controllers to increase transmission and reception throughput. FEC also includes the AFT option. You can use FEC only with a switch that has FEC capability.

The BladeCenter HS20 has a control panel which is located at the top of the blade servers, as shown in Figure 1-5.

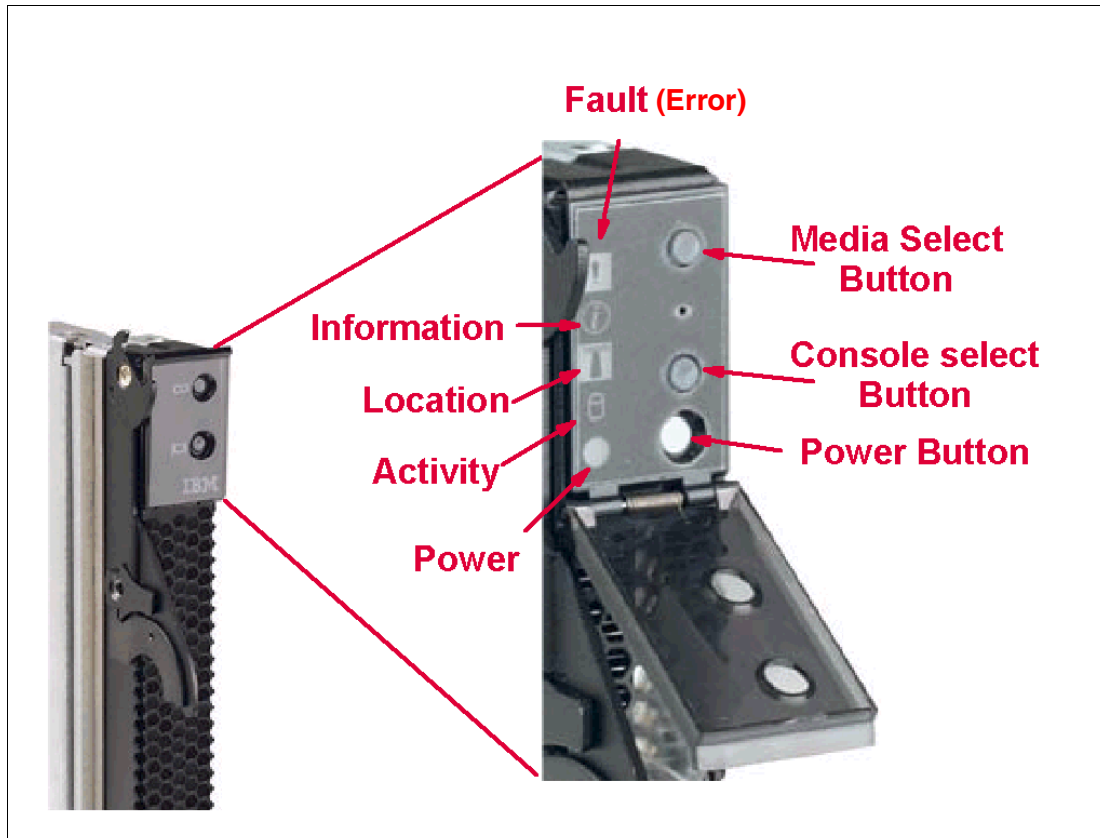


Figure 1-5 Blade server operators panel

Like the IBM @server BladeCenter's media tray, this control panel also has system information LEDs. The only difference is that the blade's panel also has control switches, which are detailed below.

<b>Media-select button</b>	Press this button to associate the CD-ROM drive, diskette drive, and USB port with this blade server. This button lights when the ownership of the CD-ROM drive, diskette drive, and USB port transfers to this blade server.
<b>Blade-error</b>	This LED is also known as the blade system-error LED. When this amber LED is on, it indicates a system error has occurred in the blade.
<b>Information</b>	When this amber LED is on, it indicates information about a system error for this server has been placed in the BladeCenter System Error log.
<b>Location</b>	This blue LED is turned on in response to a programmed condition, or remotely by the system administrator, to aid in blade identification for maintenance. The location LED on the IBM @server BladeCenter will be on also. Turn off the location LED after maintenance is complete.
<b>Activity</b>	When this green LED is on, it indicates that there is activity in the blade server; this includes hard disk and network activity.
<b>Power-on</b>	While the IBM @server BladeCenter has AC power, this green LED turns on and stays on when you turn on your blade server.
<b>Console select button</b>	Press this button to associate the keyboard, mouse, and video ports with this blade server. This button lights when the ownership of the keyboard, mouse, and video transfers to this blade server.
<b>Power-control button</b>	This button is located behind the control panel door. Press this button to manually turn the blade server on or off.

**Note:** The power-control button only has effect if the local power control option is enabled via the Management Module.

### 1.2.3 BladeCenter Management Module

The BladeCenter Management Module's primary function is to provide systems management for your IBM @server BladeCenter and blade servers, but it does have other important functions such as multiplexing the keyboard/video/mouse (KVM) to provide a local console for the individual blade servers and configuring the BladeCenter unit and switch modules. The management module communicates with all of the key components of the IBM @server BladeCenter including the switch, power and blower modules, as well as the blade servers themselves. The management module detects the presence, absence and condition of each of these components. A picture of the BladeCenter Management Module is shown in Figure 1-6 on page 9.

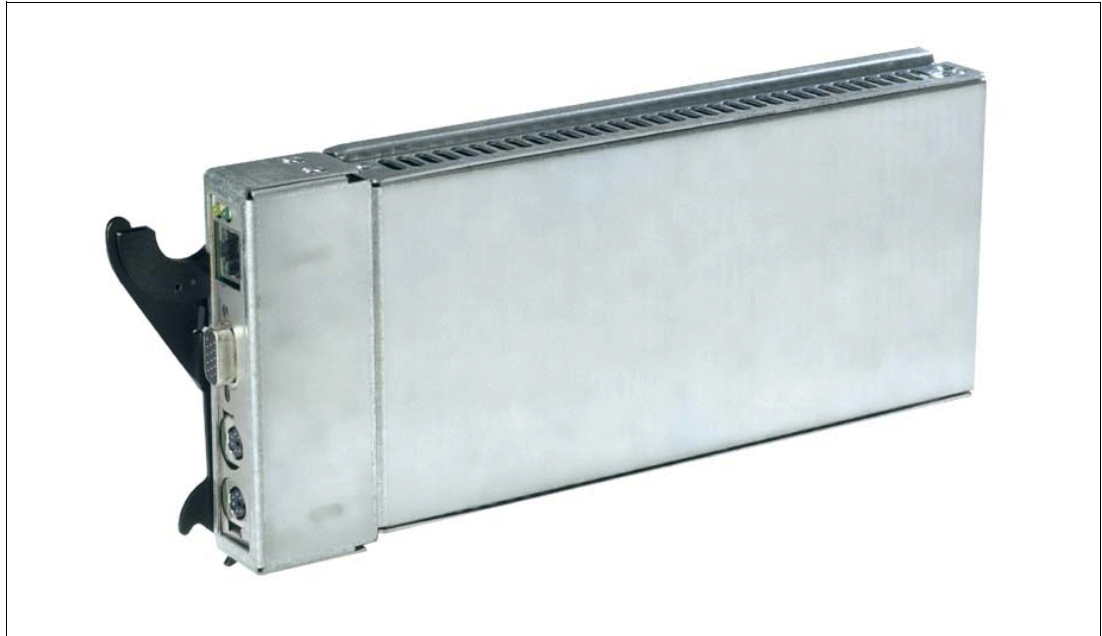


Figure 1-6 BladeCenter Management Module

The Management Module has a standard RJ45 connector for a 10/100MB Ethernet remote console connection, as well as two PS/2 connectors for keyboard, mouse and a 15-pin D-shell connector for video which are provided for the local console. Although the connectors for the keyboard and mouse are PS/2 type connectors, these devices are routed to a USB bus, enabling them to be switched between blades.

**Note:** The operating system in each blade must provide USB support for the blade server to recognize and make use of the keyboard and mouse.

The Management Module will retrieve and monitor critical information about the chassis and blade servers such as temperature, voltages, power supply, memory, fan and HDD status; this information will then be fed into an error and status log.

The manageability functions of the IBM @server BladeCenter are accessible via a Web GUI that is contained in the management module. This GUI allows you to view the status of, and control each blade server, which includes shutting down and restarting.

## 1.2.4 BladeCenter 1200W Power Supply Module

The standard BladeCenter chassis will ship with two 1200W Power Supply Modules, but, depending on the configuration of your IBM @server BladeCenter, you may require all four power modules. The standard two power modules provide power for the following components:

- ▶ Blade slots 1 through 6
- ▶ Blowers
- ▶ Management modules
- ▶ Switch modules
- ▶ Media tray



Figure 1-7 BladeCenter 1200W Power Supply Module

Power Modules 3 and 4 are required to provide power to blade slots 7 to 14. Figure 1-8 on page 11 shows how power is distributed by each power module. One power module is capable of providing enough power in the event of a power module failure. Power module 2 provides redundancy for power module 1 and power module 4 does the same for power module 3, although these power modules will effectively share the load under normal operating conditions. Supported configurations require either two or four power supplies, which is why when you order the optional BladeCenter 1200W Power Supply Module kit, you will receive two of the power modules.

**Important:** Nonredundant power is not supported in BladeCenter products. Power modules must always be present in power bays 1 and 2. When any blade server or option is in blade bay 7 through 14, power modules must be present in power bays 1 and 2, as well as in power bays 3 and 4. If a power module fails or an ac power failure occurs, BladeCenter units configured for redundant power operation, as described in this document, will operate in a nonredundant mode, and the blower modules will run at full speed. You must replace the failing power module or restore ac power as soon as possible to regain redundant power operation and to reset the blower modules to their normal operating speed.

### BladeCenter power module upgrade guidelines

This section contains information that will help you determine whether you need to upgrade the power modules in your IBM @server BladeCenter unit when installing IBM @server BladeCenter HS20 blade servers.

As of the date of this printing, three BladeCenter power-module options are available: IBM BladeCenter 1200W Power Supply Module (part number 48P7052), IBM BladeCenter 1200W to 1400W Power Supply Upgrade Kit (part number 90P0197), and IBM BladeCenter 1800W Power Supply Module (part number 13N0570). Go to <http://www.ibm.com/pc/compat/> for information about ordering these options. Obtain and use the Technical Update with your BladeCenter and blade server documentation for future reference.

The Technical Update can be obtained from the following URLs:

<http://www-1.ibm.com/support/docview.wss?uid=psg1MIGR-53353>

[ftp://ftp.software.ibm.com/pc/pccbbs/pc\\_servers\\_pdf/13n0308.pdf](ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/13n0308.pdf)

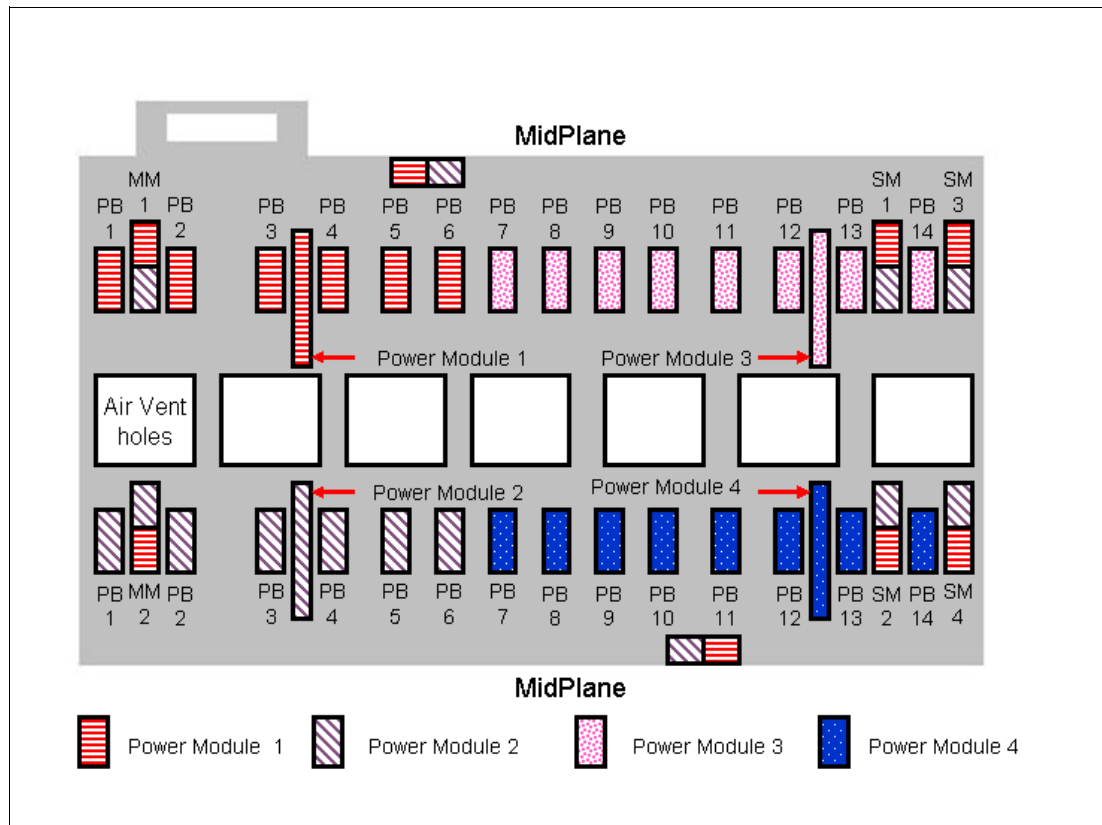


Figure 1-8 MidPlane power connector

## 1.2.5 BladeCenter blowers

The IBM *@server* BladeCenter ships with both hot-swap blowers which are required to provide adequate cooling; these blowers provide a total airflow of approximately 325 CFM; however, each blower will run at approximately 50% under normal conditions. If one blower fails, the other blower is capable of providing enough cooling for the entire chassis. However, the failed blower should be replaced within 48 hours. The speed of the blowers is controlled via the Management Module which receives signals from thermal monitors located in critical locations. There are two scenarios which will cause both blowers to function at full speed:

- ▶ The management module fails and the redundant module is not present.
- ▶ One of the power supply modules fails.

In Figure 1-9 on page 12, you can see that there are four fins which are currently closed since the blower is not operational. When operational, the blower draws the air from the front to the rear. Each blower also has an LED which will light up in the event of an error.



Figure 1-9 BladeCenter Blower Module

### 1.2.6 BladeCenter 4-Port Ethernet Switch Module

The Ethernet Switch Module (Figure 1-10 on page 13) has several purposes; in addition to providing network connectivity for the IBM @server BladeCenter and blades, it also provide interconnectivity between the blades and management modules. The Ethernet switch module does not come standard with the IBM @server BladeCenter; it is available for purchase as an option but it is required in most cases and should be installed in switch bay 1. This module is a fully functional Ethernet switch which has four 1000 Mbps ports externally, two internal 10/100 Mbps links to the management modules and fourteen 1000 Mbps links to the blades, which are also internal. Two of these switch modules can be added for redundancy. The switch module is configured via the Management Module.





Figure 1-10 BladeCenter 4-Port Ethernet Switch Module

In Figure 1-10, the two LEDs at the top of the switch module indicate power-on and Ethernet switch errors. There are also LEDs next to each port which indicate Ethernet link and activity.

### 1.2.7 BladeCenter Layer 2-7 GbE Switch Module

The Ethernet switch module (Figure 1-11 on page 14) has several purposes. In addition to providing network connectivity for the BladeCenter unit and blade servers, it also provides interconnectivity between the blades and management modules. The Layer 2-7 GbE Switch Module does not come standard with the IBM *eServer* BladeCenter. It is available for purchase as an option, but it is required in most cases and should be installed in switch bay 1. This module is a fully functional Ethernet switch that has four 1000 Mbps ports externally, two internal 10/100 Mbps links to the Management Modules and 14 1000 Mbps links to the blades, which are also internal. Two of these switch modules can be added for redundancy. The switch module is configured via the Management Module. For a more in-depth look at Layer 2-7 Switching, refer to the Redpaper IBM *eServer BladeCenter Layer 2-7 Network Switching*, REDP3755.



*Figure 1-11 BladeCenter 4-port Ethernet Switch Module*

In Figure 1-11, the two LEDs at the top of the switch module indicate power-on and Ethernet switch error. There are also LEDs next to each port that indicate Ethernet link and activity.

### **1.2.8 BladeCenter 2-Port Fibre Channel Switch Module**

If you require Fibre Channel connectivity for your IBM @server BladeCenter, there are two things you are required to do:

1. Install the IBM HS20 Fibre Channel Expansion Card in each blade that requires an FC connection.
2. Install one BladeCenter 2-Port Fibre Channel Switch Module (Figure 1-12 on page 15) in switch bay 3. If redundancy is required, a FC switch module must be installed in switch bay 4.

Each port on the FC switch module is capable of supporting transmission speeds of either 1 or 2 Gbps and must auto-negotiate to match the speed of any connected devices. A Small Form factor Pluggable (SFP) transceiver is required to populate these ports; these SFP transceivers are hot pluggable. The FC switch module is also managed through the Management Module.



Figure 1-12 BladeCenter 2-Port Fibre Channel Switch Module

The storage options for the IBM @server BladeCenter are covered in Chapter 3, “Storage options for the BladeCenter” of the Redpaper *The Cutting Edge: IBM @server BladeCenter*, REDP3581.

## 1.2.9 BladeCenter Acoustic Attenuation Module

In environments where it is important to minimize sound emissions, there is a noise reduction option available that can be installed on the rear of the IBM @server BladeCenter. This option is called the BladeCenter Acoustic Attenuation Module (acoustic module or muffler). The acoustical noise emissions for a single BladeCenter unit configured with 14 IBM @server BladeCenter HS20 servers are:

- ▶ 7.4 bels (operating)
- ▶ 7.4 bels (idling)

The acoustical noise emissions for a single BladeCenter unit with a BladeCenter Acoustic Attenuation Module option installed and configured with 14 IBM @server BladeCenter HS20 servers are:

- ▶ 6.9 bels (operating)
- ▶ 6.9 bels (idling)

For visibility purposes, the system LEDs on the rear of the BladeCenter unit have been replicated on the acoustic module, as these are covered when this option is fitted. The acoustic module also fully covers the blower modules and partly covers the other modules installed.

**Note:** The BladeCenter Acoustic Attenuation Module requires approximately eight inches between the rear of the IBM @server BladeCenter and the rack door. For this reason, the NetBay 42 Enterprise Rack Cabinet should be used when installing the IBM @server BladeCenter with this option.

## 1.3 The advantages of IBM eServer BladeCenter

Unlike typical server architecture which scales up, the BladeCenter allows for the scale out approach, yet balances performance and density. In this section, we identify the advantages of the BladeCenter for your business, such as:

- ▶ Systems management
- ▶ High density computing
- ▶ Redundancy

### 1.3.1 Systems management

The systems management component for the BladeCenter is the combination of IBM Director, the Web interface and Rapid Deployment Manager (RDM). With these tools, you can reduce system outages, increase IT personnel productivity and reduce support costs.

#### **IBM Director**

IBM Director is a comprehensive workgroup hardware manager designed for use with IBM @server xSeries servers, PCs, notebooks and now IBM @server BladeCenter.

IBM Director provides a comprehensive view of the xSeries servers.

- ▶ Remote access to the server regardless of its status
- ▶ Resetting or cycling of the server
- ▶ Server inventory, AssetID, blade slot numbers utilized
- ▶ Monitoring and setting thresholds on the server events, including PFA
- ▶ Flash BIOS
- ▶ Monitoring and identifying potential performance bottlenecks

IBM Director allows you to reduce system outages, increase IT personnel productivity and reduce support costs.

These goals can be accomplished by:

- ▶ Monitoring server health
- ▶ PFA - Predictive Failure Analysis®
- ▶ Integration with enterprise system management environments

#### ***Monitoring server health***

By setting thresholds on components within IBM Director, you can monitor the following:

- ▶ Operating system load
- ▶ POST time-out
- ▶ Voltage
- ▶ Temperature

#### ***PFA - Predictive Failure Analysis***

Setting alerts on disk, memory and processors via PFA allows you to identify imminent component failure. PFA can monitor the following:

- ▶ Processors
- ▶ Memory

- ▶ Fans
- ▶ Power supplies
- ▶ SCSI HDDs

### ***Integration with enterprise system management environments***

IBM Director agents should be installed on each of the blade servers as this allows system management of the blades and also provides the advanced management capabilities of the xSeries servers to be accessed from such products as:

- ▶ Tivoli® Enterprise™ and Tivoli Netview
- ▶ Computer Associates CA Unicenter TNG
- ▶ HP OpenView
- ▶ Microsoft® SMS
- ▶ BMC Patrol
- ▶ NetIQ

This is an important consideration for organizations who have already spent time, money and resources on existing system management tools.

### **Web interface**

The Web interface allows you to configure and remotely manage your IBM @server BladeCenter via a browser; this is built into the management module.

Supported browsers and required components are:

- ▶ Microsoft Internet Explorer 4.0 Service Pack 1, or later
- ▶ Netscape Navigator 4.72, or later (version 6.0 is not supported)
- ▶ Java-enabled Web browser
- ▶ Support for JavaScript 1.2 or later
- ▶ HTTP 1.0, or later
- ▶ Minimum display resolution 800\*600 pixels and 256 colors

**Note:** The Web interface does not support double-byte character set languages (DBCS).

The Management Module Ethernet port either receives a DHCP assigned address within two minutes of connecting to the LAN or it defaults to the following IP address 192.168.70.125 with a subnet address of 255.255.255.0. The default hostname is MMxxxxxxxxxxxx where xxxxxxxxxxxx is the MAC address.

**Note:** If multiple IBM @server BladeCenters are to be configured, only one can be assigned the default IP address of 92.168.70.125, otherwise IP address conflicts will occur.

If your DHCP server is not on the same subnet as the BladeCenter Management Module console, DHCP traffic needs to be allowed to traverse the router to the Management Module console to receive an DHCP assigned address, or IBM Director Server needs to be on the same subnet as the IBM @server BladeCenter.

The Web interface allows you to manage and check the status of each of the modules and blade servers. Below is a list of the functions and sub-functions available.

- ▶ Monitor
  - System status
  - Event log
  - Vital product data
- ▶ Blade Tasks
  - Power/restart
  - Firmware update
  - Configuration
- ▶ Switch tasks
  - Power/restart
  - Management
- ▶ MM console (Management Module)
  - General settings
  - Login profiles
  - Alerts
  - Network interface
  - Network protocols
  - Security
  - Configuration file
  - Firewall update
  - Restore defaults
  - Reset MM
- ▶ Log off

### **RDM - Rapid Deployment Manager**

This powerful tool allows you to deploy system images to the blade servers from the administrator's console.

RDM supports the following environments:

- ▶ Windows® 2000
- ▶ Windows 2000 Advanced Server

The advantages of Rapid Deployment Manager are:

- ▶ Rapid deployment of Operating System image to the destination server
- ▶ Hot-spare blade option: see “Hot-spare blades” on page 22.

## **1.3.2 High density computing**

As data centers have grown with the proliferation of Wintel servers over recent years, it is important to note that rack space and floor space can be more efficiently taken up with the use of blade servers. A fully populated 42U rack is capable of holding six IBM @server BladeCenters and 84 dual processor blade servers, for a total of 168 CPUs per rack. This is

twice the current density of a non-blade server. The IBM eServer BladeCenter supports a minimum of one 4 port 1 GB Ethernet switch for up to fourteen blade servers. A total of four switch modules can be utilized within the IBM eServer BladeCenter. This can be a combination of either Fiber Channel or Ethernet.

We recommend the use of blade servers for the following situations:

- ▶ Space constrained environments
- ▶ WebSphere
- ▶ Linux clusters
- ▶ Web caching
- ▶ Collaboration applications (Lotus Notes®, Microsoft Exchange and Citrix)
- ▶ Dynamic Web serving - Load balancing
- ▶ Firewall
- ▶ Telecommunications
- ▶ Active directory services
- ▶ Scientific and technical computing

These applications are typically processor and memory intensive, and so lend themselves to the scale out option rather than the scale up option. The scale out option is where the strength of the IBM eServer BladeCenter becomes obvious. Due to the highly scalable range of components available with the BladeCenter unit, the blade server has a huge market.

