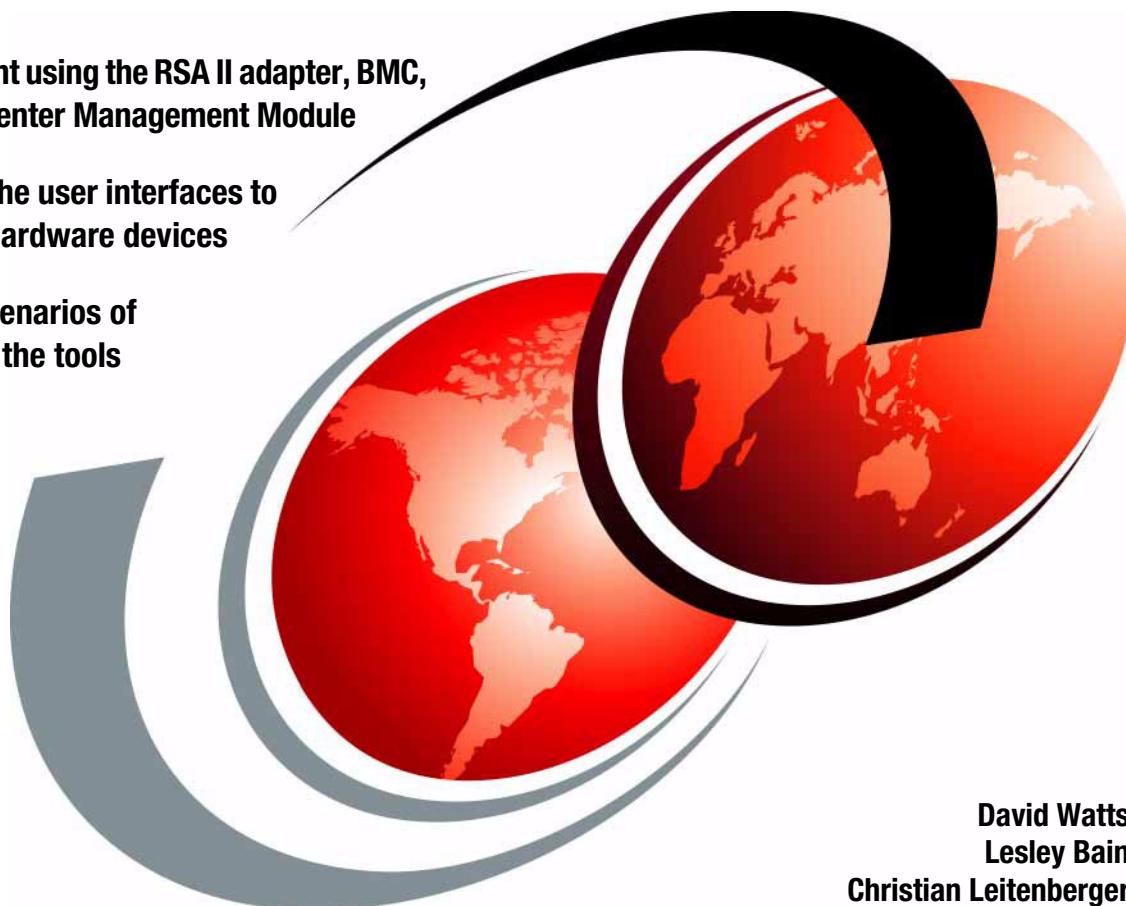


IBM eServer xSeries and BladeCenter Server Management

Management using the RSA II adapter, BMC,
and BladeCenter Management Module

Describes the user interfaces to
use these hardware devices

Includes scenarios of
how to use the tools



David Watts
Lesley Bain
Christian Leitenberger

Redbooks



International Technical Support Organization

**IBM @server xSeries and BladeCenter Server
Management**

March 2005

Note: Before using this information and the product it supports, read the information in "Notices" on page vii.