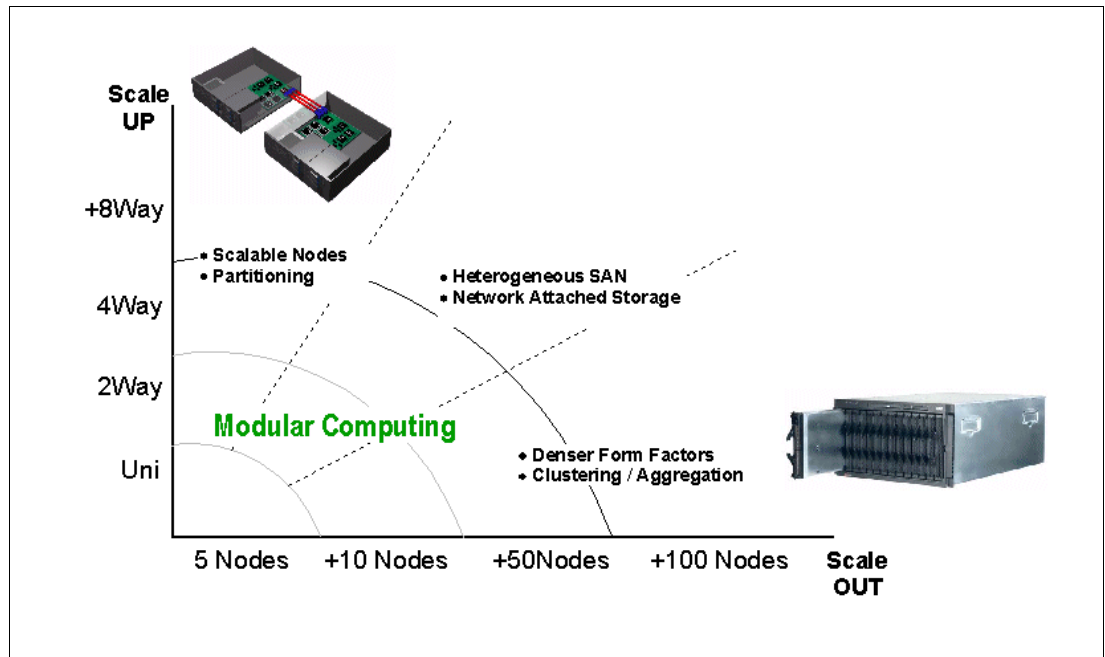


Figure 1-13 Scale up versus scale out

Attractive cost savings are also possible where a large number of rack installed servers are required. These savings run from power usage, to hardware procurement (due to not duplicating components), through to server management. Table 1-1 on page 20 demonstrates the input voltage required for different servers providing the same number of

CPUs. It also shows the heat output in BTUs, which can affect the cooling of your computer room and other equipment within the computer room.

Table 1-1 Power and BTU usage

	Number of Servers	Processor	Maximum load watts	BTU
IBM x330 4MX	14	Pentium® III 1.4GHz	3080	10502
IBM x335	14	Xeon 2.4GHz	4760	16231
IBM x342 - Dual Power	14	Pentium III 1.4GHz	5250	19821
IBM x345 - Dual Power	14	Xeon 2.4GHz	7000	23870
IBM @server BladeCenter	14	Xeon 2.4GHz	2500	8530

**Note:** The IBM @server BladeCenter in Table 1-1 is utilizing the onboard IDE controller.

Deploying an IBM @server BladeCenter is far simpler than deploying 14 1U servers and the associated cables. A single IBM @server BladeCenter only requires a KVM cable, one power cable, one Ethernet cable and a single system management cable. Even with a redundancy of these components, cabling can be reduced by eighty-three percent (see Table 1-2 for a typical example).

Table 1-2 Cable utilization

	1U Solution (2 - 42U Racks)	IBM @server BladeCenter Solution (2 - 42U Racks)
Power	84	12
Ethernet	168	48
KVM	84	6 (ACT)
Switch	6 (boxes)	1 (ACT)
KVM interconnect	5	0
Management connect	84	6
Total	431	73

The IBM @server BladeCenter is not intended to replace any of the xSeries suite of products, but rather to provide additional configuration options.

### 1.3.3 Redundancy

We all know failures occur occasionally; we also know that redundancy of key components increases system availability. Although previously, it was expensive to purchase redundant options for individual servers, the high availability features found in conventional xSeries rack servers have also been included within IBM @server BladeCenter. These features include:

- ▶ Hot-spare blades
- ▶ Processor
- ▶ Memory protection



- ▶ Disk mirroring
- ▶ MidPlane
- ▶ Hot-swap power and cooling modules
- ▶ Switch modules

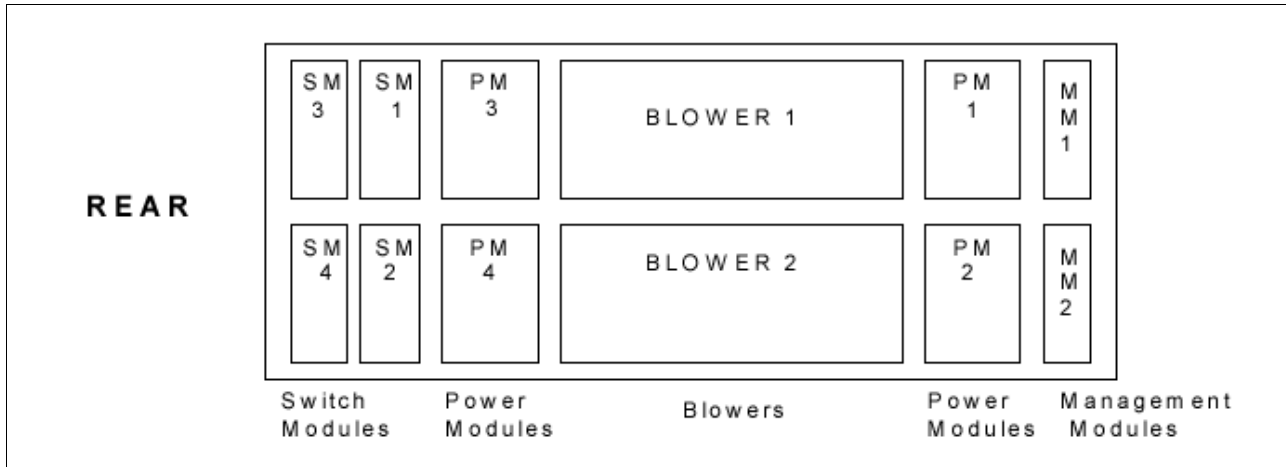


Figure 1-14 Module location on the rear of the IBM eServer BladeCenter

Table 1-3 outlines which components can be redundant, hot swap, PFA or have Light Path diagnostics.

Table 1-3 Redundant, Hot-swap, PFA or Light Path

	Redundant	Hot Swap	PFA	Light Path
<b>Blade</b>	Yes	Yes	No	Yes
<b>Processor</b>	Auto Recovery	No	Yes	Yes
<b>Memory</b>	ECC w/Auto down size	No/Tool less	Yes	Yes
<b>Power Supplies</b>	Yes	Yes	Yes	Yes
<b>Cooling Fans</b>	Yes	Yes	Yes	Yes
<b>Management Module</b>	TBD	TBD	TBD	TBD
<b>Switch Module</b>	Yes	Yes	TBD	TBD
<b>Backplane</b>	Yes	No	No	No
<b>Front Plane /Media Tray</b>	No	Yes	No	No
<b>CD ROM Drive</b>	No	No	No	No
<b>Floppy Drive</b>	No	No	No	No
<b>Hard Drive</b>	Raid	Only with Blade Storage expansion (HS SCSI drives)	Yes	Yes
<b>Power Cable</b>	Yes	Yes	No	No

## Hot-spare blades

MidPlane supports hot-spare blade servers; this operates in the same fashion as the hot-spare drive. By creating events within IBM Director, you can deploy an operating system to a hot-spare blade server automatically.

## Processor

In a dual processor blade server, if a CPU fails, the following steps are taken by the system.

1. Force failed processor offline
2. Automatically re-boot server
3. Generate alerts
4. Continue operating with the working processor

## Memory

There are four memory slots; memory must be installed in matching pairs. The following redundancy options are available:

- ▶ Chipkill™ ECC - provides correction for up to 4 bits per DIMM
- ▶ Memory hardware scrubbing - corrects soft memory errors automatically
- ▶ PFA - Creates alerts of imminent failure

## Disk mirroring

Refer to Chapter 3, “Storage options for the BladeCenter” of the Redpaper *The Cutting Edge: IBM @server BladeCenter*, REDP3581 for hardware and software mirroring options of IDE and SCSI disks.

## MidPlane

The middle plane provides connectivity between the blades and the modules at the rear of the BladeCenter unit. There are two connections on each blade server to independent middle planes for redundancy.

## Hot-swap power and cooling modules

By sharing fans, power supplies, cables and other components within a BladeCenter unit and installing the redundant options for these, your organization can reduce the number of points of potential failure, thus increasing system availability.

## Blowers

Two hot-swap blowers are standard in the IBM @server BladeCenter; the blower speed varies depending on the temperature. A failed blower needs to be replaced within 48 hours.

**Note:** An Acoustic Attenuation Module can be fitted to reduce noise.

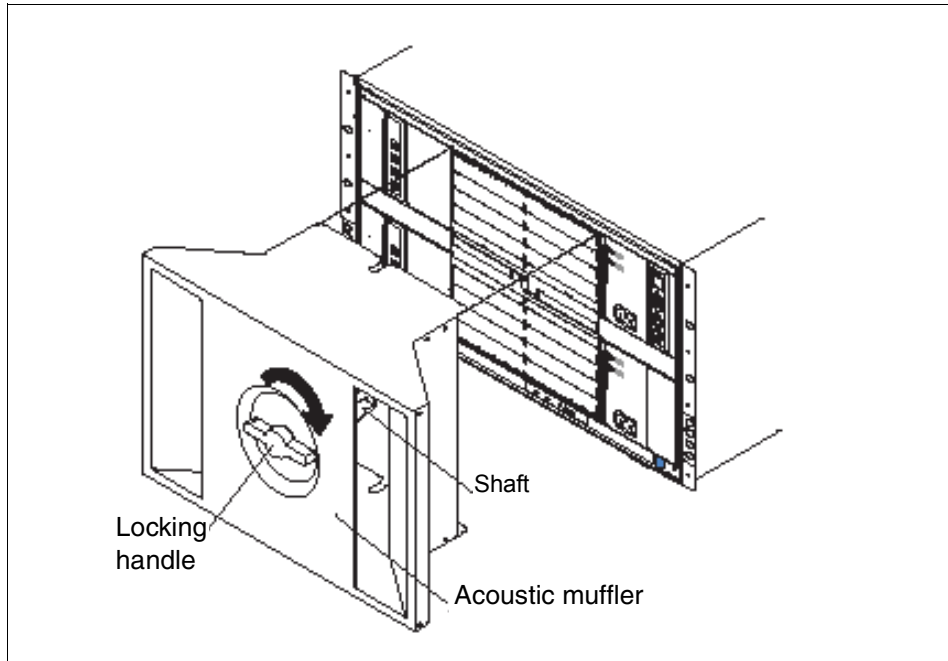


Figure 1-15 Acoustic Attenuation Module

### Power

The IBM @server BladeCenter comes with two 220 volt 1200 watt hot-swap power modules in power bays 1 and 2. Table 1-4 outlines the power module bays and their functions.

Table 1-4 Power module bays

Power module bays	Power module function
1	Provides power to all the BladeCenter modules in server bay slots 1-6.
2	Redundancy for Power module bay 1.
3	Provides power to all the BladeCenter modules in server bay slots 7-14.
4	Redundancy for Power module bay 3.

**Note:** A blade server in bay 6 with a SCSI storage expansion option requires a power module in power module bays 3 and 4 to support the SCSI storage expansion.

### Cabling modules

The IBM @server BladeCenter is capable of managing four switch modules of either Ethernet or Fibre, the minimum requirement being a single Ethernet switch.

**Ethernet**

Two hot-swap 1 GB Ethernet four port switch models can be installed in switch module bays 1 and 2.

**Fibre**

Two hot-swap Fibre channel network interface switch modules can be placed in switch module bays 3 and 4.

**Note:** The IBM @server BladeCenter also includes a hot-swap media tray, which includes the CD-ROM and floppy drive.



## Samba

Samba is an implementation of a Server Message Block (SMB) protocol server that can be run on almost every variant of UNIX® in existence. Samba is an open source project, just like Linux. Since the code is written in C, it is easily portable to all flavors of UNIX. Samba is a tool which allows UNIX systems to peacefully coexist with Windows systems by performing file and print sharing using the NetBIOS protocol. It allows UNIX systems to move into a Windows “Network Neighborhood” without causing problems. With Samba, UNIX servers act like any other Windows server, offering their resources to the SMB clients. SMB was renamed by Microsoft to Common Internet File System (CIFS) when the protocol was updated for Windows NT®.

## 2.1 What is Samba?

Samba is a suite of programs that work together to allow UNIX systems to access server file systems and printers via the Server Message Block (SMB) protocol. The two key programs are `smbd` and `nmbd`. These two programs implement the four basic modern-day CIFS servers:

- ▶ File and print services
- ▶ Authentication and authorization
- ▶ Name resolution
- ▶ Service announcement (browsing)

The `smbd` program, the SMB Daemon, handles file and print services and share mode and user mode authentication and authorization. The name resolution and browsing parts are handled by `nmbd`.

The other programs in the suite are utilities. The most commonly used of these are:

- ▶ `smbclient`  
A simple FTP-like SMB client. It is used to access SMB shares on other compatible servers and to allow a submission of print jobs to a printer attached to any SMB server.
- ▶ `nmblookup`  
A NetBIOS name service client. It can be used to find NetBIOS names and look up the IP address of systems.
- ▶ `smbstatus`  
A tool for accessing information about the current connections to `smbd`.
- ▶ `smbpasswd`  
A tool for changing LanMan and Windows NT passwords on Samba and Windows NT servers.
- ▶ SWAT  
The Samba Web Administration Tool allows the configuration of Samba using a Web browser.

## 2.2 What can you do with Samba?

The Samba Linux server:

- ▶ Can act as a file/print server for Windows networks. It can replace an expensive Windows NT file/print server in this role, creating a less expensive solution.
- ▶ Can act as a NetBIOS name server (NBNS) in a Windows world, where it is referred to as WINS - Windows Internet Name Service.
- ▶ Can participate in NetBIOS browsing and master browser elections.
- ▶ Can provide a gateway for synchronizing UNIX and Windows NT passwords.

With the utilities in the Samba suite:

- ▶ You can access any shared directory or printer on Windows NT servers or Samba servers and allow UNIX machines to access Windows NT files.
- ▶ You can mount any share from a Windows NT server or Samba server in your directory structure (this is available only on Linux using Samba File System, SMBFS).
- ▶ You can look up an NetBIOS names, map them to IP address, and check the status of the systems.







## Installation of Red Hat Linux 7.3 and IBM Director Agent

In this chapter, we will describe in detail the basic installation of Red Hat Linux 7.3, SuSE Linux Enterprise Server 8 (SLES 8), and IBM Director Agent on an IBM @server BladeCenter system.

## 3.1 Installation of Red Hat Linux 7.3

We will discuss three methods of installing Red Hat Linux on a BladeCenter system.

- ▶ CD installation
- ▶ Network installation
- ▶ PXE boot installation

The only difference between these is the means used to start the install. Once the installation process is started, everything else is the same.

## 3.2 CD installation

This is the most direct and simplest method of installing Red Hat on a blade server. Since the HS20 blade server uses USB CD-ROM, you must make a special boot disk with USB support.

### 3.2.1 Creating the boot disk

Download the diskette image from:

<http://people.redhat.com/msw/boot-usb-sleep-7.3.img>

The diskette can be created on a Windows or Linux system. Using a Windows system, copy the rawrite utility for DOS on Red Hat Install CD 1 in \dosutils\ to the hard drive. In a command prompt, run **rawrite** and type in image name and diskette later when prompted. Using a Linux system, run **dd if=boot-usb-sleep-7.3.img of=/dev/fd0**.

### 3.2.2 Installing Red Hat 7.3

In this section, we will install Red Hat on an IBM @server BladeCenter HS20 server. Perform the following steps:

1. Insert the boot diskette into the diskette drive and Red Hat Install CD 1 into the CD-ROM.
2. Power on the blade server and press the **Media Select** and **Console Select** buttons on the blade server.

**Note:** Do not switch the KVM from the blade server until the installation has proceeded to install the packages after the About to Install window appears, otherwise the mouse will lose functionality.

3. At the Welcome to Red Hat Linux Version 7.3 window, press **Enter**.

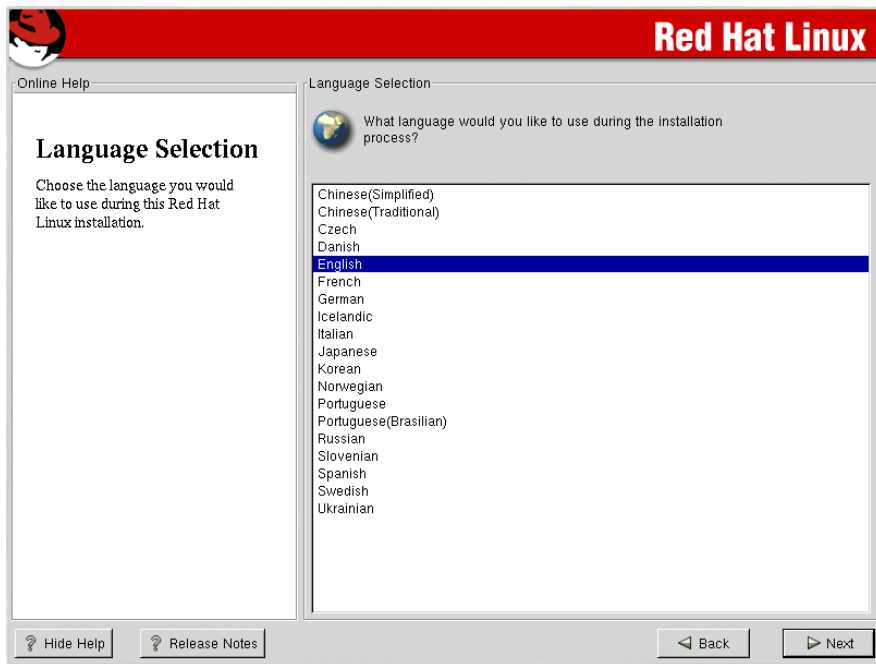


Figure 3-1 Language Selection

4. Select **English** and click **Next**.

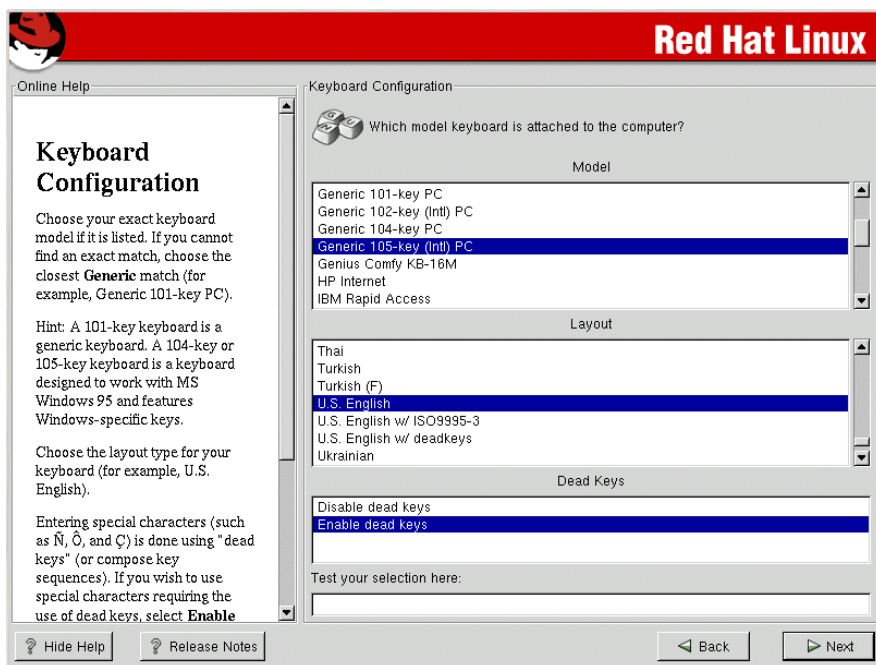


Figure 3-2 Keyboard Selection and Configuration

5. Select the auto selected **Generic 105-Keyboard**, **US English**, **Enable dead keys**, and click **Next**.

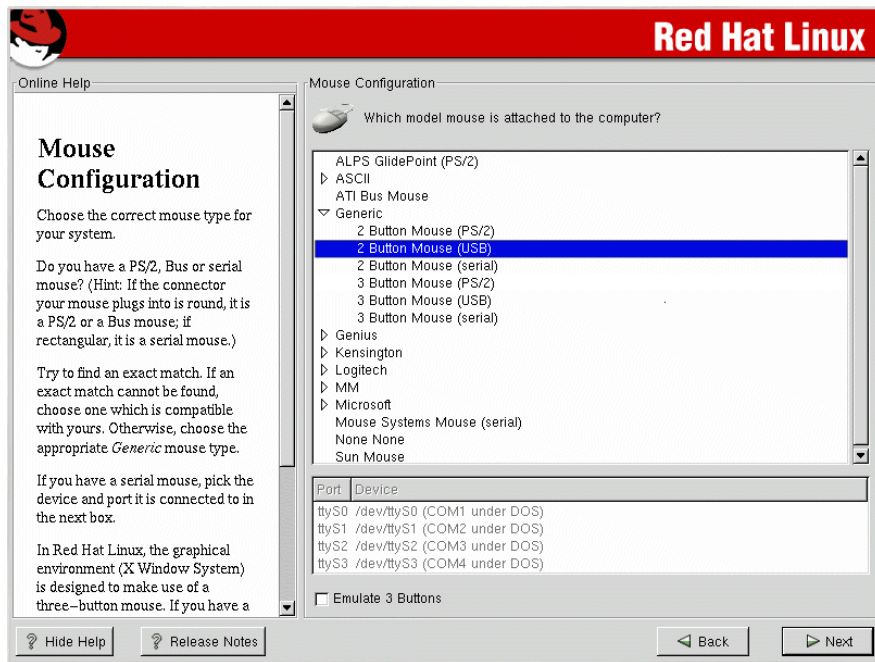


Figure 3-3 Mouse Selection

6. Select **2 Button Mouse (USB)** and click **Next**.

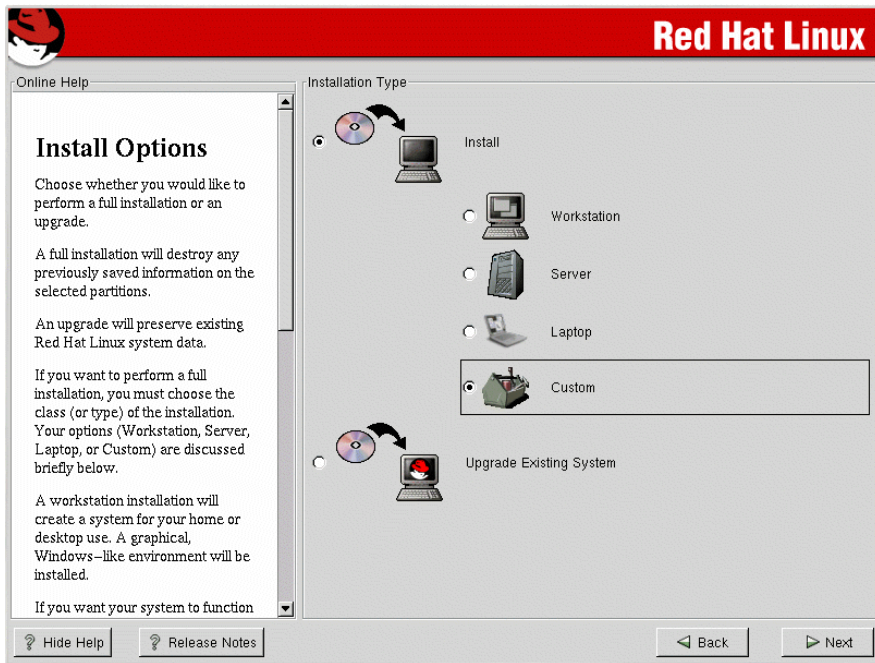


Figure 3-4 Install Options

7. Select **Install, Custom**, and click **Next**.

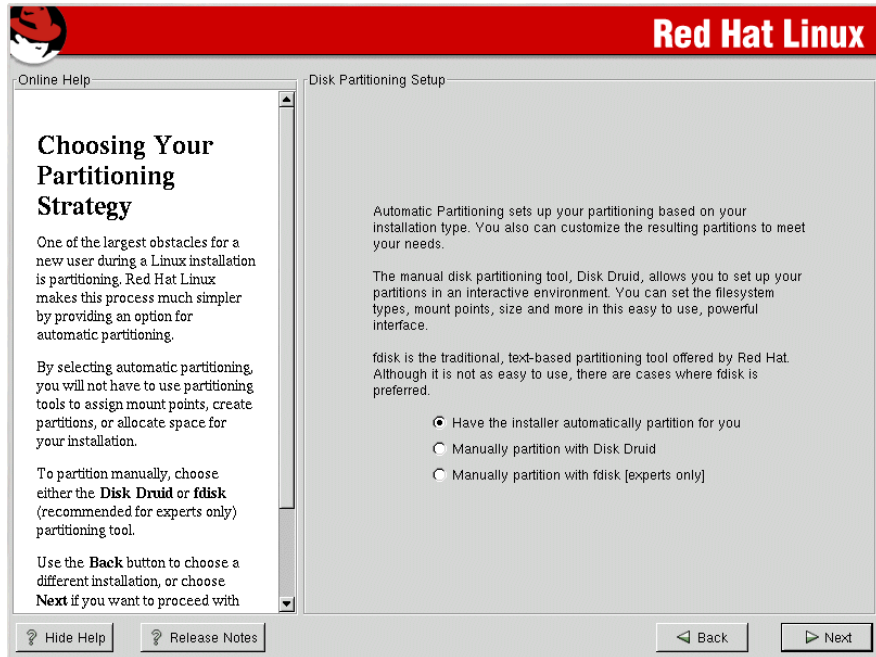


Figure 3-5 Disk Partitioning

8. Partition the hard drive using either the automatic partition (default choice) or manually. See:

<http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-diskpartsetup.html>

for more information about partitioning the hard drive.

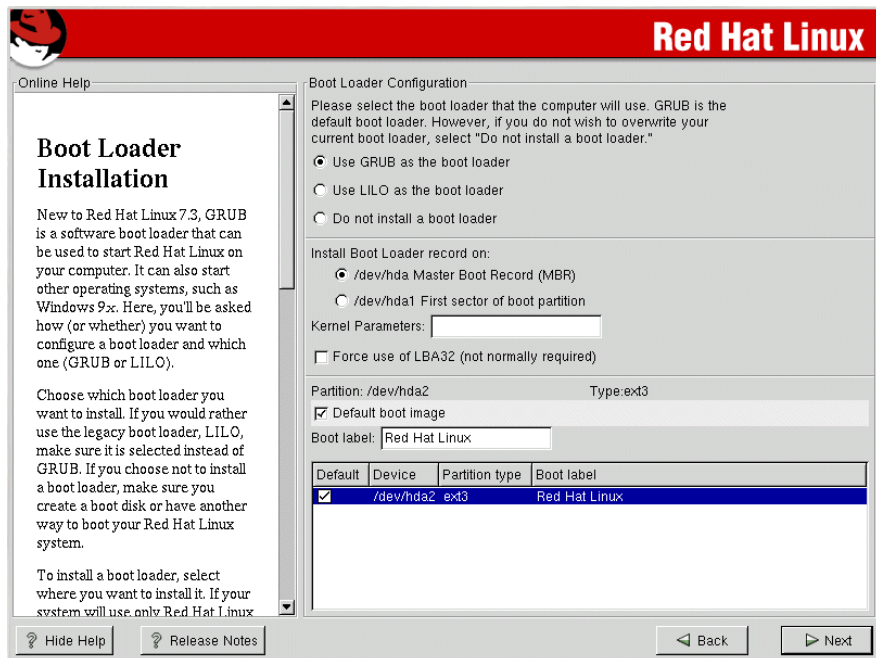


Figure 3-6 Boot loader options

9. Select **Use GRUB as the boot loader, /dev/hda Master Boot Record (MBR), Default boot image**, and click **Next**.

10. Do not select **Use a GRUB Password**; click **Next**.

11. On eth0 page, deselect **Activate on boot**, click the **eth1** tab, select **Configure using DHCP**, select **Activate on boot**, and click **Next**.

12. Follow the Red Hat Linux 7.3 install instructions at:

<http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-firewallconfig.html>

to finish the install setup process.



Figure 3-7 Boot Disk Creation.

13. Select **Skip boot disk creation** and click **Next**.

A boot diskette can be created with `mkbootdisk` after the diskette drive is defined, as shown in Step 17 on page 35.

14. Follow the Red Hat Linux 7.3 install instructions at:

<http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-xconfig.html>

to finish the install. We selected the following software groups.

- Printing Support
- Classic XWindow System
- X Window System
- GNOME
- KDE
- Network Support
- Network Managed Workstation

- Utilities
- Software Development
- Kernel Source

15. After the system is rebooted, log in as root.

16. If X11 is installed, edit `/etc/X11/XF86Config-4`:

- a. Add
 

```
Section "ServerFlags"
AllowMouseOpenFail
EndSection
```

to the top of the file

- b. Save and exit.

17. The diskette drive is connected to the SCSI bus. It is configured to take the last ID on the SCSI bus. Since the blade server we are using has no SCSI hard drives, the diskette drive resides on `/dev/sda`. So we perform these steps to make the diskette drive available.

- a. Edit `/etc/fstab` and add

```
/dev/sda/mnt/floppyauto,auto0 0
```

after all hard drive entries.

- b. Make the `/mnt/floppy` directory by running `mkdir /mnt/floppy`

- c. Mount the drive by running `mount /dev/sda /mnt/floppy`

18. Make a boot disk by running `mkbootdisk` and following the prompts.

19. Update the Ethernet drivers by editing `/etc/modules` so the entries for `eth0` and `eth1` look like what is shown in Example 3-1.

*Example 3-1 /etc/modules showing correct Ethernet drivers*

---

```
alias parport_lowlevel parport_pc
alias eth0 bcm5700
alias eth1 bcm5700
```

---

### 3.2.3 Applying updates and installing the latest kernel

In this section, we will apply updates and install the latest kernel to Red Hat. Perform the following steps:

1. Log on to the system as root.
2. Make a directory to store the updates in a file system which has at least 600 MB of free space. We created `/usr/updates` to store the updates.
3. Change to the updates directory.
4. Create `kernels` and `noInstall` directories.
5. Download all the current Red Hat 7.3 updates:
  - a. Anonymous ftp to `updates.redhat.com`
  - b. `cd` to `7.3/en/os`
  - c. Download all the files in the `i386`, `i686`, and `noarch` directories
6. Move all the kernel files into the `kernels` directory by typing: `mv kernel-* kernels`

7. Move the i386 rpms that are replaced by i686 rpms into the noInstall directory using the following command sequence:
 

```
for i in $(ls *.i686.rpm); do mv ${i/i686.rpm/i386.rpm} noInstall; done
```
8. Install the updates by typing `rpm -Fvh *.rpm`.
9. Install the kernel updates by
  - a. Using `rpm -ivh kernels/kernel-2.4.18-18.7.x.i686.rpm` to install the uni processor kernel.
  - b. Using `rpm -ivh kernels/kernel-smp-2.4.18-18.7.x.i686.rpm` to install the smp kernel.
  - c. Using `rpm -Fvh kernels/kernel-source-2.4.18-18.7.x.i386.rpm` to install the latest kernel source, if it is already installed.
  - d. Editing `/boot/grub/grub.conf`, changing `default=2` to `default=0`, and saving.
10. Reboot the system using the command `shutdown -r 0`.
11. Verify that the system boots without any errors.

## 3.3 Network installation

Network installation is useful when you are installing multiple systems and do not want to have several copies of installation CDs. The system requirements for a Linux install server are:

1. 2 GB of free disk space
2. Network card
3. Anonymous ftpd or NFS service

This can be installed on a Linux system that satisfies requirements 1 and 2 above.

### 3.3.1 Setting up the NFS install server

A desktop system with enough free hard drive space was selected to be the install server. We transformed it into the install server by performing these steps.

1. Install `nfs-utils` rpm.
2. Create the `/var/iso/RedHat` directory.
3. Download Red Hat Linux 7.3 install iso images 1 through 3 and the md5 file.
  - `rh-7.3-en-i386-cd1.iso`
  - `rh-7.3-en-i386-cd2.iso`
  - `rh-7.3-en-i386-cd3.iso`
  - `rh-7.3-en-i386.md5`

*Example 3-2 Output of md5sum check*

---

```
[root@portall iso]# md5sum -c rh-7.3-en-i386.md5
rh-7.3-en-i386-cd1.iso: OK
rh-7.3-en-i386-cd2.iso: OK
rh-7.3-en-i386-cd3.iso: OK
md5sum: rh-7.3-en-i386-cd4.iso: No such file or directory
rh-7.3-en-i386-cd4.iso: FAILED open or read
md5sum: rh-7.3-en-i386-cd5.iso: No such file or directory
rh-7.3-en-i386-cd5.iso: FAILED open or read
```



```
md5sum: rh-7.3-en-i386-cd6.iso: No such file or directory
rh-7.3-en-i386-cd6.iso: FAILED open or read
md5sum: WARNING: 3 of 6 listed files could not be read
```

---

4. Check the files using **md5sum -c rh-7.3-en-i386.md5**.

If any of the files are corrupt, delete those and download again. The output should be similar to that shown in Example 3-2 on page 36.

5. Check that other has read and execute permissions on `/var/iso/RedHat` and has read permission on all the iso files.
6. Edit `/etc/export` and add `/var/iso/RedHat *(ro)` to the end of the file.
7. Make NFS reload the export file using **service nfs reload**.

### 3.3.2 Setting up the FTP install server

A desktop system with enough free hard drive space was selected to be the install server. We transformed it into the install server by performing these steps.

1. Install the `anonftp rpm` package.
2. Create the `/var/iso` directory.
3. Download Red Hat Linux 7.3 install iso images 1 through 3 and the md5 file.
  - `rh-7.3-en-i386-cd1.iso`
  - `rh-7.3-en-i386-cd2.iso`
  - `rh-7.3-en-i386-cd3.iso`
  - `rh-7.3-en-i386.md5`

*Example 3-3 Output of md5sum check*

---

```
[root@portall iso]# md5sum -c rh-7.3-en-i386.md5
rh-7.3-en-i386-cd1.iso: OK
rh-7.3-en-i386-cd2.iso: OK
rh-7.3-en-i386-cd3.iso: OK
md5sum: rh-7.3-en-i386-cd4.iso: No such file or directory
rh-7.3-en-i386-cd4.iso: FAILED open or read
md5sum: rh-7.3-en-i386-cd5.iso: No such file or directory
rh-7.3-en-i386-cd5.iso: FAILED open or read
md5sum: rh-7.3-en-i386-cd6.iso: No such file or directory
rh-7.3-en-i386-cd6.iso: FAILED open or read
md5sum: WARNING: 3 of 6 listed files could not be read
```

---

4. Check the files using **md5sum -c rh-7.3-en-i386.md5**.

If any of the files are corrupt, delete and download again. The output should be similar to the output shown in Example 3-3.

5. Create `7.3`, `7.3/cd1`, `7.3/cd2`, `7.3/cd3`, `7.3/RedHat`, `7.3/RedHat/RPMS` directories in `/var/ftp/pub`.

*Example 3-4 Mounting iso images*

---

```
mount -o loop,ro -t iso9660 /var/iso/rh-7.3-en-i386-cd1.iso /var/ftp/pub/cd1
mount -o loop,ro -t iso9660 /var/iso/rh-7.3-en-i386-cd2.iso /var/ftp/pub/cd2
mount -o loop,ro -t iso9660 /var/iso/rh-7.3-en-i386-cd3.iso /var/ftp/pub/cd3
```

---

6. Mount the three install iso images to the cd directories.
7. Change to the directory `/var/ftp/pub/7.3`.

- Copy all the files in `cd1/RedHat/base` into `RedHat/base` using `cp -r cd1/RedHat/base/RedHat`.
- Make symbolic links for in the rpm files in `RedHat/RPMS` directory on `cd1`, `cd2`, and `cd3` in `/var/ftp/pub/RedHat/RPMS`.

*Example 3-5 Creating symbolic links*

---

```
cd RedHat/RPMS
ln -s ../../cd1/RedHat/RPMS/*.rpm .
ln -s ../../cd2/RedHat/RPMS/*.rpm .
ln -s ../../cd3/RedHat/RPMS/*.rpm .
```

---

- Configure the FTP server to start on reboot using the command:

```
chkconfig wu-ftpd on
```

- Start the FTP server with the command:

```
service xinetd restart
```

*Example 3-6 Restarting xinetd*

---

```
[root@portall etc]# service xinetd restart
Stopping xinetd:          [ OK ]
Starting xinetd:         [ OK ]
```

---

- Verify that the FTP server is working by connecting to the system using an FTP client and logging in as anonymous.

*Example 3-7 Testing anonymous FTP setup*

---

```
[root]# ncftp 9.24.105.99
NcFTP 3.1.3 (Mar 27, 2002) by Mike Gleason (ncftp@ncftp.com).
```

```
Copyright (c) 1992-2002 by Mike Gleason.
All rights reserved.
```

```
Connecting to 9.24.105.99...
portall FTP server (Version wu-2.6.2-5) ready.
Logging in...
The response 'NcFTP@' is not valid
Next time please use your e-mail address as your password
  for example: joe@blade4.itso.ral.ibm.com
Guest login ok, access restrictions apply.
Logged in to portall.
ncftp / >
```

---

### 3.3.3 Creating the network boot diskette

To perform a network installation on the IBM @server BladeCenter, a modified version of the normal Red Hat network boot diskette, which includes the drivers for the blade server Ethernet adapters, has to be created.

- Install the `kernel-BOOT-2.4.18-3.i386.rpm` package from the Red Hat Linux CD 2 or from the Red Hat FTP site using `rpm -ivh kernel-BOOT-2.4.18-3.i386.rpm`.

2. Create a temporary work directory for all the files and two directories for mounting images by executing the commands:
  - mkdir /tmp/newboot
  - mkdir /mnt/loop0
  - mkdir /mnt/loop1
3. Copy the bootnet.img file from the images directory on Red Hat Linux CD1 to the work directory just created, cp /mnt/cdrom/images/bootnet.img /tmp/newboot.
4. Change to the working directory, cd /tmp/newboot.
5. Mount this image using the loopback device using **mount -o loop /tmp/newboot/bootnet.img /mnt/loop0**.
6. Copy the initrd.img file to the work directory and add .gz extension to the end by executing `cp /mnt/loop0/initrd.img ./initrd.img.gz`.
7. Unzip initrd.img.gz by executing **gunzip initrd.img.gz**.
8. Mount this RAMdisk image using **mount -o loop initrd.img /mnt/loop1**.
9. Copy the module-info and pcitable files to the working directory by executing:
  - cp /mnt/loop1/modules/module-info
  - cp /mnt/loop1/modules/pcitable
10. Edit module-info and add the lines in Example 3-8 to the bottom.

*Example 3-8 Lines added to module-info*

---

```
bcm5700
    eth
    "Broadcom BCM5700 10/100/1000 Ethernet adapter"
    line_speed "Line speed"
```

---

11. Save and close the file.
12. Edit the file pcitable and add the lines in Example 3-9 the bottom:

*Example 3-9 Lines added to pcitable*

---

```
0x14e4 0x1644 "bcm5700" "BROADCOM Corporation|NetXtreme BCM5700 Gigabit Ethernet"
0x14e4 0x1645 "bcm5700" "BROADCOM Corporation|NetXtreme BCM5701 Gigabit Ethernet"
0x14e4 0x1646 "bcm5700" "BROADCOM Corporation|NetXtreme BCM5702 Gigabit Ethernet"
0x14e4 0x1647 "bcm5700" "BROADCOM Corporation|NetXtreme BCM5703 Gigabit Ethernet"
0x14e4 0x164d "bcm5700" "BROADCOM Corporation|NetXtreme BCM5702FE Gigabit Ethernet"
0x14e4 0x16a6 "bcm5700" "BROADCOM Corporation|NetXtreme BCM5702X Gigabit Ethernet"
0x14e4 0x16a7 "bcm5700" "BROADCOM Corporation|NetXtreme BCM5703X Gigabit Ethernet"
```

---

13. Save and close the file.
14. Copy these files over the original ones in the RAMdisk image by executing:
  - cp -f module-info /mnt/loop1/modules
  - cp -f pcitable /mnt/loop1/modules
15. Copy the modules.cgz file to the working directory and add the .gz extension to the end by executing `cp /mnt/loop1/modules/modules.cgz ./modules.cpio.gz`.
16. Unzip the file using **gunzip modules.cpio.gz**.
17. Make a directory named 2.4.18-3BOOT using **mkdir 2.4.18-3BOOT**.

18. Copy into this directory the bcm5700 module, installed on the system in step 1, by executing:

```
cp /lib/modules/2.4.18-3B00T/kernel/drivers/addon/bcm5700/bcm5700.o \  
./2.4.18-3B00T/
```

19. Add this driver to the modules.cpio file by executing:

```
ls 2.4.18-3B00T/* | cpio -o --append -H crc -F modules.cpio
```

20. Zip the modules.cpio file using **gzip modules.cpio**.

21. Copy this file over the original in the mounted RAMdisk by executing **cp -f modules.cpio.gz /mnt/loop1/modules/modules.cgz**.

22. Unmount the RAMdisk using **umount /mnt/loop1**.

23. Zip the RAMdisk by executing **gzip initrd.img**.

24. Copy the RAMdisk to the mounted boot diskette image by running **cp -f initrd.img.gz /mnt/loop0/initrd.img**.

25. Unmount the boot diskette image using **umount /mnt/loop0**.

26. Create a boot diskette from this image by placing a diskette into the floppy drive and executing **dd if=bootnet.img of=/dev/fd0**.

This install diskette is used to perform the network-based installations described in the next two sections.

### 3.3.4 Installing from the NFS server

In this section, we will install Red Hat Linux via the NFS server. Perform the following steps:

1. Insert the network install diskette created in 3.3.3, "Creating the network boot diskette" on page 38 into the IBM @server BladeCenter diskette drive.
2. Power on the blade server and press the **Media Select** and **Console Select** buttons on the blade server.

**Note:** Do not switch the KVM from the blade server until the installation has proceeded to install the packages after the About to Install window appears, otherwise the mouse will lose functionality.

3. Choose **English**.
4. Choose **us**.
5. Choose **NFS image**.
6. Choose the interface you want to use. In our case eth1 was connected to switch 1.
7. Accept the default **Use dynamic IP configuration (BOOTP/DHCP)**. Choose or type in the IP address, netmask, default gateway, and primary name server.

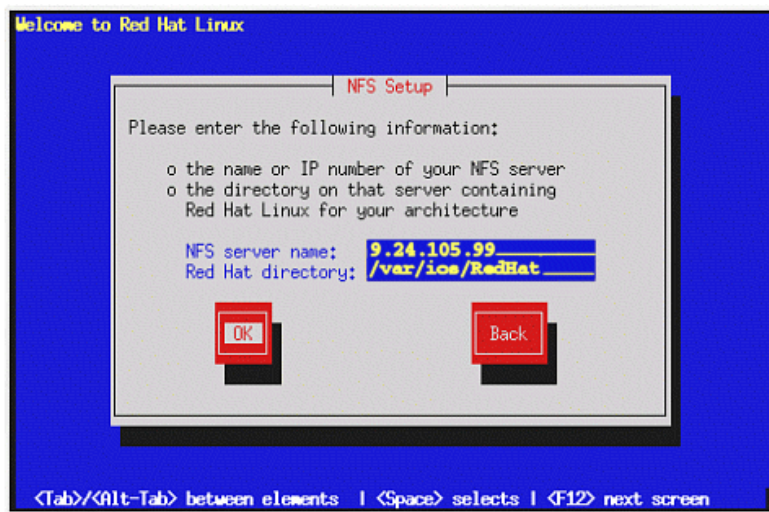


Figure 3-8 NFS install server settings

8. Type in the NFS sever IP address and the path to the iso files.

**Note:** If the server cannot be reached and DHCP has been used for the client configuration, choose **Back** and type in the TPC/IP info. Then try again from the server.

9. Follow the CD installation process from step 3 on page 30.

### 3.3.5 Installing a Linux operating system from the FTP server

In this section, we will install Red Hat Linux via the FTP server. Perform the following steps:

1. Insert the network install diskette created in 3.3.3, “Creating the network boot diskette” on page 38 into the IBM @server BladeCenter diskette drive.
2. Power on the blade server and press the **Media Select** and **Console Select** buttons on the blade server.

**Note:** Do not switch the KVM from the blade server until the installation has proceeded to install the packages after the About to Install window appears, otherwise the mouse will lose functionality.

3. Choose **English**.
4. Choose **us**.
5. Choose **FTP**.
6. Choose the interface you want to use. In our case eth1 was connected to switch 1.
7. Accept the default **Use dynamic IP configuration (BOOTP/DHCP)** or type in the IP address, netmask, default gateway, and primary name server.



Figure 3-9 FTP setup window

8. Type in the IP address of the FTP server and directory path to RedHat relative to /var/ftp.

**Note:** If the server cannot be reached and DHCP has been used for the client configuration, choose **Back** and type in the TPC/IP info. Then try again from the server.

9. Follow the CD installation process from step 3 on page 30.

## 3.4 PXE Boot installation

PXE stands for Pre eXecution Environment. This is a special function of modern network adaptors that allows execution of special pieces of code during the boot process. This is usually used to access files on other servers for booting itself; for example, you can download the Linux kernel from another server into memory and then boot this kernel.

This enables computers to boot without the need of any local disk. We will use this process to start the installation process without the need for diskettes and CD's. Once the blade server starts the installation process, it will be similar to the Network installation in the previous section.

### 3.4.1 Configuration of the PXE Boot server

We will use a boot server that contains the installation media and the necessary network services for the remote installation. The boot server will be an eServer BladeCenter HS20 server installed using the CD installation process.

1. First, complete the server setup steps for an NFS install server detailed in in 3.3, "Network installation" on page 36. In short, make sure you have a local copy of the Red Hat installation files and that these files are accessible using NFS. See section 3.3.1, "Setting up the NFS install server" on page 36 for details. Also make sure that the boot server has a static IP address.
2. Download or copy the DHCP server from the Red Hat CDs (the full name is dhcp-2.0pl5-8.i386.rpm).

3. Install the DHCP server using `rpm -ivh dhcp-2.0p15-8.i386.rpm`.
4. Copy the sample DHCP server configuration file to the /etc directory using `cp /usr/share/doc/dhcp-2.0p15/dhcpd.conf.sample /etc/dhcpd.conf`
5. Edit the /etc/dhcpd.conf file to make it look like Example 3-10.

*Example 3-10 /etc/dhcpd.conf file for PXE boot*

---

```

subnet 192.168.0.0 netmask 255.255.255.0 {
# --- default gateway
    option routers          192.168.0.1;
    option subnet-mask     255.255.255.0;

    option nis-domain      "itso.ral.ibm.com";
    option domain-name     "itso.ral.ibm.com";
    option domain-name-servers 192.168.0.1;

    option time-offset     -18000; # Eastern Standard Time

    option dhcp-class-identifier "PXEClient";
    option vendor-encapsulated-options ff;

    range dynamic-bootp 192.168.0.128 192.168.0.255;
    default-lease-time 21600;
    max-lease-time 43200;

}
}

```

---

Replace the IP addresses of the default gateway (option routers) and domain-name-servers, and the domain-names with the correct value for your network.

6. Start the DHCP server using `service dhcpd start`. If you want, test to verify that the DHCP server is working.
7. Download from the updates section on the Red Hat FTP site or any of its mirrors the latest version of the PXE package. In our case it is `pxe-0.1-31.99.7.3.i386.rpm`.
8. Install the PXE using `rpm -ivh pxe-0.1-31.99.7.3.i386.rpm`.
9. Add the following lines to the end of the /etc/services file:

*Example 3-11 Lines required in /etc/services for PXE boot*

---

```

mtftp      1759/udp
pxe        67/udp
pxe        4011/udp

```

---

10. Add the following lines to /etc/xinetd.conf before the includedir /etc/xinetd.d line:

*Example 3-12 Configuration of the PXE FTP server in /etc/xinetd.conf*

---

```

service mtftp
{
    socket_type = dgram
    wait = yes
    user = root
    server = /usr/sbin/in.mtftpd
    server_args = /tftpboot
}

```

---

11. Add the following lines to the end of the `/etc/rc.d/rc.local` file:

*Example 3-13 Commands in rc.local file needed for PXE boot*

---

```
route add -host 255.255.255.255 eth0
route add -net 224.0.0.0 netmask 224.0.0.0 eth0
```

---

12. Copy the Linux kernel and initial ramdisk file for PXE boot from the first CD to the TFTP install section. In our case, it looked like this:

*Example 3-14 Copying of Linux kernel and initrd for PXE boot*

---

```
cp /var/ftp/pub/7.3/cd1/images/pxeboot/vmlinuz /tftpboot/X86PC/UNDI/linux-install/linux.1
cp /var/ftp/pub/7.3/cd1/images/pxeboot/initrd-everything.img \
/tftpboot/X86PC/UNDI/linux-install/linux.2
```

---

13. Open the file `/etc/pxe.conf` in a editor and look for the lines in Example 3-15.

*Example 3-15 Default configuration of PXE daemon in /etc/pxe.conf*

---

```
[UseDHCPPort]
1
```

---

Change the 1 to a 0 and save this change.

14. Open the file `/etc/init.d/pxe` in an editor and look for the lines in Example 3-16.

*Example 3-16 Changes to /etc/init.d/pxe*

---

```
# Starts the pxe daemon
#
# chkconfig: - 56 54
```

---

Change the 56 to a 98. This will make the PXE daemon start after the DHCP daemon.

15. Set up the DHCP and PXE services so that they will start up at boot using the commands in Example 3-17.

*Example 3-17 Enabling dhcpd and pxe daemon at boot*

---

```
[root@portall root]# chkconfig dhcpd on
[root@portall root]# chkconfig pxe on
```

---

16. Now reboot the server using `shutdown -r now`.

17. In the messages displayed in the startup sequence, see if both the DHCP and the PXE daemon start without any error messages. You can also check in `/var/log/boot.log` for any errors.

Our PXE boot server is now ready for action.

## 3.4.2 Starting the installation

First we have to configure the blade server so that it will use PXE in its startup boot sequence.

1. Log in to the Web interface of the IBM @server BladeCenter management module.
2. Select **Blade Tasks -> Configuration**.
3. Click **Boot Sequence**.
4. Click the name of the blade server you want to edit.
5. Select **Network - PXE** as the first device, the rest is your personal setup.