First Edition (March 2005)

This edition applies to:

- ▶ Baseboard Management Controller in xSeries servers and the eServer 325/326
- ▶ Remote Supervisor Adapter II, part 59P2984
- ▶ Remote Supervisor Adapter II SlimLine, part 73P9341
- ▶ Remote Supervisor Adapter II-EXA, part 13N0382
- ▶ BladeCenter Management Module

© Copyright International Business Machines Corporation 2005. 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

Notices	vii
Trademarks	viii
Preface	ix
The team that wrote this redbook	ix
Become a published author	xi
Comments welcome	xi
Chapter 1. Introduction	1
1.1 Service processors supported in xSeries servers	2
1.2 Industry standards	4
1.2.1 Distributed Management Task Force	4
1.2.2 IPMI	5
1.2.3 SNMP	6
Chapter 2. Baseboard Management Controller	7
2.1 Feature comparison	8
2.2 BMC in the e325 and e326	9
2.2.1 External connections	9
2.2.2 Upgrading the BMC firmware	10
2.2.3 Configuring the BMC	11
2.2.4 Installing the OSA IPMI device drivers	17
2.2.5 Event log	18
2.3 BMC in the xSeries Servers	18
2.3.1 Functionality	18
2.3.2 External connections	19
2.3.3 Updating the BMC firmware	22
2.3.4 Configuring the BMC using BMC_CFG	22
2.3.5 Configuring the BMC in BIOS	34
2.3.6 Event Log	35
2.3.7 Configuring the BMC with IBM Director	37
2.3.8 Remote control	40
2.3.9 Installing the BMC device drivers	40
2.3.10 Ports used by the BMC	44
2.4 Integrated system management processors	44
2.4.1 Features	45
2.4.2 Limitations	45
2.4.3 Configuration	46

Chapter 3. Remote Supervisor Adapter II	47
3.1 Functions and features	48
3.2 Overview of the Remote Supervisor Adapter family	49
3.2.1 Remote Supervisor Adapter II	50
3.2.2 Remote Supervisor Adapter II-EXA	52
3.2.3 Remote Supervisor Adapter II SlimLine	53
3.3 Advanced Systems Management network	55
3.3.1 Specifying the ASM Gateway	58
3.4 Basic configuration of Remote Supervisor Adapter II	59
3.4.1 Installing the RSA II	60
3.4.2 Network settings	60
3.4.3 Update firmware	62
3.4.4 Installing the device driver	64
3.4.5 MIB files	67
3.5 Remote console and remote media	67
3.5.1 Linux support for remote control	70
3.5.2 Using remote media	74
3.5.3 Remote diskette	77
3.5.4 Remote CD-ROM and DVD	80
3.5.5 Remote file	82
3.6 Ports used by Remote Supervisor Adapter II	85
Chapter 4. BladeCenter management module	87
4.1 Features and functions	88
4.2 Basic configuration of the management module	91
4.2.1 Installation in a BladeCenter	91
4.2.2 Network settings	92
4.2.3 Update firmware	95
4.2.4 MIB files	97
4.3 Redundant management modules	97
4.3.1 Installation and cabling	97
4.3.2 Manual switch over	99
4.4 Remote console and remote media	100
4.4.1 Linux support for remote control	104
4.4.2 Using remote media	105
4.4.3 Remote diskette	108
4.4.4 Remote CD-ROM and DVD	112
4.4.5 Remote file	115
4.5 Basic configuration of blade-specific features	119
4.5.1 Device drivers	119
4.5.2 Blade tasks	120
4.5.3 I/O Module tasks	124
4.6 Ports used by the management module	126

4.7 Resetting the management module back to factory defaults	127
Chapter 5. Security and authentication	129
5.1 Security using SSL	130
5.1.1 Secure Sockets Layer (SSL)	130
5.1.2 Secure Shell (SSH)	135
5.2 Authentication using LDAP	139
5.2.1 LDAP authentication attribute	140
5.2.2 Configuring the LDAP server	141
5.2.3 Testing the LDAP server configuration	148
5.2.4 Configuring the LDAP client	150
Chapter 6. System management utilities	157
6.1 Comparing the tools	158
6.2 Advanced Settings Utility	160
6.2.1 Support list for ASU	161
6.2.2 Supported platforms for ASU	161
6.2.3 Downloading ASU and definition files	162
6.2.4 Using the ASU definition files	163
6.2.5 Using the ASU command	164
6.2.6 Using ASU to view a systems setting	166
6.2.7 Using ASU to configure RSA or RSA II settings	173
6.2.8 ASU batch commands	174
6.3 Management processor command-line interface	175
6.3.1 Supported service processor configurations	176
6.3.2 Functions	178
6.3.3 Limitations	180
6.3.4 Supported platforms for the MPCLI	180
6.3.5 Installing the MPCLI	181
6.3.6 Using the MPCLI	182
6.4 OSA SMBridge utility	192
6.4.1 Configuring BIOS	195
6.4.2 Installation	196
6.4.3 Connecting via the telnet server	199
6.4.4 Configuring Windows Server 2003 to support SOL	205
6.4.5 Configuring Red Hat Linux to support SOL	211
6.4.6 Configuring SUSE LINUX to support SOL	214
6.4.7 Connecting via the command-line interface	216
6.5 Web interface	219
6.5.1 Structure of the Web interfaces	219
6.6 Telnet interface	220
6.7 IBM Director integration	225
6.7.1 Management Processor Assistant	227

6.7.2 BladeCenter Assistant	228
6.7.3 Alerting	229
Chapter 7. Scenarios and best practices	233
7.1 Securing communication and authentication.	234
7.1.1 General considerations	234
7.1.2 Web interface	235
7.1.3 Command-line interfaces	236
7.2 Backing up and restoring the configuration.	236
7.2.1 Backup procedure	237
7.2.2 Restore procedure	238
7.3 Provide remote access to all BladeCenter modules	239
7.4 Multi-subnet environment	243
7.4.1 General considerations	243
7.4.2 Access to other subnets	244
7.4.3 DHCP in different subnets.	245
7.5 Mass configuration of user IDs and passwords.	245
7.6 Resetting the RSA II back to factory defaults	248
7.6.1 Using ASU.	249
7.6.2 Using IBM Director	250
7.6.3 Using MPCLI	252
7.7 How to use ASU remotely	253
7.8 Remote BIOS and firmware updates.	256
7.8.1 Using MPCLI to upgrade firmware	257
7.8.2 Using IBM Director to upgrade firmware	259
7.8.3 Using UpdateXpress RemoteUX to update firmware	266
7.9 UpdateXpress firmware update scripts for BladeCenter	274
Abbreviations and acronyms	285
Related publications	287
IBM Redbooks	287
Other publications	287
Online resources	288
How to get IBM Redbooks	291
Help from IBM	291
Index	293

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:

BladeCenter™

@server®

✉ server®

eServer™

ibm.com®

IBM®

Netfinity®

PowerPC®

PS/2®

RETAIN®

ServerProven®

ServeRAID™

Wake on LAN®

Redbooks (logo) ™

X-Architecture™

xSeries®

The following terms are trademarks of other companies:

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.

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

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Portions of Chapter 2 and Section 6.4 of this IBM Redbook are Copyright (c) 2004-2005 - OSA Technologies, an Avocent Company. All Rights Reserved. Used by permission.

Preface

The systems management hardware that is part of IBM @server® xSeries® and BladeCenter™ servers serves as an important part of the overall management strategy for customers. This hardware, either integrated into the server or BladeCenter chassis, installed at the factory as an adapter, or available as an option, provides vital information back to the administrator and gives the administrator the ability to remotely control the server, even when the operating system is not running.