6. Click **Save**.

To use PXE for the installation, press **F12** at the BIOS startup window when the different function keys are shown.

Now we will reboot the blade server so that the installation process can begin.

1. Log back in to the Web interface of the BladeCenter management module if you have logged out.
2. Click **Blade Tasks -> Power/Restart**.
3. Select the checkbox on the line of the blade server where you will perform the installation.
4. Click **Restart Blade**.
5. Press the **KVM Select** button on the front of the blade server to follow the installation process.

**Note:** Do not switch the KVM from the blade server until the installation has proceeded to install the packages after the About to Install window appears, otherwise the mouse will lose functionality.

We will now begin the actual installation process.

1. Follow the boot sequence of the blade server until you see the message Press F8 to view menu ....
2. Select the line **Remote Install Linux** and press **Enter**.
3. When you see the line Press any key to enter kernel parameters... press the **Enter** key twice. This will boot the kernel with the default parameters.
4. You should see some messages indicating that the kernel and the initrd are being downloaded and then the Linux kernel will boot.
5. Choose **English**.
6. Choose **us**.
7. Choose **NFS image**.
8. Choose the interface you want to use. In our case eth1 was connected to switch 1.
9. Accept the default **Use dynamic IP configuration (BOOTP/DHCP)** and choose or type in the IP address, netmask, default gateway, and primary name server.

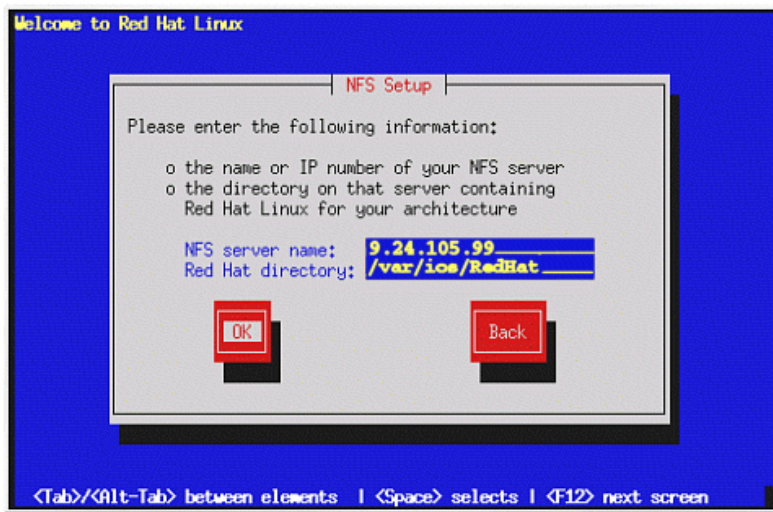


Figure 3-10 NFS install setup window

10. Type in the NFS sever IP address and the path to the iso files.

**Note:** If the server cannot be reached and DHCP has been used for the client configuration, choose **Back** and type in the TPC/IP info. Then try again from the server.

11. Follow the CD installation process from step 3 on page 30.

## 3.5 Installation of SuSE Linux Enterprise Server 8

In this section, we will discuss the installation of SuSE Linux Enterprise Server (SLES) version 8 for the IA-32 platform. We will only handle the CD-ROM installation. Information about the other methods of installing SLES 8 can be found in the SLES Installation guide.

1. Start the server and insert the SuSE Linux Enterprise Server 8 for IA-32 CD 1 into the CD-ROM drive.
2. At the boot options: prompt, press **Enter**. You see a bar stating Loading Linux kernel and when it reaches 100% the Linux kernel will boot.
3. When the installer is started, you get a dialog containing the end user license agreement. Press **Enter** to accept.

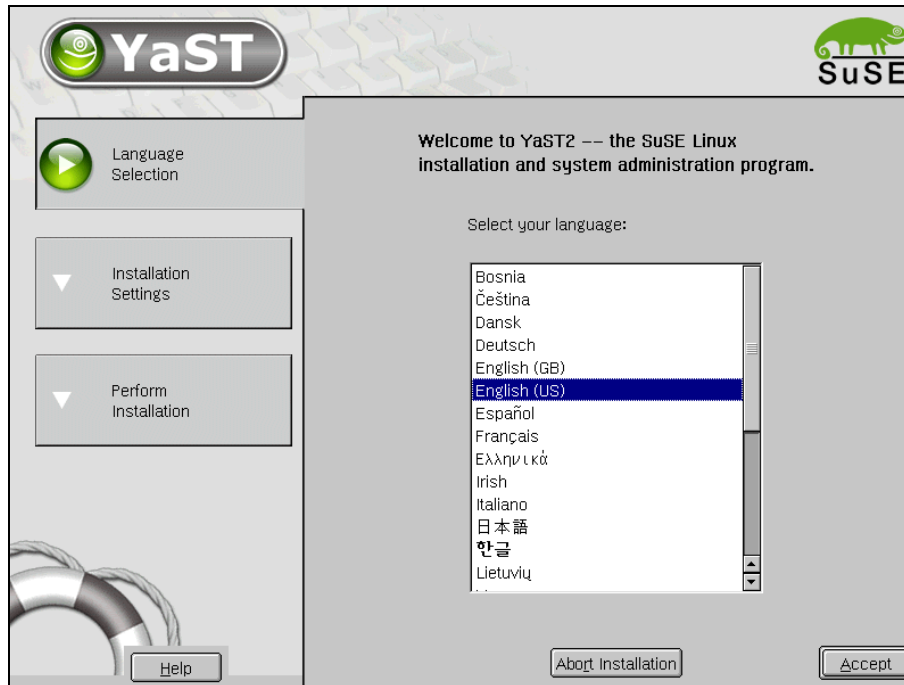


Figure 3-11 SLES Installation - Language selection

4. For the IBM *@server* BladeCenter HS20, the mouse will not work initially when the installer starts. Follow these directions:
  - a. Press **Alt + A** to select **English (US)**.
  - b. If the Please select dialog box appears, press **Alt + O** to select **New installation**.
  - c. Press **Alt + C** and scroll, with the arrow keys, to Mouse to change the mouse, then press **Enter**. Scroll down through the list to USB mouse and press **Alt + T**, Test, to ensure that it is working with your mouse. Click **Accept** when finished.
5. At the Installation Settings display, your settings are preselected for the installation that is specific to your system. You may not need to alter many of these settings, but make sure you do follow the instructions under the Boot section. Click **Accept** when finished:
  - **Mode**: Do not change this.
  - **Keyboard layout**: If the language is set correctly, in most cases the correct keyboard setting will be automatically selected. Click **Keyboard Layout** to modify the keyboard mapping, if needed. Select the keyboard layout from the list. You can check that it works properly by typing in the Keyboard test box. Click **Accept** when finished.

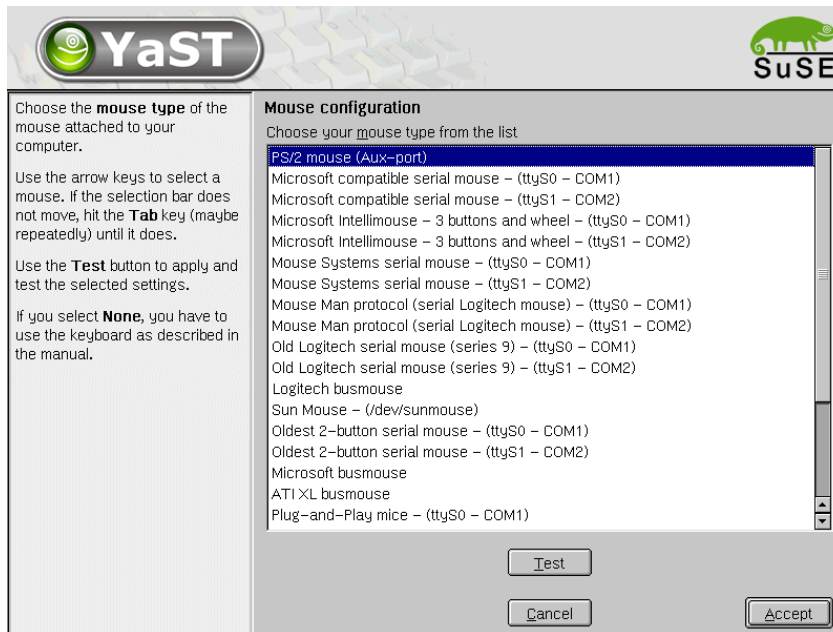


Figure 3-12 SLES Installation - Mouse Configuration

- **Mouse:** Click **Mouse** if you need to change the type of mouse you are using. Changing the mouse type is not necessary in most cases. Select the correct mouse from the list and click **Test** to ensure that it is working with your mouse. Click **Accept** when finished.
- **Partitioning:** Click **Partitioning** if you need to change the partitioning scheme for your drive(s). You will see YaST2's proposed partitioning scheme and can do one of the following:
  - Accept the suggestion, by clicking **Next**.

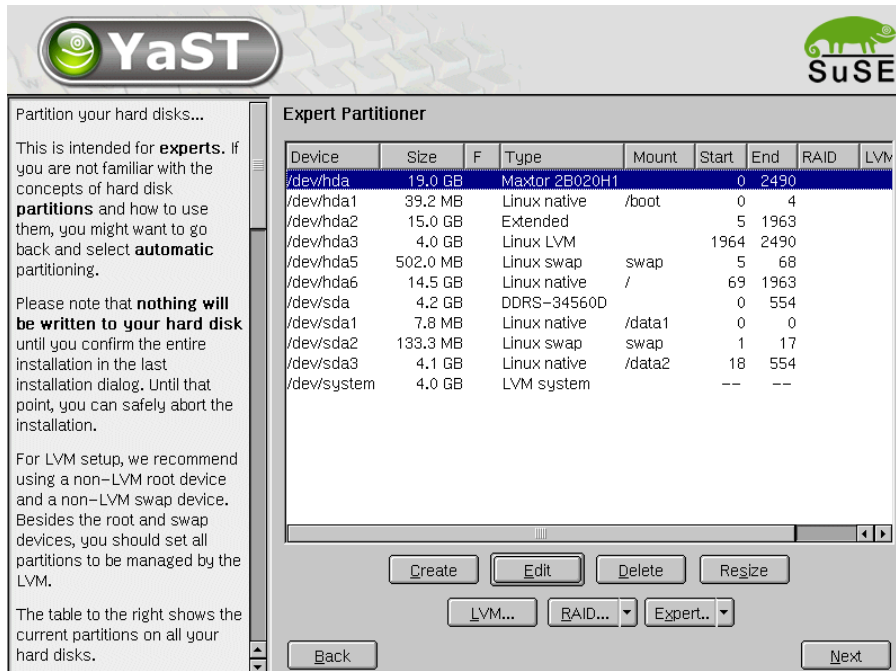


Figure 3-13 SLES Installation - Expert Partitioner

- Modify the proposal, by clicking **Base partition setup on this proposal** and then clicking **Next**.

The Expert Partitioner window opens, which allows you to view and manipulate the existing partitions on the hard drive(s).

Click **Create** to add new partitions, **Delete** to delete partitions (highlight partition you wish deleted first), **Edit** to make changes to existing partitions, and **Resize** to resize ext2, ext3, ReiserFS, XFS, and swap partitions.

When finished, select **Next**.

- Discard the proposal, by clicking **Create custom partition setup** and clicking **Next**. This will bring you to the Preparing Hard Disk - Step 1 window, where you can:

Select the hard disk where you want to install SuSE Linux Enterprise Server 8. Click **Next**. Depending on the current state of the hard disk, you will have the opportunity to erase the complete hard disk, delete certain partitions or install SLES 8 on the free space currently available on the disk.

Or you can click **Custom partitioning -- for experts** and then click **Next**. This will bring you to the Expert Partitioner window as mentioned previously.

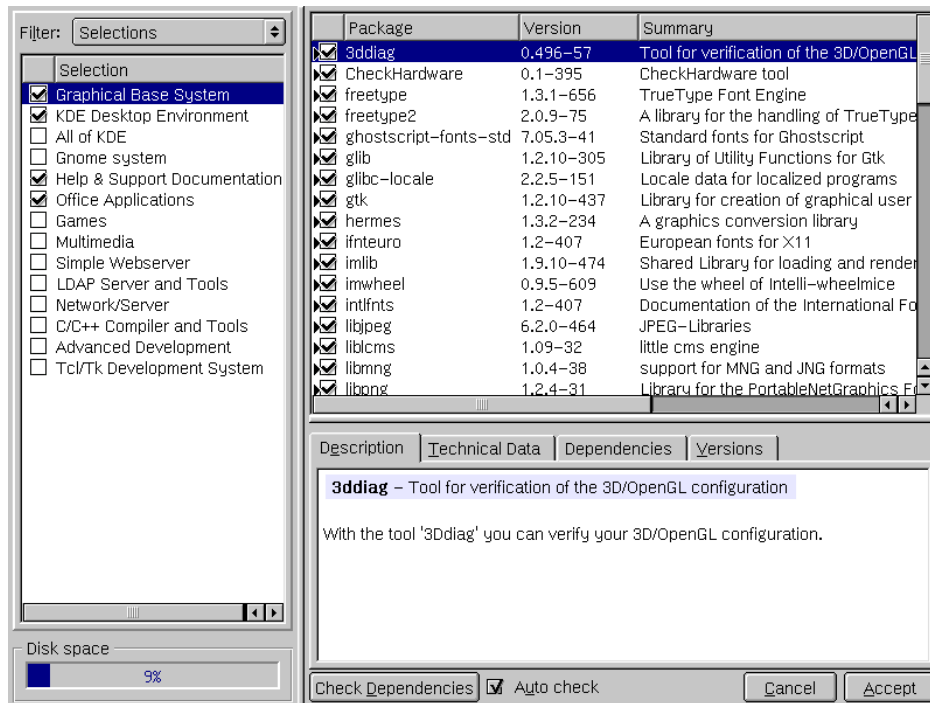


Figure 3-14 SLES Installation - Software packages installation

- **Software:** Click **Software** to change the default software configuration. The default configuration installs most basic networking, administrative, and development tools needed. In the Software Selection window, select the software configuration you want. Click **Accept** after you have chosen the software you want.

For a specialized selection, click **Detailed selection**. You can then select specific software using the package tool. When finished, click **Accept**.

- **Bootng:** Click **Bootng** and make sure that **Write GRUB to the boot disk ('MBR on <device>')** is selected. Add the parameter `acpi=olddbboot` under the Kernel boot.

- **Time zone:** Click **Time zone** to modify the default time zone for the installation. Select the correct time zone from the list. Under the Hardware clock set to section, select either local time or UTC, as appropriate. Click **Accept**.
  - **Language:** Click **Language** to modify the default language for the installation. Select the needed language from the list and click **Accept**.
6. If all Installation Settings are to your preference, click **Accept** and click **Yes, install** at the Warning window.
  7. You will be asked to insert the 'UnitedLinux Version 1.0' CD 1. Do so and click **OK**.
  8. Later in the installation process, you will be asked to insert additional CDs to finish installing the packages. You will need the 'UnitedLinux Version 1.0' CD 2 and the 'SuSE SLES Version 8' CD1.
  9. When all packages are installed, the installer will run some post installation scripts and then reboot into the final installer section on the hard disk. Remove any CDs from the CD-ROM drive as the prompt indicates and press **Enter**.

**Note:** In our case, the mouse did not work in the next steps of the installation process. We had to use keyboard navigation.

10. At the *Password for 'root', the system administrator* window, type the administrative password that you want twice and click **Next**.

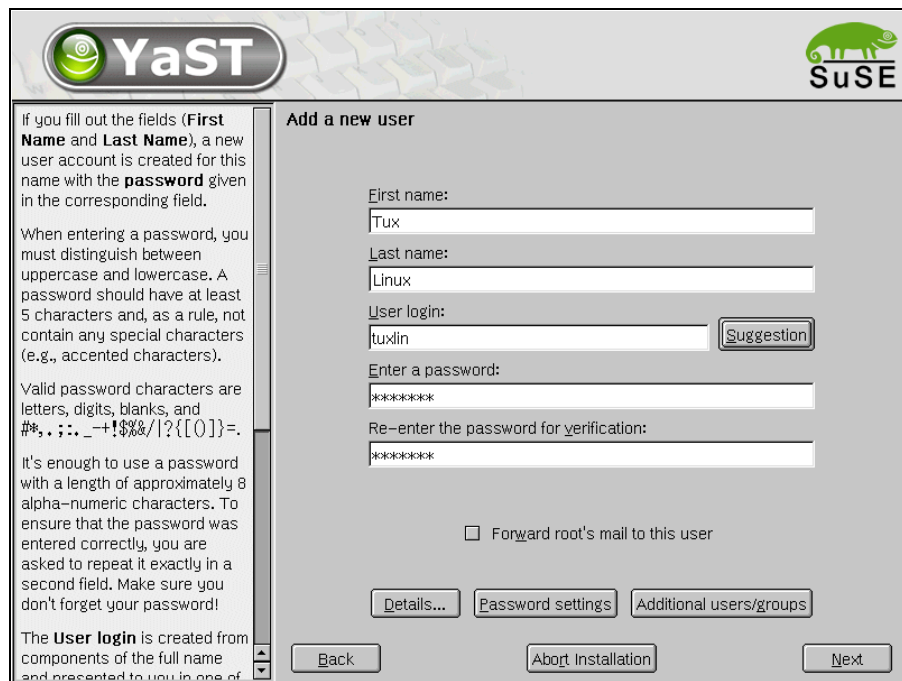


Figure 3-15 SLES Installation - Adding new users

11. At the Add a New User window, type the information for one system user. You can also add additional users and groups or change the password settings by clicking the appropriate buttons to do so. When finished, click **Next**.

**Note:** You need to add at least one user to let the installation continue.

12. The Desktop Settings window displays. Select one of the following options:
  - *Text mode only -- no graphical desktop* (this setting will not configure the graphical environment). If this setting is selected, click **Next** and continue to step 23.
  - *Graphical desktop environment* (this setting is the default selection). When making this selection, you will see some auto-detected settings for the graphical environment.
13. Click **Accept** to accept the settings and continue to step 23. To alter the settings, continue with step 15.
14. Click **Change** to change the graphic environment settings.
15. If your monitor was not detected, you will be prompted to start the configuration dialog to set up the display. Click **Yes** and then the **Properties** button. Select the appropriate vendor and model. (for IBM Monitor specifications go to:  
<ftp://ftp.pc.ibm.com/pcicrse/psref/mbook.pdf>) Click **OK** to return to SaX2. Click **Finish**.
16. For the mouse to work, choose the following in the mouse configuration dialog. At the **General** tab, select **USB-Mouse** and then **PS/2**. At the Port tab, select **/dev/input/mice**. Then click **OK**.

**Note:** We needed to modify a configuration file after installation. See step 26.

17. If needed, select the correct resolution, color depth, and refresh rate (for your monitor) by clicking **Desktop** (on the left), **Color and Resolution**, and then the **Properties** button. It is possible to damage your hardware by making these settings too high. Do not make changes if you do not know the correct settings. Click **OK** and then **Finish** when done.
18. Click **Finalize >>**.
19. Click **Test...** at the informational window.
20. A window displays, allowing you to fine tune the configuration with arrows (if the window does not appear, press **Ctrl+Alt+Backspace** to return to SaX2 and change the settings). If everything looks good, click **Save**.
21. Click **OK** at the dialog that confirms that the configuration was saved.
22. Click **Accept** at the Desktop Settings window if the settings are acceptable. If the settings are not acceptable, refer to step 15 again.
23. You may receive a warning at this time asking if you want to detect your printers. Select **Skip detection** unless you will be configuring a printer, in which case you should click **Yes**.

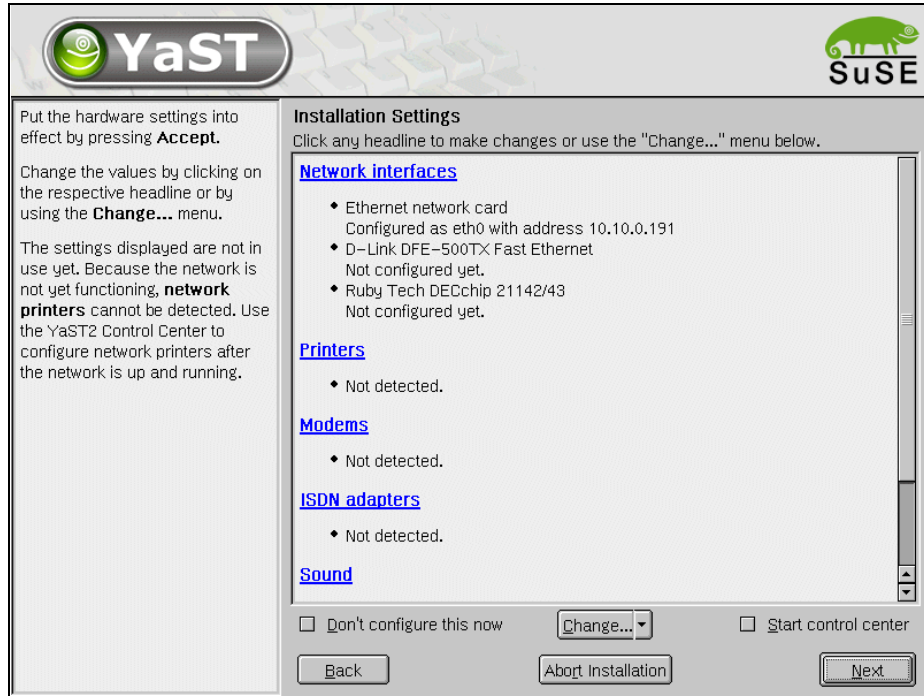


Figure 3-16 SLES Installation - Hardware configuration

24. The Installation Settings display enables you to configure various types of hardware. The hardware configuration can also be done later with the program YaST2. For example, you can set up your network interfaces here. When satisfied, click **Next** to finish the installation.

25. The installer will then reboot into the installed Linux. The installation is finished.

26. In our case, we needed to change the file `/etc/sysconfig/hotplug` to make the mouse work in X. Search for the line that start with `HOTPLUG_USB_STATIC_MODULES=...` and add `mousedev` to the list at that line. At the next reboot, the mouse should work in X.

If the server starts up by default in X, you can switch to a console terminal with **Crtl+Alt+F1** or, in KDE, you can use **Alt+F1** to access the menu for a terminal.

## 3.6 Installation of IBM Director Agent

In this section, we will give you a short overview of what IBM Director is and how to install the IBM Director Agent section on a Linux system. For more information about IBM Director and system management of the IBM @server BladeCenter, we refer you to the *IBM @server BladeCenter Systems Management Redpaper, REDP3582*.

### 3.6.1 Overview of IBM Director V4

IBM Director is a comprehensive workgroup hardware manager designed for use with IBM @server xSeries servers, PCs, notebooks and now IBM @server BladeCenter.

IBM Director V4 includes support for your IBM @server BladeCenter server, enabling you to manage, deploy and monitor your system much more efficiently. IBM Director includes features such as self-management and proactive and predictive tools which provide higher levels of availability and reliability. The IBM Director software is made up of three components:



- ▶ IBM Director Server
- ▶ IBM Director Agent
- ▶ IBM Director Console

A different combination of these components is required for each of the hardware groups in your IBM Director environment. The management server must contain all three of these components. The IBM Director Console must be installed on the management console or any system from which a system administrator will remotely access the management server. The IBM Director Agent must be installed on each system you intend to manage.

## **IBM Director Server**

The IBM Director Server is the main component of IBM Director software. The server component contains the management data, the server engine, and the application logic. IBM Director Server provides basic functions such as:

- ▶ Discovery of the managed systems
- ▶ Storage of configuration and management data
- ▶ Inventory database
- ▶ Event listening
- ▶ Security and authentication
- ▶ Management console support
- ▶ Administrative tasks

IBM Director comes with the Microsoft Jet database engine, however other database applications can be used in larger IBM Director management solutions. The IBM Director Console and IBM Director Agent are automatically installed when you install the IBM Director server. Every IBM @server xSeries comes with an IBM Director Server license.

## **IBM Director Agent**

The IBM Director Agent allows the Director server to communicate with systems on which it is installed. The agent provides the server with management data which can be transferred using TCP/IP, NetBIOS and IPX protocols. The IBM Directors Agent Web-based access can only be enabled on Windows operating systems. All IBM systems come with an IBM Director Agent license. Additional licenses can be purchased for non-IBM systems.

## **IBM Director Console**

The IBM Director Console enables systems administrators to manage all systems which have an agent installed. This is done easily via the graphical user interface (GUI) by either a drop-and-drag action or a single click. Unlike the agent, the console and server communicate and transfer data using TCP/IP. The IBM Director Console does not require the Director agent to be installed unless you want to manage this system as well, in which case the agent must be installed separately. IBM Director Console does not require a license and can be installed on as many systems as needed.

## 3.6.2 Installation of IBM Director Agent on Linux

This section discusses the requirements and installation steps for the IBM Director.

### IBM Director Agent requirements

The following are the hardware and software requirements for installing IBM Director Agent on Linux:

Table 3-1 Requirements for IBM Director Agent

	IBM Director Agent
CPU	Pentium 266+ MHz
Memory (RAM)	128 MB
Diskspace	220 MB
Supported Linux OS	Red Hat Linux, versions 7.1, 7.2, 7.3 Red Hat Linux Advanced Server, version 2.1 SuSE Linux, versions 7.2, 7.3, 8.0, 8.1

**Note:** The above values for the hardware are the minimum requirements; for performance reasons and depending on the size of your Director management solution, these values may need to be increased. These requirements are in addition to any other requirements for software that may be running on the system.

### Installation steps

Complete the following steps to install IBM Director Agent 4.1.

**Note:** Some packages from the IBM Director Agent require that the kernel source for the running kernel be installed. You can find the kernel source in the package `kernel-source` on the Red Hat CDs or FTP site.

1. Insert the Director 4.1 CD into the CD-ROM drive.
2. If the CD-ROM drive automounts, go to step 3. Otherwise, type the following command and press **Enter**:

```
mount /mnt/cdrom
```

Where `/mnt/cdrom` is the mount point of the CD-ROM drive.

3. Type the following command and press **Enter**:

```
cd /mnt/cdrom/director/agent/linux/
```

Where `/mnt/cdrom` is the mount point of the CD-ROM drive.

4. Copy the `i386/` folder that contains the IBM Director Agent for Linux code to a place on the hard disk:

```
cp -a i386/ /usr
```

5. The IBM Director Agent will be installed in the `/opt` directory. Depending on how you partitioned your hard disk, there might not be enough space on the partition that contains the `/opt` directory. If this is the case, then the following commands will move the `/opt` directory to another partition:

- a. `mv /opt /usr/opt`

- b. `ln -s /usr/opt /opt`

The `/opt` directory has now been moved to the partition holding the `/usr` directory.

6. Open a text editor and modify the `dirinstall` script. This file is located in the `i386/` directory copied in step 4 and is fully commented.

You can specify the location of the `.rpm` files (if they are located in a different directory from what is set in the `dirinstall` script), select the IBM Director Extensions you want to install, and choose log file options.

7. Save the modified installation script.

8. Enable execution of the installation script with `chmod a+x dirinstall`.

9. Start the installation by running the command:

```
./dirinstall
```

10. To enable encryption, run the command:

```
/opt/IBM/director/bin/cfgsecurity
```

11. To start IBM Director Agent, run the command:

```
/opt/IBM/director/bin/twgstart
```

12. To unmount the CD-ROM using the command:

```
umount /mnt/cdrom
```

Where `/mnt/cdrom` is the mount point of the CD-ROM drive.

The IBM Director Agent is now installed on the blade server. For more information on how to use the IBM Director Agent, refer to the IBM Director documentation and the Redpaper *IBM @server BladeCenter Systems Management*, REDP3582.





# Installing and configuring Samba

In this chapter, we will perform the installation of Samba onto our IBM @server BladeCenter HS20 server. This chapter describes how to:

- ▶ Install and configure Samba
- ▶ Use SWAT to configure Samba
- ▶ Stop, start, and restart Samba

## 4.1 Installing Samba

Since the version of Samba on the install CDs is usually downlevel, it is best to download the latest version from <http://www.samba.org/>. The latest stable code is available in binary, rpm file, and source code, tar.gz file, form. We downloaded the latest binary code for Red Hat 7.3 from [http://us2.samba.org/samba/ftp/Binary\\_Packages/redhat/RPMS/7.3/](http://us2.samba.org/samba/ftp/Binary_Packages/redhat/RPMS/7.3/).

1. Check whether Samba is already installed with the command:

```
rpm -qa |grep samba
```

This command will return the name and version of all the Samba packages installed on the system. If there are Samba packages installed, uninstall these packages with the command sequence:

```
for i in $(rpm -qa |grep samba); do rpm -e --nodeps $i; done
```

This command might return some errors while running.

2. Change to the directory where the downloaded RPM file is located and install the latest version using the command:

```
rpm -ivh samba-2.2.6-1.i386.rpm
```

## 4.2 Configuring the Samba server

We will now explain how to configure Samba so it can participate as a file/print server in an existing Windows network or as a stand-alone file/print server for Windows and Linux clients.

The Samba server configuration is stored in `smb.conf`. This file is usually found in the `/etc/samba` directory. The file can be modified by directly editing it or by using the Samba Web Administratin Tool (SWAT). We will configure Samba by directly editing the file. Then we will show how SWAT can be used to configure and control Samba.

### 4.2.1 Samba configuration file

The SAMBA configuration file `smb.conf` is divided into two main sections:

1. Global Settings - these settings affect the general operation of the server.
2. Share Definitions - these settings are used in defining shares. A share is a directory on the server that is accessible over the network by SMB client systems. There are three kinds of shares:
  - a. Homes - in this subsection, the user's home directories are defined.
  - b. Printers - in this subsection, available printers are defined.
  - c. Shares - this subsection is where all the shares are defined for the system.

We will now explain the common settings in each section of the configuration file. These settings will configure the server so it can participate as a file/print server in an existing Windows network or as a stand-alone file/print server for Windows and Linux clients. Only the most necessary parameters will be covered. For more detailed information, see the manual pages for `smb.conf` at:

```
/usr/share/doc/samba-2.2.7/docs/htmldocs/smb.conf.5.html
```

or the Samba documentation on the Samba project Web site at:

<http://www.samba.org>

You will find our sample smb.conf configuration file in Appendix A, “Samba configuration file” on page 99.

## Global NetBIOS parameters

The NetBIOS parameters should be at the top of the global section in the configuration file. When you open the smb.conf file, you will see something similar to Example 4-1.

*Example 4-1 NetBIOS global settings*

---

```
#===== Global Settings =====
[global]
    netbios name = Blade1
    workgroup = LINUX
    server string = Samba Server on Red Hat Linux
```

---

The parameters are described in Table 4-1.

*Table 4-1 NetBIOS parameters*

Parameters	Descriptions
NetBIOS name	The Samba server is known by this name on the network, similar to the Windows NT computer name. The default value is the first component of the host name.
workgroup	Specifies which Windows NT domain or workgroup the server will participate. It is equivalent to the Windows domain or workgroup name.
server string	Specifies the system description string which appears in the network browser list next to the machine name. It serves the same role as the Windows NT description field.

## Global printing parameters

The global printing settings will look similar to what is shown in Example 4-2.

*Example 4-2 Global printing settings*

---

```
load printers = yes
printcap name = /etc/printcap
# printing = lprng
```

---

The parameters are described in Table 4-2.

*Table 4-2 Printing parameters*

Parameter	Description
load printers	This parameter controls whether Samba loads all the printers in the printcap files for browsing by default. Possible values are yes and no.
printcap name	This parameter sets the location of the printcap file. Default value is /etc/printcap.
printing	This parameter controls how printer status information is interpreted on your system. Red Hat Linux uses LPRNG style by default.

## Global security settings

The global security settings will look similar to what is shown in Example 4-3.

*Example 4-3 Global security settings*

---

```
security = user
; password server = <NT-Server-Name>
encrypt passwords = yes
smb passwd file = /etc/samba.d/smbpasswd
```

---

The parameters are described in Table 4-3.

*Table 4-3 Security parameters*

Parameter	Description
security	This parameter affects how clients respond to Samba. The four possible values are: share, user, server, domain. Default settings is user.
password server	When the security parameter is server or domain, Samba will do all username/password validation via this SMB server. The parameter value must be the server NetBIOS name.
encrypt passwords	This parameter controls whether Samba uses the Encrypted Password Protocol when negotiating with clients. This is required to communicate with Windows NT Service Pack 3, Windows 2000, and Windows 98 clients.
smb passwd file	This parameter specifies the encrypted SMB password file.

The security modes are as follows:

- ▶ **Share** - in this security mode, clients only need to supply the password for the resource. This mode of security is the default for the Windows 95 file/print server. It is not recommended for use in UNIX environments, because it violates the UNIX security scheme.
- ▶ **User** - the user/password validation is done on the server that is offering the resource. This mode is most widely used.
- ▶ **Server** - the user/password validation is done on the specified authentication server. This server can be a Windows NT server or another Samba server. Each username must be associated with a UNIX user.
- ▶ **Domain** - this is the same as server security level with the additional requirement that the server is part of a domain. All user/password validation is done by the Primary or Backup Domain Controller. Since the server is part of a domain, it can anticipate in trust relationships. Also, Samba generates a UID and GID based on the information returned by the Primary Domain Controller.

How to create the encrypted password file and manage user IDs is discussed in 4.3, “Encrypted password file” on page 76.

## Global name resolution settings

The global name resolution settings will look similar to what is shown in Example 4-4.

*Example 4-4 Global name resolution settings*

---

```
name resolve order = wins lmhosts bcst
wins support = yes
; wins server = w.x.y.z
```

---



The parameters are described in Table 4-4.

Table 4-4 Name resolution parameters

Parameter	Description
name resolve order	This parameter determines which naming services to use and the order used to resolve host names to IP addresses. The preferred value is wins lmhosts bcast. See the smb.conf manual page for more information.
wins support	This parameter controls whether the Samba server will act as a WINS server. Default value is no.
wins server	The WINS server IP address that Samba should register with and use. Only used with wins support parameter: set to no.

**Note:** Samba can act as a WINS server or a WINS client, but not both. So only one of the parameters (wins support or wins server) can be set at the same time. If you specify the IP address of WINS server, then wins support must be set to no.

## Defining shares

The previous sections covered the general configuration parameters. In this and the next four sections, we will explain the parameters used in defining shared resources.

A simple share definition in the smb.conf file looks similar to Example 4-5.

Example 4-5 Redbook share parameters

```
[redbook]
comment = Redbook files
path = /redbook
browseable = yes
printable = no
writable = yes
write list = @users
```

Table 4-5 describes the most important parameters for defining a share.

Table 4-5 Share parameters

Parameter	Description
comment	Description of the share.
admin users	List of users who have administrative privileges on the share. These users can perform all operations with root authority.
path	The full path to the directory being shared.
browsable	Controls whether this share is seen in the list of available shares in a net view and in the browse list. Possible values are yes and no. Default value is yes.
printable	Specifies whether this is a print share. Possible values are yes and no. Default is no.
write list	List of users that have write access to the share. Can include group names using the @group syntax.
writable	Controls whether the share is writable. Possible values are yes and no.

Parameter	Description
read list	List of users that have read access to the share. Can include group names using the @group syntax.
read only	If set to yes, share is read only. Possible values are yes and no.
valid users	List of users that can access the share.

Each share definition starts with the share name in brackets “[ ]”. Below this name are the parameters and values that define the share.

## Share masks

When files are made available through a share, Samba must translate the UNIX permissions into Windows permissions. Share mask are used for setting and controlling UNIX file and directory permissions or modes. The most important parameters are explained in Table 4-6.

Table 4-6 Share mask parameters

Parameter	Description
create mask	Mask used for converting DOS modes to UNIX modes when creating files. Value is 0744 if parameter is not set.
security mask	Mask determines which UNIX modes bits a user can modify on a file from a Windows client. Any mask bits set to 1 can be modified. Default is 0777.
force create mode	Any permission bits set to 1 will be set on all files created in this resource. The setting can be modified after the file is created. Default setting is 000.
force security mode	Any mode or permission bits set to 1 will be set on all files and can not be modified from a Windows client. Default setting is 000.
directory mask	Mask used for converting DOS permissions to UNIX permission then creating directories. Value is 0755 if parameter is not set.
directory security mask	Mask used for determining which UNIX permission bits can be modified by a Windows NT client through the security dialog box. Value is 0777 if parameter is not set.
force directory mode	Any permission bits set to 1 will be set on all directories created in this resource. Default setting is 000.
force directory	Mask determines which UNIX permission bits on a directory can be modified from a Windows client. Default setting is 0777.

## Defining home directories

Samba has a special section called [homes] for defining user home directories. The home directory for each user id is specified in /etc/passwd on the server.

When a client requests a connection to a file share, existing file shares are scanned for the share. If a match is found, that share is used. If no match is found and there is a [homes] share defined in the configuration file, the requested share is assumed to be a user name. Samba then queries the password database for the name. If a matching entry is found, the home directory for that ID is shared as home using the [homes] parameters. The home share definition uses the same parameters as a normal share definition. An example of a home share definition in the smb.conf configuration file is shown in Example 4-6 on page 63.

*Example 4-6 Home directory parameters*

---

```
[homes]
  comment = Home Directories
  path = %H
  valid users = %S
  browseable = no
  writable = yes
  create mode = 0700
  directory mode = 0700
```

---

The special variables used in this definition are explained in Table 4-7.

*Table 4-7 Variable description*

Variable	Description
%H	The home directory of the current user.
%S	The name of the current service. Since the requested share is the user name, this variable is replaced by the user name.
%u	The user name of the current service.
%g	The primary group name of %u.

In Example 4-6 the create mode and directory mode masks are used to limit access to created files and directories to the owner of the home directory.

## Defining printer shares

A Samba server uses the same procedure for printer shares as for home shares. If the share does not match a defined share or a user name on the system, Samba then looks in the file specified by the global `printcap name` parameter, Example 4-2 on page 59, for the name. If there is a matching printer name, Samba creates a share named after the printer. All the printer shares will use the parameters of the `[printers]` definition. Example 4-7 shows an example of the printers definition.

*Example 4-7 Printers share parameters*

---

```
[printers]
  comment = All Printers
  path = /var/spool/samba
  browseable = no
  # Set public = yes to allow user 'guest account' to print
  guest ok = no
  writable = no
  printable = yes
  create mask = 0700
```

---

As you can see, the `[printers]` section is just another share definition. When a user prints, the output of the local printing system is copied into the spool directory. The only big difference between a printer share and other share definitions is that the `printable` parameter is set to `yes`. This means that a client can write a spool file to the directory specified under the share definition. If the share is printable, then it is also writable by default.

The major benefit of the special `[homes]` and `[printers]` sections is not having to maintain a share for each home directory and printer on the system.

**Note:** After any changes are made to the configuration file, the Samba server must be restarted. Restarting the server is detailed in 4.4, “Starting and stopping the Samba server” on page 77.

## 4.2.2 Using SWAT

The Samba Web Administration Tool (SWAT) allows the remote modification of the `smb.conf` configuration file through a Web browser. That means you can configure Samba in a GUI-like environment. SWAT itself is a small Web server and CGI scripting application, designed to run from `inetd` and provides access to the configuration file.

An authorized user with the root password can modify the configuration file via the SWAT Web pages. The Web pages also have help links next to all configurable options, which is very useful when making changes.

Before using SWAT, you must check:

1. That `/etc/services` has the line:

```
swat 901/tcp
```

2. That there is a `swat` file in the `/etc/xinetd.d` directory and it contains the line:

```
disable = no
```

3. And, if you want to access SWAT from another system, that the following line in the `swat` file is commented out:

```
only_from = localhost
```

If any changes were made to either file, restart `xinetd` by executing the command:

```
service xinetd restart
```

Access to the SWAT service can be controlled through entries in the `/etc/hosts.deny` and `/etc/hosts.allow` files.

To access SWAT, open your favorite Web browser and type in the IP address of your Samba server appended with port 901:

```
http://localhost:901
```

After the SWAT home page is loaded, you will see a window similar to Figure 4-1.



Figure 4-1 Login prompt

Type in the user name and password of the Linux user defined on your Linux server. Click **OK** to continue. If the root ID is used, you will see a page similar to Figure 4-2 on page 65.

**Important:** Any Linux user can access SWAT, but only a root user can make changes.

Remember, when you are logging on to SWAT from a remote machine, you are sending the password in clear text. This can be a security issue, so we recommend that you perform SWAT administration locally or over a secure network.

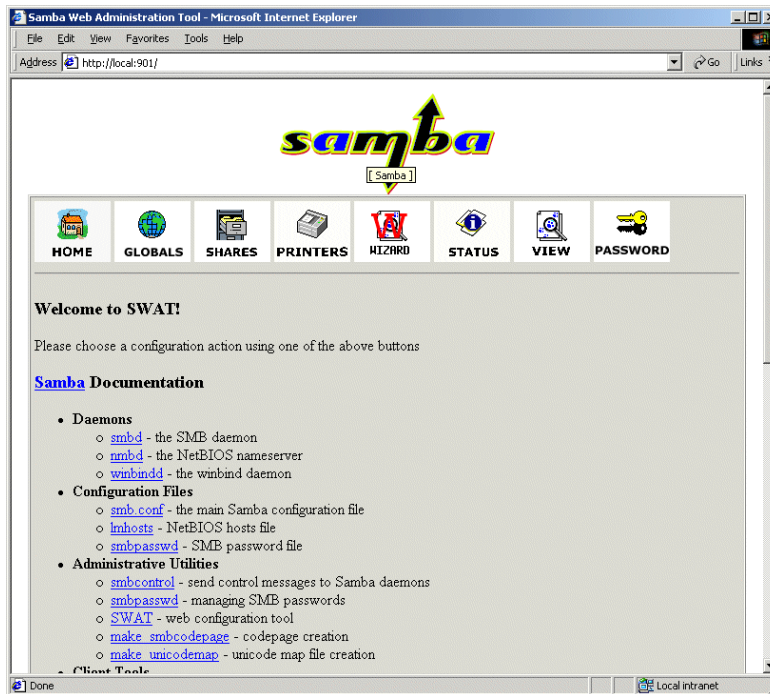


Figure 4-2 SWAT home page

As you can see in Figure 4-2, there are seven categories available:

1. Home - where you can view all the documentation you need about Samba.
2. Globals - where you can view and modify the global parameters.
3. Shares - where you can view, modify, and add shares.
4. Printers - where you can view, modify, and add printers.
5. Status - where you can check the current status, start, and stop the Samba server.
6. View - where you can view the configuration settings in smb.conf.
7. Passwords - where you can manage users and passwords.

Now we will briefly describe the functions available in SWAT.

**Note:** The seven function icons are at the top of all the SWAT Web pages.

After you make configuration changes, the Samba server must be restarted.

## Globals

Clicking the **Globals** icon will take you to a page similar to Figure 4-3.

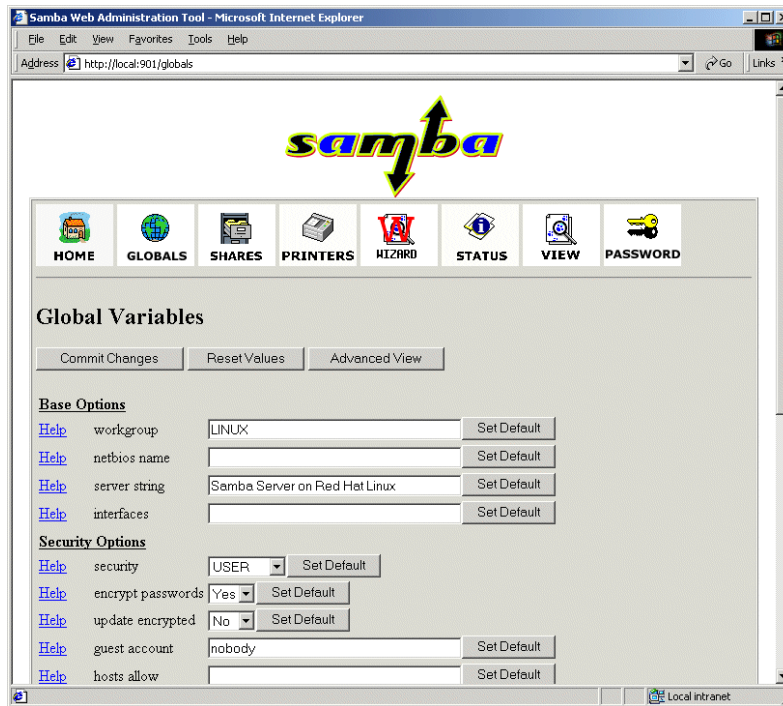


Figure 4-3 Globals page

From this page, any of the global parameters can be modified. The default Basic View show only the basic options. Clicking **Advanced View** will show all the global options. Click **Basic View** to return from the Advanced View back to the Basic View. Changes are saved to the configuration file by clicking **Commit Changes**. If a pop-up window similar to Figure 4-4 appears when saving changes, click **Continue** to close the window. Restart the Samba server to activate changes. This is described in "Starting, stopping, and restarting the Samba Server" on page 73.

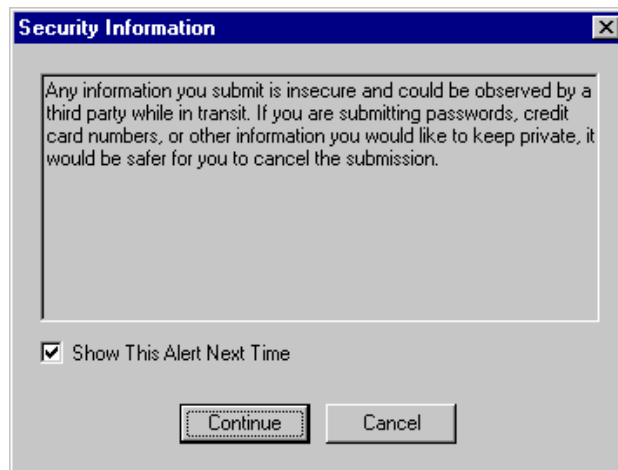


Figure 4-4 Security reminder

## Shares

Clicking the **Shares** icon will take you to a page similar to Figure 4-5.

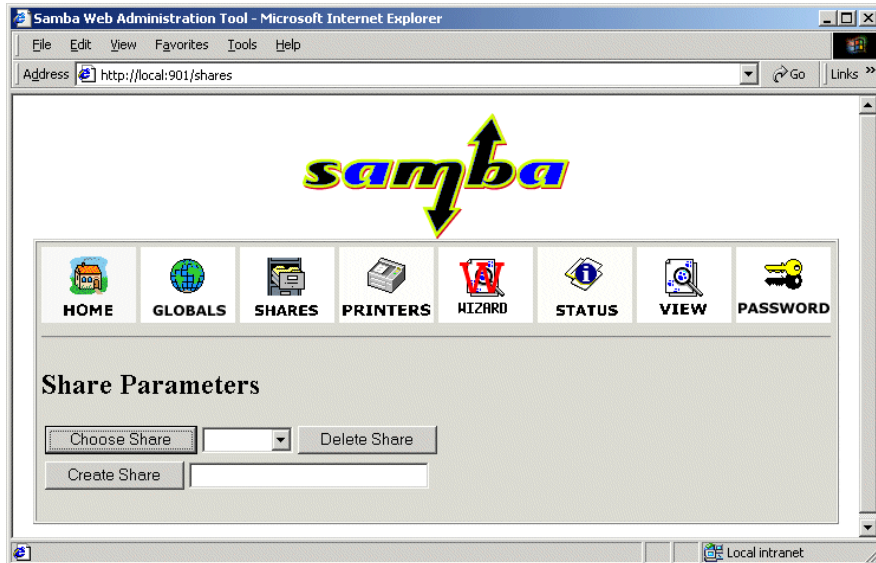


Figure 4-5 Shares page

On this page you can:

- ▶ View the defined share
- ▶ Delete the share
- ▶ Create a new share

### **Viewing or modifying an existing share**

To view or modify options for an existing share, follow these steps.

1. Select the share from the field to the right of the Choose Share button, as in Figure 4-6.

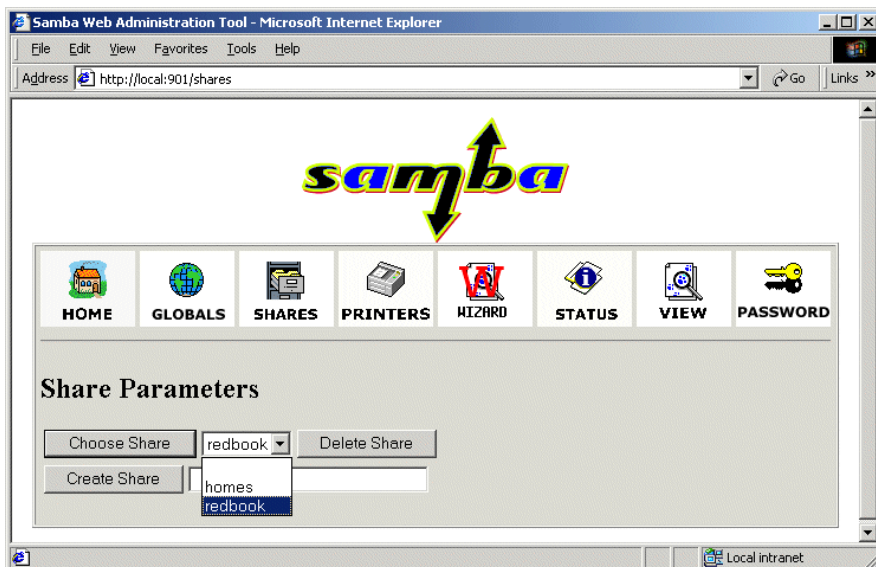


Figure 4-6 Selecting a defined share

2. Click **Choose Share**. The options will be displayed on a page similar to Figure 4-7, which shows the basic options.

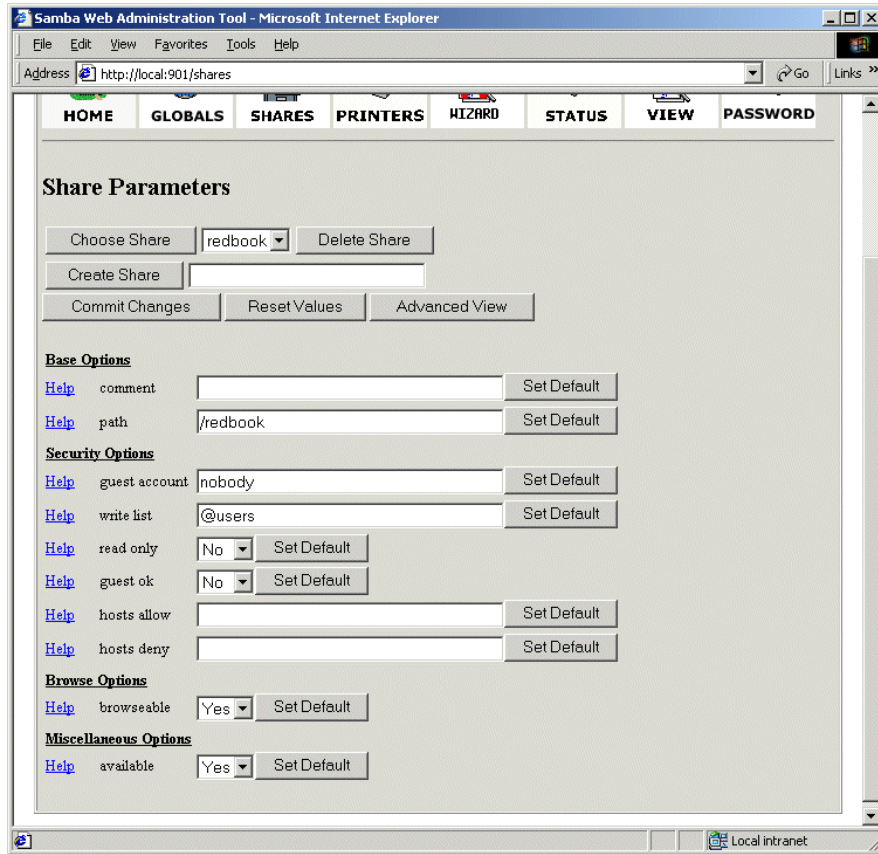


Figure 4-7 Modifying share options

3. Click **Advanced View** to view and modify all the share options.
4. Click **Commit Changes** to save any changes made.
5. Restart the Samba server. This is described in “Starting, stopping, and restarting the Samba Server” on page 73.