This IBM Redbook describes the full range of management hardware currently available for the xSeries and BladeCenter systems. We cover the integrated Baseboard Management Controller, the Remote Supervisor Adapter II family of adapters, and the BladeCenter management module. The user interfaces used to access this hardware are discussed in detail, as is information on how to configure security features such as SSL and authentication features such as LDAP.

This book is aimed at customers, IBM® Business Partners, and IBM employees who need to understand the capabilities of our systems management hardware, and how to configure and use it to assist with the management of their servers.

Update July 2006: Corrected the change to the /etc/inittab file as discussed in 6.4.5, “Configuring Red Hat Linux to support SOL” on page 211 and 6.4.6, “Configuring SUSE LINUX to support SOL” on page 214.

The team that wrote this redbook

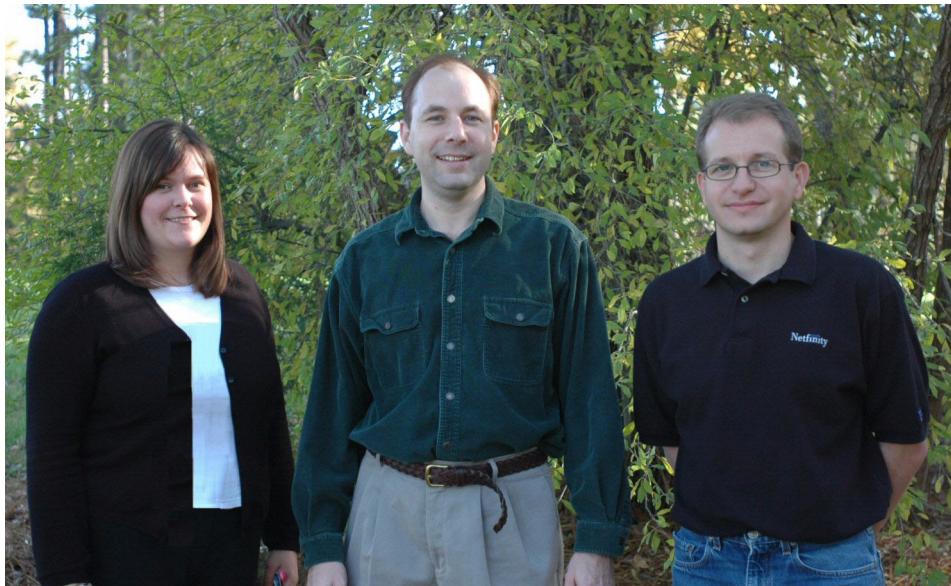
This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

David Watts is a Consulting IT Specialist at the IBM ITSO Center in Raleigh. He manages residencies and produces redbooks on hardware and software topics related to IBM @server xSeries systems and associated client platforms. He has authored over 30 redbooks and redpapers. He has a Bachelors of Engineering degree from the University of Queensland (Australia) and has worked for IBM for over 15 years. He is an IBM @server Certified Specialist for xSeries and an IBM Certified IT Specialist.

Lesley Bain is a Systems Engineer and xSeries Server Specialist working for the EMEA Advanced Technical Support Organization, and is based in Greenock,

Scotland. She has five years of experience working for the Presales Technical Support Organization and five years of experience working for the IBM Server Development and Test Organization. She has a degree in Computing Information Systems from Glasgow Caledonian University. Her area of expertise is xSeries systems management hardware and software, including the Remote Supervisor Adapter, integrated management controllers, and the IBM Director software suite.

Christian Leitenberger is a Systems Engineer and xSeries Specialist working for PROFI Engineering Systems AG, an IBM Business Partner in Germany. He has 11 years of experience in the IT field, including six years with IBM Netfinity® and xSeries servers. He graduated with a Diploma in Business Information Technology at the University of Cooperative Education (BA) in Mannheim, Germany. He is an MCSE for Windows® NT and IBM @server Certified Expert for xSeries. His areas of expertise are xSeries hardware, Windows clustering, Storage Area Networks, and VMware ESX Server.