### **Deleting an existing share**

To delete a share definition, do the following.

1. Select the defined share, as shown in Figure 4-6 on page 67.
2. Click **Delete Share**.

**Note:** The share is deleted immediately and without warning.

3. Restart the Samba server. This is described in “Starting, stopping, and restarting the Samba Server” on page 73.



### **Creating a new share**

To create a simple share, do the following.

1. Create a directory that will be used for the share. You can do this by executing the command from a terminal:

```
mkdir /home/public
```

In our example we created a “public” directory in the “home” directory.

2. Adjust the UNIX permissions for the directory, so that only intended users have access.
3. Type in the share name in the field next to the Create Share button, similar to Figure 4-8.

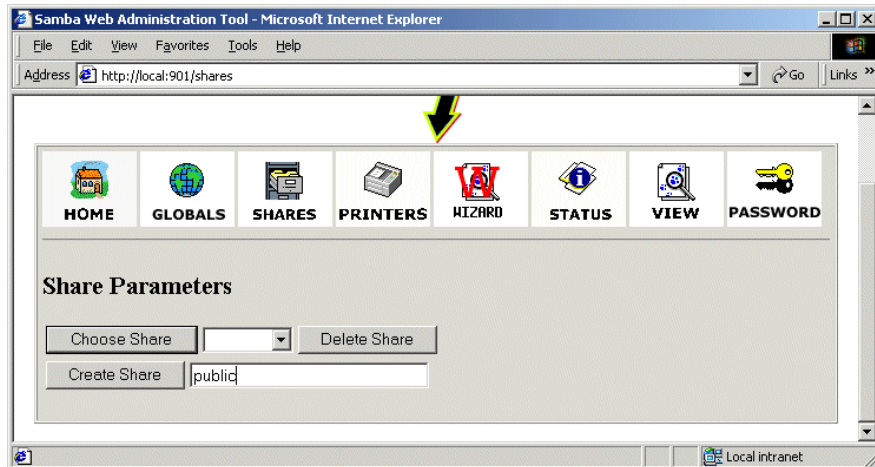


Figure 4-8 Create share

4. Click **Create Share**.

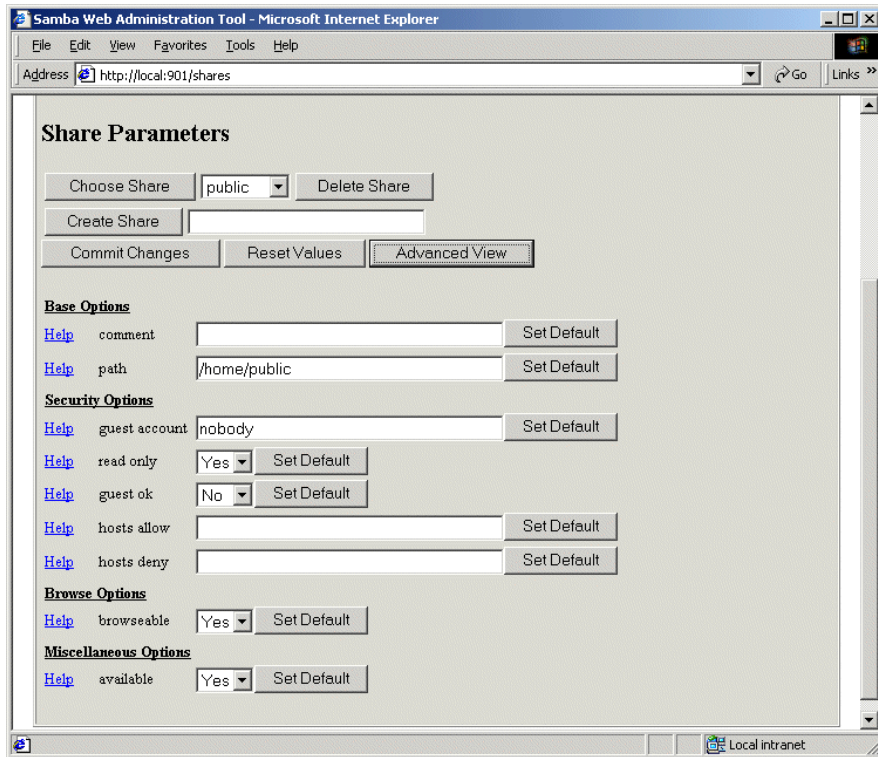


Figure 4-9 Setting share parameters

5. Fill in the needed parameters, as in Figure 4-9. If you need to set more advanced parameters, click **Advanced View**.
6. Click **Commit Changes** to save the new share settings.
7. Click the **View** icon to display the configuration file to verify that all the settings were recorded. The page will look similar to Figure 4-10 on page 71.

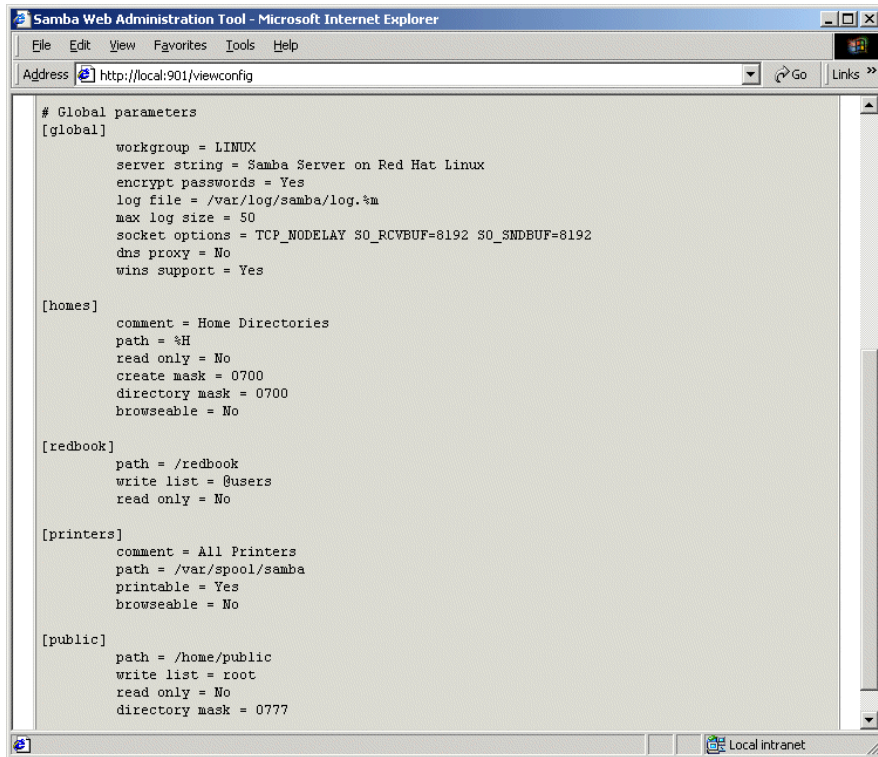


Figure 4-10 Viewing configuration file

- Restart the Samba server is described in section “Starting, stopping, and restarting the Samba Server” on page 73.

## Printers

Clicking the **Printers** icon will take you to the Printer Parameters page, similar to Figure 4-11 on page 72. On this page you can view, modify, or add printers. The operations for handling printers are the same as for handling shares.

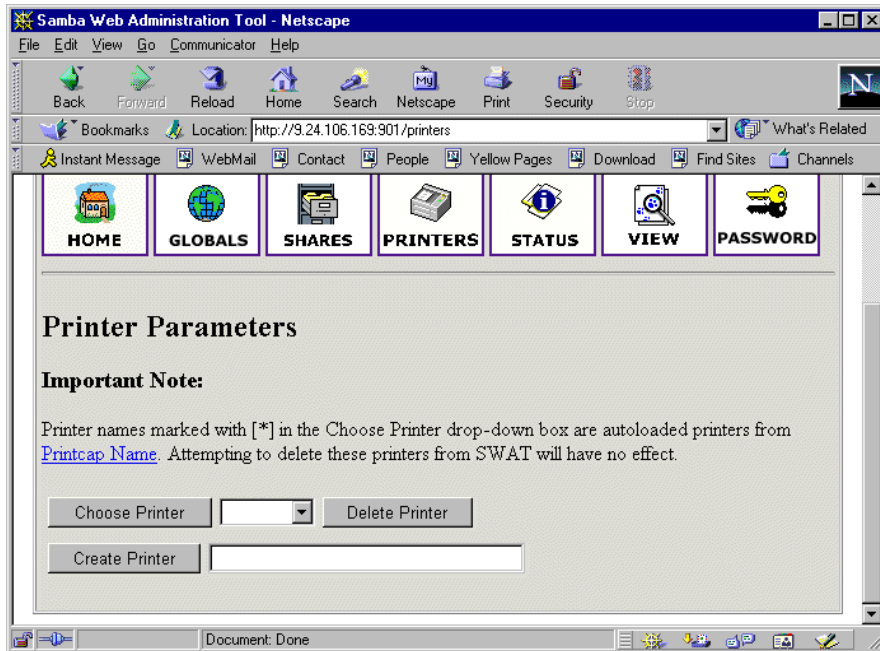


Figure 4-11 Printers page

To view the printers parameters, do the following.

1. Select printers from the list, as shown in Figure 4-12.

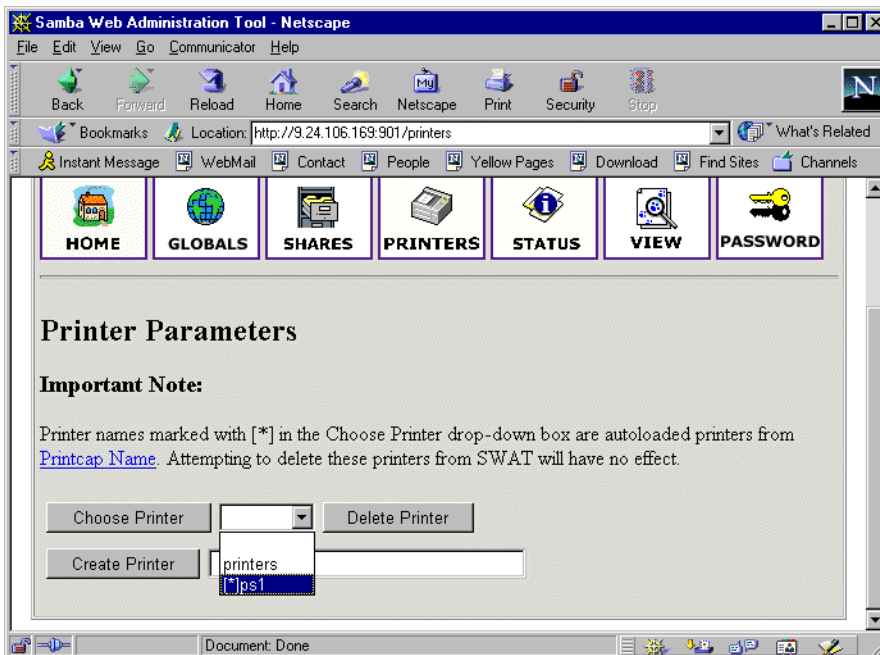


Figure 4-12 Selecting printer

2. Click **Choose Printer** to show the parameters in a page similar to Figure 4-13 on page 73.

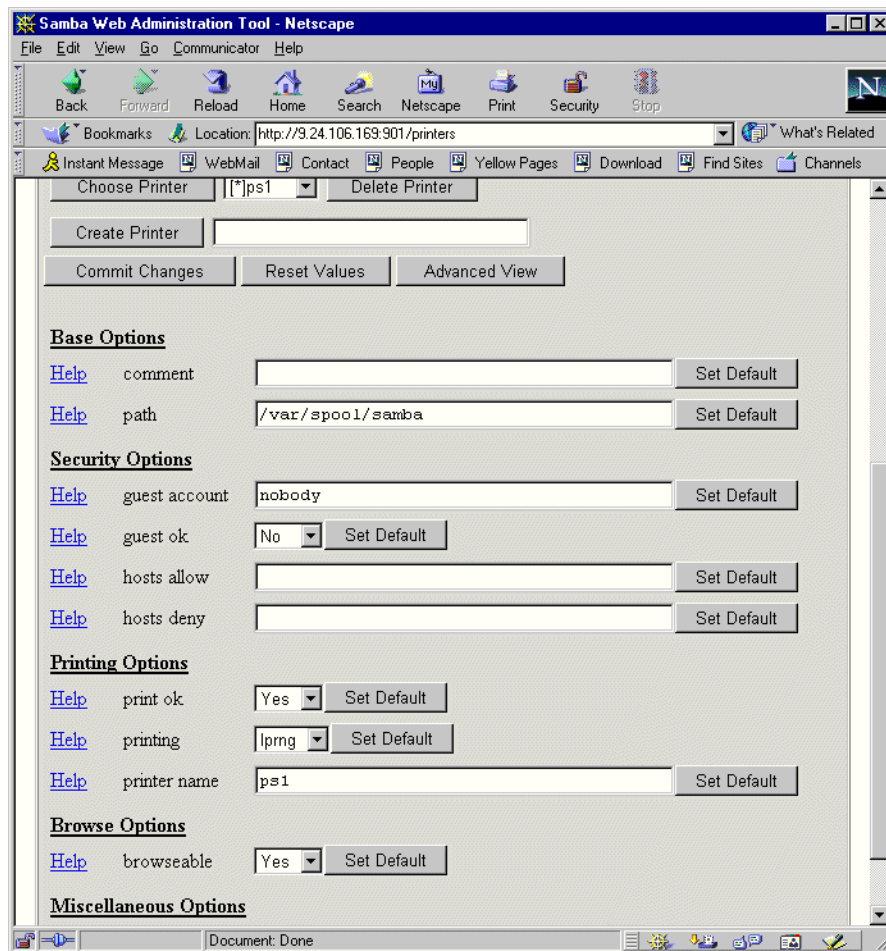


Figure 4-13 Modify printer settings

3. If any options are modified, clicking **Commit Changes** will save the changes to the configuration file.
4. Restart the Samba server as described in “Starting, stopping, and restarting the Samba Server” on page 73.

## Status

Clicking the **Status** icon will take you to the server status page, similar to Figure 4-14 on page 74. This page shows all the connections and open files. The Samba daemons can be started or restarted from this page.

### **Starting, stopping, and restarting the Samba Server**

If the Samba server is not running, clicking **Start smb** and **Start nmb** will start the two Samba daemons and change the button names to Stop smb and Stop nmb.

Clicking **Stop smb** will stop the Samba or smb daemon. Clicking **Stop nmb** will stop the WINS or nmb daemon.

When printer or share parameters have changed, clicking **Restart smb** will restart Samba and activate the changes. If global parameters have changed, restart both daemons by clicking **Restart smb** and **Restart nmb**.

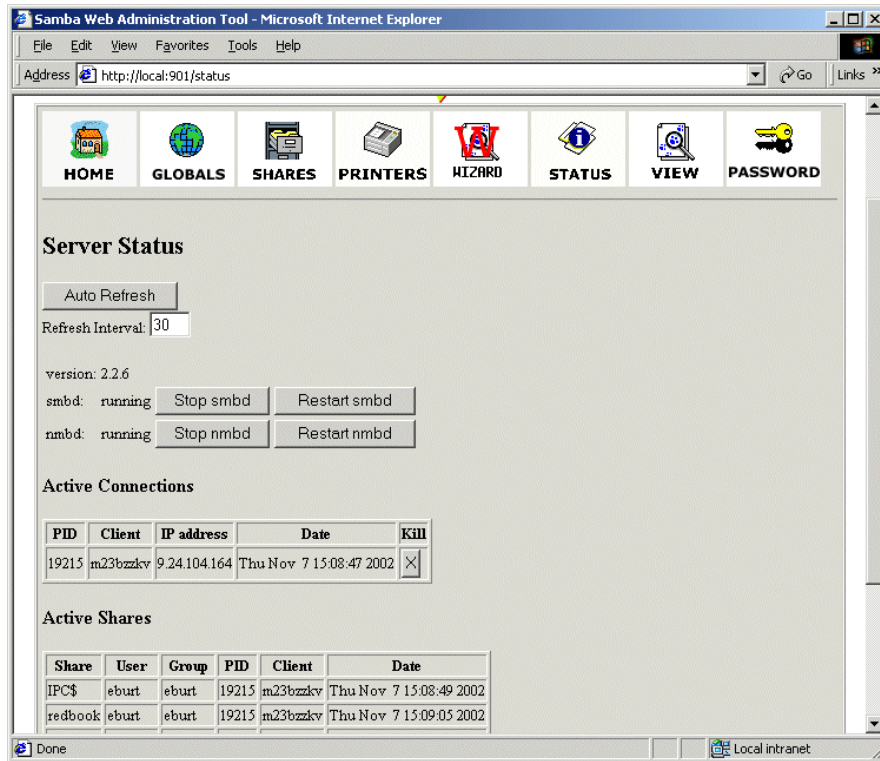


Figure 4-14 Server status

## View

Clicking the **View** icon will display a page with contents of the configuration file, without comments. The page will look similar to Figure 4-10 on page 71.

## Password

Clicking the **Password** icon will take you to the password management page, similar to Figure 4-15 on page 75. On this page, you can change passwords and add, delete, disable, and enable user IDs for this Samba server. Type in the user name, the new password twice and click **Change Password**; change the encrypted password or click **Add New User** to add the ID and set the password in the encrypted password file. To delete, disable, or enable an user, type in the user name and click **Delete User**, **Disable User**, or **Enable User**.

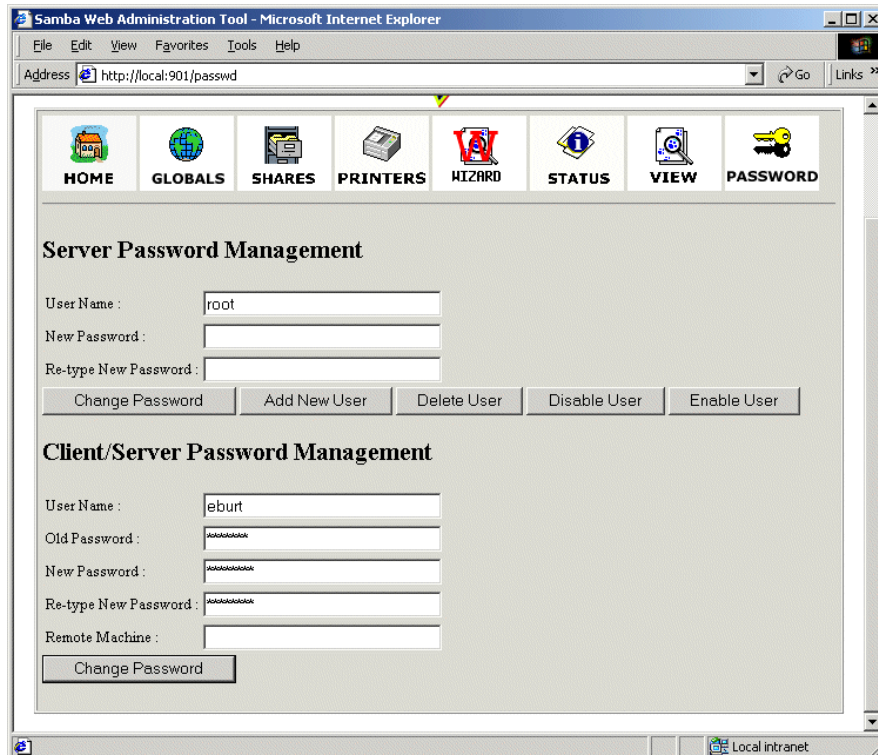


Figure 4-15 Password page

### ***Users changing a password***

When a non-admin ID logs into SWAT and click the **Password** icon, a page similar to Figure 4-16 on page 76 will be displayed. This user can change the password on this system by filling in four fields in the **Server Password Management** section and clicking **Change Password**. The user can change the password on another system by filling in the five fields in the **Client/Server Password Management** section and clicking **Change Password**.

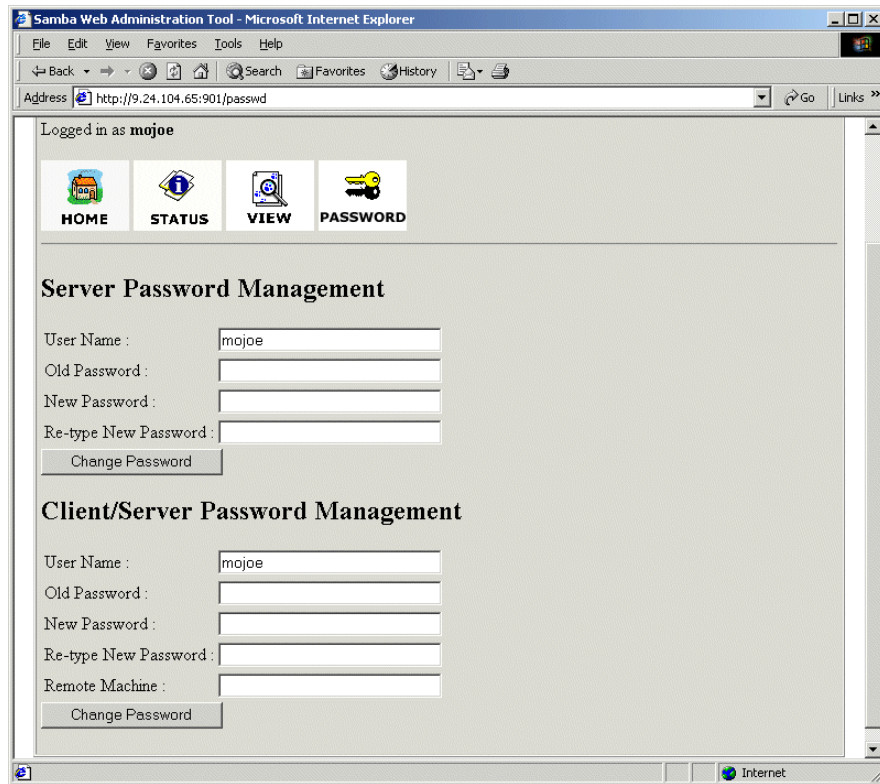


Figure 4-16 User changing password

## 4.3 Encrypted password file

Since password encryption is required for Windows 2000, Windows NT 4.0 Service Pack 3 or later, Windows 95, and Windows 98, you need to enable encrypted password support and create the encrypted password file before starting the Samba server. The encrypted password file can be created with the `mksmbpasswd` utility. It is recommended to first create the user accounts on Linux and then create the Samba password file with the command:

```
cat /etc/passwd | /usr/bin/mksmbpasswd.sh > /etc/samba/smbpasswd
```

This creates the Samba password file from the Linux password file.

**Note:** Use the same filename specified in the `smb passwd` file parameter in `smb.conf`.

By default, the passwords for the Samba users are undefined. Before any connection is made, a password must be set for each user ID.

Now a password must be set for each user ID that will be a connection from a SMB client. The password can be changed or set by executing the command:

```
/usr/bin/smbpasswd -U <username>
```

You will see prompts similar to those shown in Example 4-8 on page 77.



#### Example 4-8 Setting SMB encrypted password

```
# /usr/bin/smbpasswd -U mojoe
New SMB password:
Retype new SMB password:
Password changed for user mojoe.
#
```

**Note:** Anyone with write access to `/usr/bin/smbpasswd` can change passwords for the Samba users.

Another way is to have each Samba user change the password for himself, by remotely connecting to the Samba server and executing the command:

```
/usr/bin/smbpasswd
```

The output will be similar to Example 4-8. If the user account already has a password defined, the person will be prompted for the old password before the new password can be entered.

A new user can be added to the encrypted password file later by typing the command:

```
/usr/bin/smbpasswd -a <username> <password>
```

This should be done after the Linux user account has been created.

**Note:** Only root can manage other user IDs. Standard users can only change their own password. The `smbpasswd` utility uses the password file specified in `smb.conf`.

## 4.4 Starting and stopping the Samba server

You can start the Samba server by executing the command:

```
service smb start
```

This will start the `smbd` and `nmbd` daemons. `Smbd` is the actual Samba server and `nmbd` is the WINS server.

The Samba server can be stopped by executing the command:

```
service smb stop
```

Whenever modifications are made to `smb.conf`, the Samba server must be restarted. This can be done by executing the command:

```
service smb restart
```

## 4.5 Starting Samba as part of the boot process

The Samba server can be configured to start when the system boots. This can be done using `chkconfig` by executing the command:

```
chkconfig smb on
```

Check that it will be started by executing the command:

```
chkconfig --list smb
```

The output should look similar to Example 4-9 on page 78.

*Example 4-9 Setting and checking smb start on boot*

---

```
[root@blade5 samba]# chkconfig smb on
[root@blade5 samba]# chkconfig --list smb
smb          0:off  1:off  2:off  3:on   4:on   5:on   6:off
```

---

## 4.6 Sources and additional information

You can find more information on the official Samba project Web site at:

<http://www.samba.org>

The Samba installation comes html documentation located on the server at:

`/usr/share/samba-2.2.6/docs/htmldocs`

There is a Web version of Using Samba located on the system at:

`file:///usr/share/samba-2.2.6/docs/htmldocs/using_samba/index.html`

There is a collection of how-to documents located on the system at:

`file:///usr/share/samba-2.2.6/docs/Samba-HOWTO-Collection.pdf`

There are always good how-to documents on the Linux Documentation project home page:

<http://www.linuxdoc.org/>

Information on joining a Samba server to a Windows domain is available at:

`file:///usr/share/doc/samba-2.2.6/docs/htmldocs/Integrating-with-Windows.html`

<http://us1.samba.org/samba/ftp/appliance/windbind.pdf>

<http://us6.samba.org/samba/ftp/htmldocs/windbind.html>

<http://us2.samba.org/samba/docs/man/windbindd.8.html>



## Samba management and troubleshooting

In this chapter, we will discuss and describe the following:

- ▶ Checking server status
- ▶ Testing the configuration file
- ▶ Closing active connections
- ▶ Configuring log files
- ▶ Sending Winpopup messages
- ▶ Viewing NetBIOS network traffic

## 5.1 Checking the server status

The Samba suite has several programs that can be used for checking the `smbd` and `nmbd` daemons.

### 5.1.1 Checking the status

The status of the Samba server can be viewed by running the `smbstatus` command or through SWAT. Checking status through SWAT is shown in “Status” on page 73.

A brief status report is returned by the command:

```
smbstatus -b
```

The report will be similar to Example 5-1.

#### *Example 5-1 Brief status report*

---

```
[root@portall root]# smbstatus -b
```

Samba version 2.2.7

PID	Username	Machine	Time logged in
23645	eburt	m23bzzkv	Mon Nov 11 09:28:08 2002
23802	mojoe	burte	Mon Nov 11 10:34:57 2002

---

The more detailed report shown in Example 5-2 is returned by the command:

```
smbstatus -d
```

#### *Example 5-2 Verbose status report*

---

```
[root@portall root]# smbstatus -d
using configfile = /etc/samba/smb.conf
Opened /var/cache/samba/connections.tdb
```

Samba version 2.2.7

Service	uid	gid	pid	machine	
redbook	mojoe	mojoe	23802	burte	(9.24.104.129) Mon Nov 11 10:38:43 2002
mojoe	mojoe	mojoe	23802	burte	(9.24.104.129) Mon Nov 11 10:34:57 2002
IPC\$	eburt	eburt	23645	m23bzzkv	(9.24.104.164) Mon Nov 11 09:28:08 2002

No locked files

---

### 5.1.2 Checking resources

Checking the available resources without using a Windows system is done with the `smbclient` command. The public browsable shares can be viewed by executing the command:

```
smbclient -U% -L localhost
```

The output will look similar to what is shown in Example 5-3 on page 81. The available shares are shown in the Sharename column.

*Example 5-3 Public resources*

```
[root@portal1 root]# smbclient -U% -L localhost
added interface ip=9.24.105.99 bcast=9.24.105.255 nmask=255.255.254.0
Domain=[LINUX] OS=[UNIX] Server=[Samba 2.2.7]
```

Sharename	Type	Comment
-----	----	-----
redbook	Disk	
public	Disk	
IPC\$	IPC	IPC Service (Samba Server on Red Hat Linux)
ADMIN\$	Disk	IPC Service (Samba Server on Red Hat Linux)

Server	Comment
-----	-----
PORTAL1	Samba Server on Red Hat Linux

Workgroup	Master
-----	-----
DUMMYBRANCH	M23BK62W
FCD90020	FCROA307
FSCLAN	T22ROEHM
LINUX	PORTAL1
MILKYWAY	SATURN
PK_NW	MSGTRX01
RAL400	AS4ACONSOLE
SCNF	TAMAS02
WORKGROUP	M23BK60L
WTRNTDM	78-BA897

**Note:** No username or password was supplied after the -U option. The username password separator, %, must be used to indicate no username and password.

The resources available for user mojoe can be seen by executing the command:

```
smbclient -U mojoe -L localhost
```

Example 5-4 shows the mojoe home directory is the only additional resource available to mojoe.

*Example 5-4 Resources available to mojoe*

```
[root@portal1 root]# smbclient -L localhost -U mojoe
added interface ip=9.24.105.99 bcast=9.24.105.255 nmask=255.255.254.0
Password:
Domain=[LINUX] OS=[UNIX] Server=[Samba 2.2.7]
```

Sharename	Type	Comment
-----	----	-----
redbook	Disk	
public	Disk	
IPC\$	IPC	IPC Service (Samba Server on Red Hat Linux)
ADMIN\$	Disk	IPC Service (Samba Server on Red Hat Linux)
mojoe	Disk	Home Directories

Server	Comment
-----	-----
PORTAL1	Samba Server on Red Hat Linux

Workgroup	Master
-----	-----

-----	-----
DUMMYBRANCH	M23BK62W
FCD90020	FCROA307
FSCLAN	T22ROEHM
LINUX	PORTAL1
MILKYWAY	SATURN
PK_NW	MSGTRX01
RAL400	AS4ACONSOLE
SCNF	TAMAS02
WORKGROUP	M23BK60L
WTRNTDM	78-BA897

---

### 5.1.3 Checking WINS

Checking the WINS server from the Samba server is done with the `nmblookup` command. The `nmbd` daemon can be queried for the special Samba server string by executing the command:

```
nmblookup -B localhost __SAMBA__
```

The output will look similar to Example 5-5 if the `nmbd` daemon is responding to requests.

*Example 5-5 Query local for Samba servers*

---

```
[root@portal1 root]# nmblookup -B localhost __SAMBA__
querying __SAMBA__ on 127.0.0.1
9.24.105.99 __SAMBA__ <00>
```

---

**Note:** The localhost address is being used as the broadcast address so the command will only receive a response from the local `nmbd` daemon.

All the Samba servers on the network will be listed by executing the command:

```
nmblookup __SAMBA__
```

Verify that the server is a member of the LINUX workgroup by executing the command:

```
nmblookup -B localhost LINUX
```

The output will look similar to Example 5-6 if it is a member of the workgroup.

*Example 5-6 Query local for members of LINUX workgroup*

---

```
[root@portal1 root]# nmblookup -B localhost LINUX
querying LINUX on 127.0.0.1
9.24.105.99 LINUX<00>
```

---

All the members of the LINUX workgroup on the local network will be seen by executing the command:

```
nmblookup LINUX
```

Example 5-7 shows all members of the LINUX workgroup on the local network.

*Example 5-7 All members of LINUX workgroup*

---

```
[root@portal1 samba]# nmblookup LINUX
querying LINUX on 9.24.105.255
9.24.105.99 LINUX<00>
9.24.104.129 LINUX<00>
```

---

## 5.2 Testing the configuration file

The Samba configuration file can be checked with the **testparm** command. The program only checks syntax, so there is no guarantee that all the defined shares will be available when the config file is loaded by the Samba server.

Checking the configuration file, `/etc/samba/smb.conf`, and displaying all non-default settings is done by executing the command:

```
testparm -sx
```

The output will look similar to the report shown in Example 5-8.

---

### *Example 5-8 Output of testparm -sx*

```
[root@portall samba]# testparm -sx
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[redbook]"
Processing section "[printers]"
Processing section "[public]"
Loaded services file OK.
# Global parameters
[global]
    workgroup = LINUX
    server string = Samba Server on Red Hat Linux
    encrypt passwords = Yes
    log level = 0
    log file = /var/log/samba/log.%m
    max log size = 50
    socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
    dns proxy = No
    wins support = Yes

[homes]
    comment = Home Directories
    path = %H
    read only = No
    create mask = 0700
    directory mask = 0700
    browseable = No

[redbook]
    comment = RedBook files
    path = /redbook
    write list = @users
    read only = No

[printers]
    comment = All Printers
    path = /var/spool/lpd
    printable = Yes
    browseable = No

[public]
    path = /home/public
    write list = root
    read only = No
    directory mask = 0777
```

---

Any errors will show up at the top of the report under the section where the error is located. The rest of the report shows what parameters the Samba server will load.

Since no errors were found, Samba will run with this configuration file.

If the public share definition is modified to what is shown in Example 5-9, the report will look similar to Example 5-10.

*Example 5-9 Resource definition with two errors*

---

```
[public]
  path = /home/public
  write list = root
  read only = No
  creat mask = 755
  directory mask = 0777
  force directory mode = 0758
```

---

The only error is noted under the public section. The report under the loaded services file OK line displays the non-default parameters. This part of the report is useful for verifying the share definition parameter settings. Notice that the force directory mode parameter will be loaded with a value of 075 for the public share in Example 5-10.

*Example 5-10 Output of testparm showing errors.*

---

```
[root@portal1 samba]# testparm -sx
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[redbook]"
Processing section "[printers]"
Processing section "[public]"
Unknown parameter encountered: "creat mask"
Ignoring unknown parameter "creat mask"
Processing section "[Samba Docs]"
Loaded services file OK.
WARNING: You have some share names that are longer than 8 chars
These may give errors while browsing or may not be accessible
to some older clients
# Global parameters
[global]
  workgroup = LINUX
  server string = Samba Server on Red Hat Linux
  encrypt passwords = Yes
  log file = /var/log/samba/log.%m
  max log size = 50
  socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
  dns proxy = No
  wins support = Yes

[homes]
  comment = Home Directories
  path = %H
  read only = No
  create mask = 0700
  directory mask = 0700
  browseable = No

[redbook]
  comment = RedBook files
  path = /redbook
```



```

write list = @users
read only = No

[printers]
comment = All Printers
path = /var/spool/lpd
printable = Yes
browseable = No

[public]
path = /home/public
write list = root
read only = No
directory mask = 0777
force directory mode = 075

[Samba Docs]
comment = Samba Documentation
path = /usr/share/doc/samba-2.2.7/docs

```

---

## 5.3 Closing connections

Closing SMB client connections can either be done from the command line or through SWAT.

### 5.3.1 Command line

Closing all connections to shares is done by executing the command:

```
smbcontrol smbd close-share *
```

Example 5-11 shows the server status before and after executing the command.

*Example 5-11 Closing all share connections*

---

```
[root@portall samba]# smbstatus
```

Samba version 2.2.7

Service	uid	gid	pid	machine
public	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:46:05 2002
mojoe	mojoe	mojoe	25694	portall (9.24.105.99) Mon Nov 11 15:43:37 2002
IPC\$	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:21:58 2002

No locked files

```
[root@portall samba]# smbcontrol smbd close-share '*'
[root@portall samba]# smbstatus
```

Samba version 2.2.7

Service	uid	gid	pid	machine
public	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:46:05 2002
mojoe	mojoe	mojoe	25694	portall (9.24.105.99) Mon Nov 11 15:43:37 2002
IPC\$	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:21:58 2002

No locked files

---

Closing all connections to a share, redbook in this case, is done by executing the command:

```
smbcontrol smbd close-share redbook
```

Example 5-12 shows the server status before and after the connection to the redbook share is closed.

*Example 5-12 Closing redbook share*

---

```
[root@portall samba]# smbstatus
```

```
Samba version 2.2.7
```

Service	uid	gid	pid	machine
redbook	mojoe	mojoe	25586	portall (9.24.105.99) Mon Nov 11 15:40:19 2002
public	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:46:05 2002
mojoe	mojoe	mojoe	25694	portall (9.24.105.99) Mon Nov 11 15:43:37 2002
IPC\$	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:21:58 2002

```
No locked files
```

```
[root@portall samba]# smbcontrol smbd close-share redbook
```

```
[root@portall samba]# smbstatus
```

```
Samba version 2.2.7
```

Service	uid	gid	pid	machine
public	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:46:05 2002
mojoe	mojoe	mojoe	25694	portall (9.24.105.99) Mon Nov 11 15:43:37 2002
IPC\$	eburt	eburt	25360	m23bzzkv (9.24.104.164) Mon Nov 11 15:21:58 2002

```
No locked files
```

---

## 5.3.2 SWAT

Connections can be closed from the SWAT status page by clicking the button in the kill column of the active connection row.

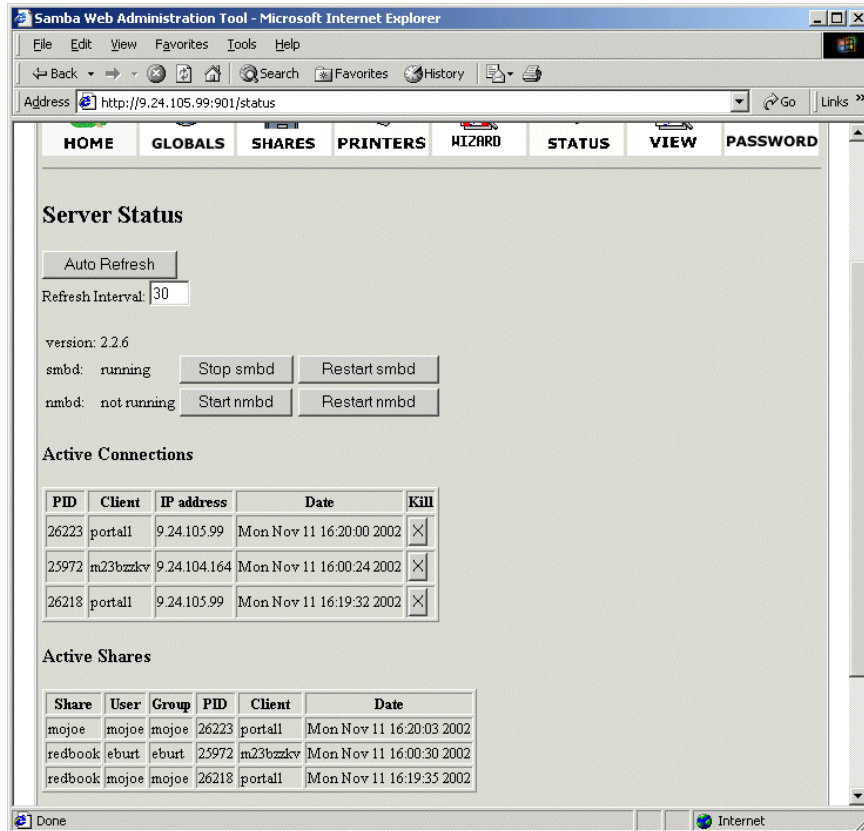


Figure 5-1 Closing connection from SWAT

Clicking the second button in the Kill column shown in in Figure 5-1 will close only that connection to the redbook share. Multiple shares cannot be closed at once through SWAT. Each connection must be closed individually.

## 5.4 Configuring log files

Log files are the best place to look when troubleshooting a problem or viewing what the server is doing.

Table 5-1 lists the global parameters that control Samba logging.

Table 5-1 Log file parameters

Parameters	Descriptions
log file	Overrides default log file settings. Allows creation of log files using variable substitution.
log level	Integer value between 0 and 10 that specifies the debug log level, where 0 sets logging errors only and 10 full debug logging. Default value is 0 when parameter is not set. Setting of 3 will provide enough information for solving problems.

Parameters	Descriptions
max log size	Integer value setting the maximum size of the log file in kilobytes. File name is appended with .old and a new file is created when this limit is reached. Default value is 5000.

The global log parameters will look similar to what is shown in Example 5-13.

*Example 5-13 Log settings*

---

```
log limit = 2
log file = /var/log/samba/log.%m
max log size = 50
```

---

Log level setting of 2 will result in log entries similar to Example 5-14.

*Example 5-14 Level 2 log entries*

---

```
[2002/11/12 09:29:31, 2] libsmb/namequery.c:name_query(421)
  Got a positive name query response from 9.24.104.164 ( 9.24.104.164 )
[2002/11/12 09:29:31, 0] smbd/service.c:make_connection(251)
  m23bzzkv (9.24.104.164) couldn't find service ::{2227a280-3aea-1069-a2de-08002b30309d}
[2002/11/12 09:29:32, 1] smbd/service.c:close_cnum(675)
  m23bzzkv (9.24.104.164) closed connection to service redbook
[2002/11/12 09:29:32, 1] smbd/service.c:close_cnum(675)
  m23bzzkv (9.24.104.164) closed connection to service public
```

---

The log level parameter settings are described in Table 5-2.

*Table 5-2 Log level settings*

Level	Description
0	Only critical failures are recorded, such as failing to open a log file, dropping a connection, or receiving an unknown command.
1	Connection and session information is logged.
2-4	System administration debugging information is logged.
5-9	Moderate developer debugging information is logged.
10	Full developer debugging information is logged.

There can be more than one log file parameter set in the configuration file. Each parameter instance will result in the creation of the specified log files.

The most useful log file settings are listed in Table 5-3.

*Table 5-3 Useful log file settings*

Parameter setting	Log created
log file = /var/log/samba/log.%m	Create a log file for each connecting client.
log file = /var/log/samba/log.%S	Create a log file for recording all share activity.
log file = /var/log/samba/log.%U	Create a log file for recording all user activity.

Samba always creates log files for the smbd and the nmbd daemons in /var/log/samba. The smbd log is usually named log.smbd and the nmbd is usually named log.nmbd. The log level

and max log size parameters do determine the amount of information logged and the maximum log size.

## 5.5 Sending Winpopup messages

Before bringing down the server or restarting Samba, it would be helpful to send Winpopup messages to all the clients that are connected to resources on the system. The smbclient command syntax is:

```
smbclient -M <NetBIOS system name>
```

After running this command, type in the messages and press **^D** (Control D) on a blank line to indicate the end of the messages. Example 5-15 shows the command that produced the messages box shown in Figure 5-2.

*Example 5-15 Sending Winpopup message*

```
[root@portall samba]# smbclient -M m23bzzkv
added interface ip=9.24.105.99 bcast=9.24.105.255 nmask=255.255.254.0
Got a positive name query response from 9.24.104.164 ( 9.24.104.164 )
Connected. Type your message, ending it with a Control-D
this is a test message
sent 24 bytes
```

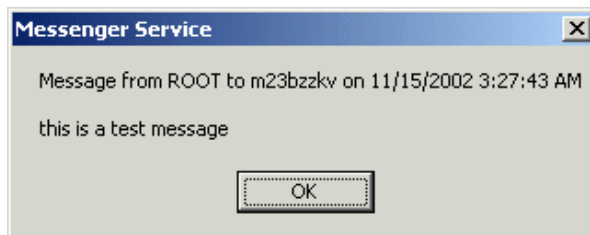


Figure 5-2 Message box

To send a prepared message, use the command sequence:

```
cat theMessage | smbclient -M foobar
```

Sending a message without pressing **^D** at the end is accomplished by the command sequence:

```
echo "The server is going down in 5 minutes." | smbclient -N foobar
```

Sending a message to all client systems using services can be done with the command sequence:

```
for c in $(smbstatus -b |awk '/^[0-9]/ {print $3}'); do echo "Server will be going down in 5 minutes" | smbclient -M $c -U 'the all powerful admin'; done
```

The message box displayed on each client will look similar to Figure 5-3.

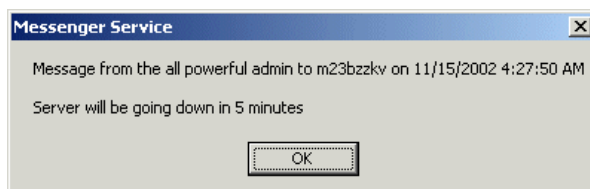


Figure 5-3 Server will be going down message

## 5.6 Viewing NetBIOS network traffic

There are times when the only way to debug is to view the network traffic. There are several tools that come with most Linux distributions for doing this. The most popular is tcpdump, because it has been around the longest. Because some versions of tcpdump do not handle NetBIOS traffic and other versions do not produce very useful output, we are going to use another popular tool, ethereal.

### 5.6.1 Installing ethereal

Depending on how the server was installed, ethereal may already be installed. Check using the command:

```
rpm -q ethereal
```

If nothing is returned, then install it from the distribution CDs. Ethereal was installed from the install server using the command shown in Example 5-16.

*Example 5-16 Installing ethereal from install server*

---

```
linux:~ # rpm -ivh
ftp://portall/pub/SLES8/disc2/UnitedLinux/i586/ethereal-0.9.6-65.i586.rpm
Retrieving ftp://portall/pub/SLES8/disc2/UnitedLinux/i586/ethereal-0.9.6-65.i586.rpm
ethereal #####
linux:~ # rpm -q ethereal
ethereal-0.9.6-65
```

---

### 5.6.2 Using ethereal

The rpm installs a GUI and non-GUI version of network protocol analyzers. We are going to use the non-GUI version, tethereal, because the traffic can be viewed live and many servers are not installed with X11 support.

Find the active network interfaced using the `ifconfig` command as shown in Example 5-17.

*Example 5-17 Output of ifconfig*

---

```
[root@blade5 root]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:09:6B:00:12:61
          inet addr:9.24.104.65  Bcast:9.24.105.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12690 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4493 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2973404 (2.8 Mb)  TX bytes:1458873 (1.3 Mb)
          Interrupt:17

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8358 (8.1 Kb)  TX bytes:8358 (8.1 Kb)
```

---

Network interface `eth1` is the only active network interface, so it will be used. If there are more than one active network interfaces, choose one.

Viewing all the NetBIOS traffic to and from the server can be done using the command:

```
tethereal -i eth1 -p -f 'port 137 or 138 or 139'
```

The `p` option runs the program without putting the interface into promiscuous mode. In many companies, special permission must be granted before running a protocol analyzer in promiscuous mode. The `f` option sets the filter string. Ports 137, 138, and 139 are all the ports defined in `/etc/services` for NetBIOS traffic. The output of the command shown in Example 5-18 contains mainly broadcast traffic.

*Example 5-18 Show all NetBIOS traffic*

---

```
linux:~ # tethereal -p -i eth1 -f 'port 137 or 138 or 139'
Capturing on eth1
0.000000 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
0.754595 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
1.509200 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
4.130283 78-ba897.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WTRNTDM<1c>
4.880309 78-ba897.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WTRNTDM<1c>
5.630557 78-ba897.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WTRNTDM<1c>
6.187107 ibm-qu716sr9cl6 -> 9.24.105.255 BROWSER Host Announcement KA6BRRA, Workstation,
Server, NT Workstation, NT Server, Backup Browser
7.085537 65652ksv -> 9.24.105.255 BROWSER Host Announcement M23CABXK, Workstation,
Server, NT Workstation, NT Server, Backup Browser
7.296587 m23x2640.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
7.761838 m23kk904.itso.ral.ibm.com -> 9.24.105.255 BROWSER Host Announcement M23KK904,
Workstation, Server, NT Workstation, NT Server, Potential Browser
8.045579 m23x2640.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
8.732341 byron5500.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WTRNTDM<1c>
8.732976 byron5500.itso.ral.ibm.com -> 9.24.105.255 NETLOGON SAM LOGON request from
client
8.795417 m23x2640.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
13.443810 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
14.197594 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
14.948812 itsons.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WTRNTBAK<20>
14.952186 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1b>
17.196362 wtrntbak.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB ITSONS<20>
18.684232 m23x2640.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1c>
19.434101 m23x2640.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1c>
20.183985 m23x2640.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1c>
22.820827 vdputteg.itso.ral.ibm.com -> 9.24.105.255 BROWSER Host Announcement VDPUTTEG,
Workstation, Server, NT Workstation, Potential Browser
23.912973 68622ksv -> 9.24.105.255 NBNS Name query NB BJD1M0<1b>
24.663972 68622ksv -> 9.24.105.255 NBNS Name query NB BJD1M0<1b>
24.882039 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1c>
25.414963 68622ksv -> 9.24.105.255 NBNS Name query NB BJD1M0<1b>
25.636634 a23ff426.itso.ral.ibm.com -> 9.24.105.255 NBNS Name query NB WORKGROUP<1c>
```

---

Filtering out all the broadcast traffic is done by including the host address in the filter string, as shown in Example 5-19.