The redbook team (left to right): Lesley, David, and Christian

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

Jay Bretzmann, Rob Sauerwalt, Bob Zuber
Worldwide xSeries Product Management

Jason Brunson, Doug Clarke, Craig Elliott
IBM xSeries Advanced Technical Support

Gerhard Buckler, Gregg Gibson, Raj Kantesaria, Eric Kern, Ed Klodnicki
IBM xSeries Systems Management Hardware

Jason Almeida, Julia Dees, Danyell Shiflett, Ileana Vila
IBM xSeries Systems Management Software

Eddy Ciliendo
IBM Switzerland

Olaf Menke
IBM Germany

Martin Gudmundsen
Scribona AS, Norway

Julie Czubik
International Technical Support Organization, Poughkeepsie Center

Reza Roodsari
IPMI Systems Architect, OSA Technologies

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'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll 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

Comments welcome

Your comments are important to us!

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

- ▶ Use the online **Contact us** review redbook form found at:
ibm.com/redbooks
- ▶ Send your comments in an email to:
redbook@us.ibm.com
- ▶ Mail your comments to:
IBM Corporation, International Technical Support Organization
Dept. HZ8 Building 662
P.O. Box 12195
Research Triangle Park, NC 27709-2195



Introduction

Important differentiators in the IBM @server xSeries server and IBM @server BladeCenter product families is the systems management features, both hardware based and software based. These features make the servers easier to manage, and provide comprehensive alerting and task-based management.

Good overall server management is key for reducing overall total cost of ownership for entry-level environments up to large high-end enterprise environments.

This book covers the hardware side of the IBM systems management solution, specifically:

- ▶ The integrated Baseboard Management Controller
- ▶ The Remote Supervisor Adapter II, both PCI and SlimLine models
- ▶ The BladeCenter management module

We explore ways to manage the xSeries servers and the BladeCenter using the available user interfaces such as the Web interface, Management Processor Command Line Interface (MPCLI), Advanced Settings Utility (ASU), and the OSA System Management Bridge (SMBridge) Utility.

A partner redbook is *Implementing Systems Management Solutions using IBM Director*, SG24-6188, which describes in detail IBM Director, the software component of the IBM systems management solution.

1.1 Service processors supported in xSeries servers

Table 1-1 details which service processors are supported in each IBM @server system. The support falls into three categories:

- ▶ No: There is no support for this service processor in this system.
- ▶ Standard: This service processor is integrated onto the system planar or is pre-installed in the server at the factory.
- ▶ Option: This service processor is available to be ordered as an optional upgrade.

Tip: The latest version of this table (including the listing of older Netfinity servers) is available as an IBM Technote, available at:

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

Table 1-1 Service processors supported in IBM @server xSeries servers

Server	ASMP	ISMP	BMC	ASM PCI Adapter	RSA	RSA II	RSA II SlimLine
xSeries 200	No	No	No	No	No	No	No
xSeries 205	No	No	No	No	Optional	Optional ¹	No
xSeries 206	No	No	No	No	No	Optional ¹	No
xSeries 220	No	No	No	No	Optional	No	No
xSeries 225 (8647)	No	No	No	No	Optional	No	No
xSeries 225 (8649)	No	No	No	No	No	Optional ¹	No
xSeries 226	No	No	No	No	No	Optional	No
xSeries 230	Standard	No	No	Optional	No	No	No
xSeries 232	No	Standard	No	No	Optional	No	No
xSeries 235	No	Standard	No	No	Optional	Optional ¹	No
xSeries 236	No	No	Standard	No	No	No	Optional
xSeries 240	Standard	No	No	Optional	No	No	No
xSeries 250	Standard	No	No	Optional	No	No	No
xSeries 255	No	Standard	No	No	Optional	Optional ¹	No
xSeries 300	No	No	No	No	No	No	No