*Example 5-19 Just NetBIOS traffic addressed to server*

---

```
[root@portall root]# tethereal -p -i eth1 -f 'host 9.24.105.99 and (port 137 or 138 or
139)'
```

Capturing on eth1

```
0.000000 ibm-76a6i5kadj8 -> portall.itso.ral.ibm.com SMB NT Create AndX Request, Path:
\srvsvc
0.003648 portall.itso.ral.ibm.com -> ibm-76a6i5kadj8 SMB NT Create AndX Response, FID:
0x70b4
```

```

0.004048 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com DCERPC Bind: UUID
4b324fc8-1670-01d3-1278-5a47bf6ee188 ver 3.0
0.004636 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 DCERPC Bind ack: accept max_xmit:
5680 max_recv: 5680
0.004942 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com SRVSVC rqst
SRV_NETSHAREENUM_ALL(...)
0.005174 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 SRVSVC rply
SRV_NETSHAREENUM_ALL(...)
0.005622 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com SMB Close Request, FID: 0x70b4
0.006655 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 SMB Close Response
0.019751 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com DCERPC Request: opnum: 69 ctx_id:0
0.020213 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 DCERPC Response: call_id: 42
ctx_id:0
0.020788 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com DCERPC Request: opnum: 29 ctx_id:0
0.021137 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 DCERPC Response: call_id: 43
ctx_id:0
0.022742 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com SMB NT Create AndX Request, Path:
\winreg
0.023053 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 SMB NT Create AndX Response, FID:
0x70b5
0.025450 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com DCERPC Bind: UUID
338cd001-2244-31f1-aaaa-900038001003 ver 1.0
0.025590 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 DCERPC Bind ack: accept max_xmit:
5680 max_recv: 5680
0.027634 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com REG rqst REG_OPEN_HKLM(...)
0.027985 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 REG rply REG_OPEN_HKLM(...)
0.028677 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com REG rqst REG_OPEN_ENTRY(...)
0.029046 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 REG rply REG_OPEN_ENTRY(...)
0.029369 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com REG rqst REG_CLOSE(...)
0.029644 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 REG rply REG_CLOSE(...)
0.030157 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com SMB Close Request, FID: 0x70b5
0.030380 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 SMB Close Response
0.200396 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com TCP 1990 > netbios-ssn [ACK]
Seq=2101757969 Ack=383092087 Win=16667 Len=0
3.189731 ibm-76a6i5kadj8 -> portal1.itso.ral.ibm.com SMB Tree Connect AndX Request, Path:
\\PORTAL1\IPC$
3.191007 portal1.itso.ral.ibm.com -> ibm-76a6i5kadj8 SMB Tree Connect AndX Response

```

---

Capturing all the NetBIOS traffic from host jojo to the Samba server is accomplished by command:

```
tethereal -p -i eth1 -f 'host jojoj and (port 137 or 138 or 139)'
```

When the summary information is not enough to find the problem, the complete packet decode is required. Using the V option causes tethereal to print the protocol tree for each packet. Unless there only a few packets, the output should be piped to a file. The command string in Example 5-20 displays all the NetBIOS traffic between the Samba server and client jojo and sends the output to file /tmp/capture.

*Example 5-20 Protocol tree output*

---

```

tethereal -i eth1 -V -p -f 'host jojo and (port 137 or 138 or 139)' | tee /tmp/capture
Capturing on eth1
Frame 1 (74 on wire, 74 captured)
  Arrival Time: Nov 15, 2002 13:11:25.157535000
  Time delta from previous packet: 0.000000000 seconds
  Time relative to first packet: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 74 bytes
  Capture Length: 74 bytes

```



```

Ethernet II
  Destination: 00:02:55:7c:75:1b (IBM_7c:75:1b)
  Source: 00:02:55:7c:75:18 (IBM_7c:75:18)
  Type: IP (0x0800)
Internet Protocol, Src Addr: jojo (9.24.105.112), Dst Addr: portall (9.24.105.99)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 60
  Identification: 0x330d
  Flags: 0x04
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
  Header checksum: 0x22ac (correct)
  Source: jojo (9.24.105.112)
  Destination: portall (9.24.105.99)
Transmission Control Protocol, Src Port: 32982 (32982), Dst Port: netbios-ssn (139), Seq:
1957020879, Ack: 0
  Source port: 32982 (32982)
  Destination port: netbios-ssn (139)
  Sequence number: 1957020879
  Header length: 40 bytes
  Flags: 0x0002 (SYN)
    0... .... = Congestion Window Reduced (CWR): Not set
    .0.. .... = ECN-Echo: Not set
    ..0. .... = Urgent: Not set
    ...0 .... = Acknowledgment: Not set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..1. = Syn: Set
    .... ...0 = Fin: Not set
Window size: 5840
  Checksum: 0x19dc (correct)
  Options: (20 bytes)
    Maximum segment size: 1460 bytes
    SACK permitted
    Time stamp: tsval 17069693, tsecr 0
    NOP
    Window scale: 0 bytes

```

Frame 2 (74 on wire, 74 captured)

---

Since so much detailed information is produced, it will take time to understand the information in the capture. A summary capture output showing the same client activity will help in understanding the detailed capture output.

## 5.7 Sources of additional information

There is more information about testing Samba using the programs that come with the Samba suite in:

```
file:///usr/share/samba-2.2.7/docs/textdocs/DIAGNOSIS.txt
```

The sources *Troubleshooting Techniques* and *Samba 2.0.x Troubleshooting Guide* contain good information about solving Samba problems. Both are available on the official Samba projects Web site at:

<http://www.samba.org>



## A brief introduction to Layer 4-7 Switching

This chapter provides a brief overview of how Layer 4-7 Switching works. The goals are to present an alternative to traditional network design and to provide enough background to understand how a Layer 2-7 switch can be beneficial to a network. While this chapter gives a brief overview of the features and benefits of Layer 4-7 switching, it also mentions the Layer 2-7 GbE Switch Module or GbESM. For a more in-depth look at Layer 4-7 Switching, refer to the Redpaper *IBM @server BladeCenter Layer 2-7 Network Switching*, REDP3755.

## 6.1 Layer 4-7 Switching

Most networks employ multiple servers without server load balancing. Each server usually specializes in providing one or two unique services. However, a server that provides applications or data in high demand can become overutilized. If this happens, it can strain network resources since when the server starts rejecting user requests, the users resubmit the requests for data. This often happens on networks where several other servers are sitting idle with resources available to service users.

Layer 4-7 Switching can harness these available idle servers without additional special equipment such as dedicated load-balancing servers. The term L4-7 is used because these switches are Layer 4 (TCP) aware. These switches use headers and data found at the OSI Layer 7 to deliver many of their key features. Layer 2 and Layer 3 switches operate on and are aware of Layers 2-3 only.

Layer 4-7 Switching can be used to improve the reliability, scalability, and performance of a wide variety of applications and services. Layer 4-7 isolates the delivery of a service, from a user's point of view, from the physical reality of how that service is delivered. A Layer 4-7 switch is aware of the services provided by each server. Based on several load-balancing algorithms, a switch can direct user session traffic to an appropriate server. This means that in addition to using the available resources on otherwise idle servers, resources can be provisioned "on the fly". This lets network administrators add or subtract to the service delivery capability to react to server failures, meet demands during peak periods and scale back resources once demand is over. All of this happens with no knowledge or participation from the users of that service.

To take advantage of L4-7 Switching, services or applications advertise themselves using normal hostnames such as `www.ibm.com` to the outside world. However, DNS resolution will resolve that hostname back to a Virtual IP Address (V\_IP) assigned to an L4-7 switch. A service advertised by a V\_IP is a Virtual Service. When application requests are sent from users to a V\_IP, the L4-7 switch forwards the request to one or more real servers with real IP addresses.

The collection of real servers to which a request for a particular Virtual Service can be sent is called the Virtual Service Pool. By adding real servers to a Virtual Service Pool, the total application delivery throughput can be increased and application delivery times reduced. By moving real servers between Virtual Service Pools, shifting loads and demands between services can be met without having to provision enough servers for each application to meet the peak demands (which would result in several unused servers in off-peak times). Figure 6-1 on page 97 shows how the Layer 2-7 GbE Switch Module installed in BladeCenter could be used to redeploy blades to service a few different applications according to demand.

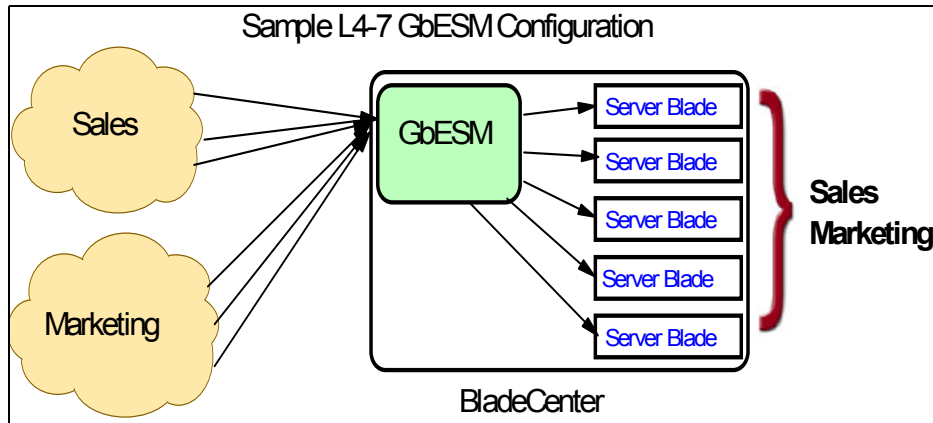


Figure 6-1 Sample L4-7 configuration

Figure 6-1 shows how services can be deployed using Layer 4-7 Switching. Using the GbESM in the BladeCenter, all server resources can be configured to support all applications, with the GbESM spreading the load among them at all times. As the loads on Sales and Marketing vary throughout the day or week or month, resources are automatically allocated in real time to meet the need.

In this scenario, to provide load balancing for any particular type of service, each server blade in the pool must have access to identical content, either directly (duplicated on each server) or through a back-end network (mounting the same file system or database server).

The GbESM acts as a front end to the servers, interpreting user session requests and distributing them among the available servers. Load balancing in the GbESM can be done in the following ways.

### Virtual server-based load balancing

This is the traditional load-balancing method. The switch is configured to act as a virtual server and is given a V\_IP for each service it will distribute. Each virtual server is assigned a list of the IP addresses (or range of addresses) of the real servers in the pool where its services reside. When the user stations request connections to a service, they will communicate with a virtual server on the switch. When the switch receives the request, it binds the session to the IP address of the best available real server and remaps the fields in each frame from virtual addresses to real addresses. HTTP, IP, FTP, RTSP, IDS, and static session WAP are examples of some of the services that use virtual servers for load balancing.

### Filter-based load balancing

A filter allows you to control the types of traffic permitted through the switch. Filters are configured to allow, deny, or redirect traffic according to the IP address, protocol, or Layer 4 port criteria. In filter-based load balancing, a filter is used to redirect traffic to a real server group. If the group is configured with more than one real server entry, redirected traffic is load balanced among the available real servers in the group. Firewalls, WAP with RADIUS snooping, IDS, and WAN links use redirection filters to load balance traffic.

### Content-based load balancing

Content-based load balancing uses Layer 7 application data (such as URL, cookies, and Host Headers) to make intelligent load balancing decisions. URL-based load balancing, browser-smart load balancing, and cookie-based preferential load balancing are a few examples of content-based load balancing.

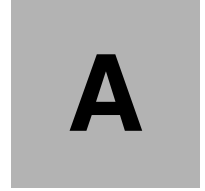
In the example in Figure 6-1 on page 97, virtual server load balancing is used. The switch has two different V\_IPs configured which correspond to each of the services (Sales and Marketing). DNS responds with these V\_IPs when these services are requested. The GbESM is also configured for the real IP addresses (R\_IPs) that are owned by blades that support requests coming into each V\_IP. In this case, all server blades can respond to requests for all services, so each V\_IP is assigned the entire set of R\_IPs.

A TCP connection consists of a series of packets sent back and forth from two destinations. If packets are misrouted and sent to the wrong destination, the session will slow down due to retransmissions and possibly fail if misrouting continues. Therefore, a Layer 4-7 switch needs to be TCP-aware in the sense that it needs to be able to:

- ▶ Identify the beginning of a new TCP connection
- ▶ Assign that connection to a real server
- ▶ Make sure that all ensuing packets related to that TCP connection continue to be sent to the same real server

This requirement is what puts the “Layer 4” in L4-7. The GbESM provides this capability. All packets arriving that are destined to a V\_IP are inspected to determine whether they are associated with an existing TCP connection (in which case they are re-directed to the real server already assigned) or whether they are a request to set up a new TCP connection. If the received packet is a request to establish a new TCP connection (a TCP SYN packet), the GbESM will determine the best available server to re-direct that request to and then do so. The “best available” consideration can be made based upon a number of factors that are beyond the scope of this chapter. It is enough to say that “best available” is based on a consideration of the present health and load of each of the candidate real servers.

This chapter introduces the concepts of Layer 4-7 Switching and how it benefits customers deploying applications on the IBM @server BladeCenter. For a more in-depth look at Layer 4-7 Switching, refer to *IBM @server BladeCenter Layer 2-7 Network Switching*, REDP3755. In addition to expanding on the concepts discussed here, this Redpaper is an excellent guide to deploying the GbESM in both Nortel and Cisco networking environments.



# **Samba configuration file**

This appendix provides a sample configuration file.

## Sample smb.conf with comments

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
# # Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable #
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors. #
#===== Global Settings =====
[global]
# workgroup = NT-Domain-Name or Workgroup-Name
workgroup = LINUX
# server string is the equivalent of the NT Description field
server string = Samba Server on Red Hat Linux
# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
; hosts allow = 192.168.1. 192.168.2. 127.
# if you want to automatically load your printer list rather
# than setting them up individually then you'll need this
printcap name = /etc/printcap
load printers = yes
# It should not be necessary to spell out the print system type unless
```



```
# yours is non-standard. Currently supported print systems include:
# bsd, sysv, plp, lprng, aix, hpux, qnx
;   printing = bsd

# Uncomment this if you want a guest account, you must add this to /etc/passwd
# otherwise the user "nobody" is used
;   guest account = pcguest

# this tells Samba to use a separate log file for each machine
# that connects
log file = /var/log/samba/log.%m
log file = /var/log/samba/log.%S

# Put a capping on the size of the log files (in Kb).
max log size = 50

# Security mode. Most people will want user level security. See
# security_level.txt for details.
security = user

# Use password server option only with security = server
;   password server = <NT-Server-Name>

# Password Level allows matching of _n_ characters of the password for
# all combinations of upper and lower case.
;   password level = 8
;   username level = 8

# You may wish to use password encryption. Please read
# ENCRYPTION.txt, Win95.txt and WinNT.txt in the Samba documentation.
# Do not enable this option unless you have read those documents
encrypt passwords = yes
```

```

smb passwd file = /etc/samba/smbpasswd

# The following are needed to allow password changing from Windows to
# update the Linux system password also.
# NOTE: Use these with 'encrypt passwords' and 'smb passwd file' above.
# NOTE2: You do NOT need these to allow workstations to change only
#         the encrypted SMB passwords. They allow the UNIX password
#         to be kept in sync with the SMB password.
; UNIX password sync = Yes
; passwd program = /usr/bin/passwd %u

# UNIX users can map to different SMB User names
; username map = /etc/samba/smbusers

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting
; include = /etc/samba/smb.conf.%m

# Most people will find that this option gives better performance.
# See speed.txt and the manual pages for details
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

# Configure Samba to use multiple interfaces
# If you have multiple network interfaces then you must list them
# here. See the man page for details.
; interfaces = 192.168.12.2/24 192.168.13.2/24

# Configure remote browse list synchronisation here
# request announcement to, or browse list sync from:

```

```
#      a specific host or from / to a whole subnet (see below)
;  remote browse sync = 192.168.3.25 192.168.5.255
# Cause this host to announce itself to local subnets here
;  remote announce = 192.168.1.255 192.168.2.44

# Browser Control Options:
# set local master to no if you don't want Samba to become a master
# browser on your network. Otherwise the normal election rules apply
;  local master = no

# OS Level determines the precedence of this server in master browser
# elections. The default value should be reasonable
;  os level = 33

# Domain Master specifies Samba to be the Domain Master Browser. This
# allows Samba to collate browse lists between subnets. Don't use this
# if you already have a Windows NT domain controller doing this job
;  domain master = yes

# Preferred Master causes Samba to force a local browser election on startup
# and gives it a slightly higher chance of winning the election
;  preferred master = yes

# Use only if you have an NT server on your network that has been
# configured at install time to be a primary domain controller.
;  domain controller = <NT-Domain-Controller-SMBName>

# Enable this if you want Samba to be a domain logon server for
# Windows95 workstations.
;  domain logons = yes
```

```

# if you enable domain logons then you may want a per-machine or
# per user logon script
# run a specific logon batch file per workstation (machine)
; logon script = %m.bat
# run a specific logon batch file per username
; logon script = %U.bat

# Where to store roving profiles (only for Win95 and WinNT)
# %L substitutes for this servers netbios name, %U is username
# You must uncomment the [Profiles] share below
; logon path = \\%L\Profiles\%U

# All NetBIOS names must be resolved to IP Addresses
# 'Name Resolve Order' allows the named resolution mechanism to be specified
# the default order is "host lmhosts wins bcast". "host" means use the UNIX
# system gethostbyname() function call that will use either /etc/hosts OR
# DNS or NIS depending on the settings of /etc/host.config, /etc/nsswitch.conf
# and the /etc/resolv.conf file. "host" therefore is system configuration
# dependant. This parameter is most often of use to prevent DNS lookups
# in order to resolve NetBIOS names to IP Addresses. Use with care!
# The example below excludes use of name resolution for machines that are NOT
# on the local network segment
# - OR - are not deliberately to be known via lmhosts or via WINS.
; name resolve order = wins lmhosts bcast

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable it's WINS Server
wins support = yes

# WINS Server - Tells the NMBD components of Samba to be a WINS Client

```

```

#      Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# WINS Proxy - Tells Samba to answer name resolution queries on
# behalf of a non WINS capable client, for this to work there must be
# at least one WINS Server on the network. The default is NO.
;   wins proxy = yes

# DNS Proxy - tells Samba whether or not to try to resolve NetBIOS names
# via DNS nslookups. The built-in default for versions 1.9.17 is yes,
# this has been changed in version 1.9.18 to no.
dns proxy = no

# Case Preservation can be handy - system default is _no_
# NOTE: These can be set on a per share basis
;   preserve case = no
;   short preserve case = no

# Default case is normally upper case for all DOS files
;   default case = lower

# Be very careful with case sensitivity - it can break things!
;   case sensitive = no

#===== Share Definitions =====
[homes]
comment = Home Directories
path = %H
create mask = 0700
directory mask = 0700
browseable = no

```

```

# Un-comment the following and create the netlogon directory for Domain Logons
; [netlogon]
;   comment = Network Logon Service
;   path = /home/netlogon
;   guest ok = yes
;   writable = no
;   share modes = no

# Un-comment the following to provide a specific roving profile share
# the default is to use the user's home directory
;[Profiles]
;   path = /home/profiles
;   browseable = no
;   guest ok = yes

# NOTE: If you have a BSD-style print system there is no need to
# specifically define each individual printer
[printers]
comment = All Printers
path = /var/spool/lpd
browseable = no
# Set public = yes to allow user 'guest account' to print
guest ok = no
writable = no
printable = yes

# This one is useful for people to share files
;[tmp]

```

```

; comment = Temporary file space
; path = /tmp
; read only = no
; public = yes

# A publicly accessible directory, but read only, except for people in
# the "staff" group
[public]
comment = Public Stuff
path = /home/public
; public = yes
read only = No
; write list = @staff
directory mask = 0777
write list = root

# Other examples.
#
# A private printer, usable only by fred. Spool data will be placed in fred's
# home directory. Note that fred must have write access to the spool directory,
# wherever it is.
;[fredsprn]
; comment = Fred's Printer
; valid users = fred
; path = /homes/fred
; printer = fred's_printer
; public = no
; writable = no
; printable = yes

```

```

# A private directory, usable only by fred. Note that fred requires write
# access to the directory.
;[fredsdir]
;  comment = Fred's Service
;  path = /usr/somewhere/private
;  valid users = fred
;  public = no
;  writable = yes
;  printable = no

# a service which has a different directory for each machine that connects
# this allows you to tailor configurations to incoming
# The %m gets replaced with the machine name that is connecting.
;[pchome]
;  comment = PC Directories
;  path = /usr/pc/%m
;  public = no
;  writable = yes

# A publicly accessible directory, read/write to all users. Note that all files
# created in the directory by users will be owned by the default user, so
# any user with access can delete any other user's files. Obviously this
# directory must be writable by the default user. Another user could of course
# be specified, in which case all files would be owned by that user instead.
;[public]
;  path = /usr/somewhere/else/public
;  public = yes
;  only guest = yes
;  writable = yes
;  printable = no

```



```
# The following two entries demonstrate how to share a directory so that two
# users can place files there that will be owned by the specific users. In this
# setup, the directory should be writable by both users and should have the
# sticky bit set on it to prevent abuse. Obviously this could be extended to
# as many users as required.
```

```
:[myshare]
```

```
; comment = Mary's and Fred's stuff
; path = /usr/somewhere/shared
; valid users = mary fred
; public = no
; writable = yes
; printable = no
; create mask = 0765
```

```
[Samba Docs]
```

```
path = /usr/share/doc/samba-2.2.6/docs
read only = yes
comment = Samba Documentation
```



# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this Redpaper.

## IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 112.

- ▶ *The Cutting Edge: IBM @server BladeCenter*, REDP3581
- ▶ *IBM @server BladeCenter Systems Management*, REDP3582
- ▶ *Deploying Citrix MetaFrame on IBM @server BladeCenter*, REDP3583
- ▶ *Deploying Lotus Domino on IBM @server BladeCenter*, REDP3584
- ▶ *Deploying Microsoft Exchange on IBM @server BladeCenter*, REDP3585
- ▶ *Deploying Apache on IBM @server BladeCenter*, REDP3588
- ▶ *Linux on IBM Netfinity Servers: A Collection of Papers*, SG24-5994-00
- ▶ *Red Hat Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5853-01
- ▶ *SuSE Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5863-01
- ▶ *IBM @server BladeCenter Layer 2-7 Network Switching*, REDP3755.

## Referenced Web sites

These Web sites are also relevant as further information sources:

- ▶ Location or Red Hat boot diskette  
<http://people.redhat.com/msw/boot-usb-sleep-7.3.img>
- ▶ Red Hat documentation  
<http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-diskpartsetup.html>  
<http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-firewallconfig.html>  
<http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/install-guide/s1-xconfig.html>
- ▶ Samba home page  
<http://www.samba.org/>
- ▶ Linux Documentation home page  
<http://www.linuxdoc.org/>
- ▶ Samba documentation  
<http://us1.samba.org/samba/ftp/appliance/windbind.pdf>  
<http://us6.samba.org/samba/ftp/htmldocs/windbind.html>  
<http://us2.samba.org/samba/docs/man/windbindd.8.html>

- ▶ IBM ServerProven  
<http://www.ibm.com/pc/compat/>
- ▶ IBM @server BladeCenter - Power Module Upgrade Guidelines  
<http://www-1.ibm.com/support/docview.wss?uid=psg1MIGR-53353>
- ▶ IBM @server BladeCenter - Power Module Upgrade Guidelines  
[ftp://ftp.software.ibm.com/pc/pccbbs/pc\\_servers\\_pdf/13n0308.pdf](ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/13n0308.pdf)

## How to get IBM Redbooks

You can order hardcopy Redbooks, as well as view, download, or search for Redbooks at the following Web site:

[ibm.com/redbooks](http://ibm.com/redbooks)

You can also download additional materials (code samples or diskette/CD-ROM images) from that site.

## IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the **CD-ROMs** button on the Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.





# Deploying Samba on IBM **@server** BladeCenter



**Installing Red Hat 7.3,  
SuSE 8.1 Linux and  
IBM Director**

**Installing Samba**

**Managing Samba  
using SWAT**

Considering how much data centers have grown with the proliferation of Intel-based servers over recent years, it is important to note that rack space and floor space can be more efficiently used with the use of the IBM **@server** BladeCenter HS20 servers. Attractive cost savings are also possible where a large number of rack installed servers are required, since the equivalent number of 1U servers would be much more expensive.

This IBM Redpaper describes how to set up and configure Linux and Samba on the IBM **@server** BladeCenter and provides some pointers on managing the installation. It also describes the functionality of the IBM **@server** BladeCenter in this type of environment.

**INTERNATIONAL  
TECHNICAL  
SUPPORT  
ORGANIZATION**

**BUILDING TECHNICAL  
INFORMATION BASED ON  
PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:  
[ibm.com/redbooks](http://ibm.com/redbooks)**