Server	ASMP	ISMP	BMC	ASMPCI Adapter	RSA	RSA II	RSA II SlimLine
xSeries 305	No	No	No	No	Optional	Optional ¹	No
xSeries 306	No	No	No	No	No	Optional ¹	No
xSeries 330 (8654)	Standard	No	No	Optional	Optional ²	No	No
xSeries 330 (8674)	Standard	No	No	No	Optional ²	No	No
xSeries 330 (8675)	Standard	No	No	No	Optional ²	No	No
xSeries 335	No	Standard	No	No	Optional	Optional ³	No
xSeries 336	No	No	Standard	No	No	No	Optional
xSeries 340	Standard	No	No	Optional	No	No	No
xSeries 342	No	Standard	No	No	Optional	No	No
xSeries 343	No	No ⁴	No	No	No	No	No
xSeries 345	No	Standard	No	No	Optional	Optional ¹	No
xSeries 346	No	No	Standard	No	No	No	Optional
xSeries 350	Standard	No	No	Optional	No	No	No
xSeries 360	No	No	No	No	Standard	No	No
xSeries 365	No	No	No	No	No	Standard	No
xSeries 366	No	No	Standard	No	No	No	Optional
xSeries 370	No	No	No	Standard	No	No	No
xSeries 380	No	No	No	No	No	No	No
xSeries 382	No	No ⁴	No	No	No	No	No
xSeries 440	No	No	No	No	Standard	No	No
xSeries 445	No	No	No	No	Standard	Optional ⁵	No
xSeries 450	No	No	No	No	Standard	No	No
xSeries 455	No	No	No	No	Standard	No	No
xSeries 460	No	No	Standard	No	No	No	Standard
eServer™ 325	No	No	Standard	No	No	No	No
eServer 326	No	No	Standard	No	No	Yes	No

Server	ASMP	ISMP	BMC	ASMPCI Adapter	RSA	RSA II	RSA II SlimLine
Notes from the table:							
1.	The server needs the latest system BIOS, ISMP firmware, and RSA II firmware to support the Remote Supervisor Adapter II.						
2.	The xSeries 330 (8654, 8674, 8675) supports the Remote Supervisor Adapter as a gateway only. The onboard ASMP provides all the system management functions. For x330 models 8674 and 8675, you should install the I2C cable (20-pin cable), which will be used to provide the Remote Supervisor Adapter with power. The external AC power supply will only be used for redundancy. However, on the x330 model 8654, you should not install the I2C cable (20-Pin Cable), but you must use the external AC power supply that is supplied with the adapter.						
3.	The xSeries 335 supports the Remote Supervisor Adapter II; however, the C2T function of the x335 will not work with the RSA II because the adapter's video disables the onboard video. Customers will need to install an RSA II in every x335, if they want to use the remote video functionality of the RSA II. See http://www.ibm.com/pc/support/site.wss/MIGR-54747.html for more information.						
4.	The xSeries 343 and xSeries 382 have built-in service processors that provide system management functions. Installing additional service processors in these systems is not supported. See the server documentation for more information.						
5.	The xSeries 445 supports the Remote Supervisor Adapter II-EXA, part 13N0382, but not the Remote Supervisor Adapter II, part 59P2984.						

1.2 Industry standards

Industry standards are important in today's IT environments to enable companies to select a product that suits their environment the best, without needing to worry about whether the product will be able to support a new piece of hardware when it is introduced in the future.

IBM is a strong advocate of using industry standard technologies, and uses these standards in the full IBM @server range. This section describes the key systems management standards.

1.2.1 Distributed Management Task Force

The Distributed Management Task Force (DMTF) develops the guidelines, standards, and documentation for a number of systems management standards, including the following:

- ▶ Common Information Model (CIM)

CIM provides a common definition of management information for systems, networks applications, and services, and allows for vendor extensions. Its

common definitions enable vendors to exchange semantically rich management information between systems throughout the network.

- ▶ **Web-based Enterprise Management (WEBEM)**

This initiative is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.

- ▶ **Alert Standard Format (ASF)**

This specification defines remote control and alerting interfaces for pre-boot environments.

- ▶ **Systems Management BIOS (SMBIOS)**

This SMBIOS specification addresses how motherboard and system vendors present management information about their products in a standard format by extending the BIOS interface on Intel® architecture system.

- ▶ **Desktop Management Interface (DMI)**

These standards generate a standard framework for managing and tracking components in a desktop PC, notebook, or server.

- ▶ **Directory Enabled Network (DEN)**

The Directory Enabled Network initiative is designed to provide building blocks for intelligent management by mapping concepts from CIM (such as systems, services, and policies) to a directory, and integrating this information with other WEBEM elements in the management infrastructure.

- ▶ **Systems Management Architecture for Server Hardware (SMASH)**

SMASH is a suite of specifications that deliver architectural semantics, industry standard protocols, and profiles to unify the management of the data center.

More detailed information on any of the standards above can be found at:

<http://www.dmtf.org/standards>

1.2.2 IPMI

Intelligent Platform Management Interface (IPMI) defines a common platform instrumentation interface to enable interoperability between:

- ▶ The onboard (baseboard) management controller and chassis
- ▶ The baseboard management controller and systems management software
- ▶ Between servers

IPMI enables the following:

- ▶ Common access to platform management information, consisting of:
 - Local access via systems management software
 - Remote access via LAN and serial/modem
 - Inter-chassis access via Intelligent Chassis Management Bus (ICMB)
 - Access via LAN, serial/modem, IPMB, PCI SMBus, or ICMB, available even if the processor is down
- ▶ Support for a wide range of servers, including porting to new server designs.
- ▶ IPMI interface isolates systems management software from hardware.
- ▶ Hardware advancements can be made without impacting the systems management software.
- ▶ IPMI facilitates cross-platform management software.

You can find more information on IPMI at the following URL:

<http://www.intel.com/design/servers/ipmi>

1.2.3 SNMP

Simple Network Management Protocol (SNMP) is a set of Internet standards for communicating with devices such as servers, workstations, printers, routers, switches, and hubs connected on an TCP/IP network.

A device is said to be SNMP compatible if it can be monitored and/or controlled using SNMP messages. These devices contain SNMP Agent software to receive, send, and act upon SNMP messages. SNMP uses Management Information Bases (MIBs), which define the information available from any SNMP-manageable device.



Baseboard Management Controller

Many xSeries servers have service processors integrated onto the system board. These provide different levels of monitoring and alerting depending on the type of service processor used. This chapter describes these integrated service processors, including communication methods, features, functionality, cabling, and configuration of each. Discussed here are:

- ▶ The Baseboard Management Controller (BMC) used in IBM @server 325 and 326. See 2.2, “BMC in the e325 and e326” on page 9.
- ▶ The BMC used in xSeries and BladeCenter-based servers. See 2.3, “BMC in the xSeries Servers” on page 18.
- ▶ The Integrated System Management Processor (ISM Processor) found in older servers. See 2.4, “Integrated system management processors” on page 44.

A fourth type is the Advanced System Management Processor (ASM processor), which is only found in older withdrawn servers. For information on this device, see the IBM Redbook *Netfinity Server Management*, SG24-5208.

2.1 Feature comparison

Table 2-1 shows the key features that are standard on each of the three types of xSeries integrated service processors.

Table 2-1 Feature comparisons of the integrated controllers

Feature	BMC (e325 and e326)	BMC (xSeries servers)	ISM processor
RS-485 Interconnect network	No	No	Supported
Remote access via LAN/serial	Supported	Supported	Supported ¹
Serial-over-LAN	Supported	Supported	No
Remote system power control	Supported	Supported	Supported ²
Text console redirection	Supported	Supported	No
Remote out-of-band alerts	Supported	Supported	Supported ²
In-band alerts	Supported ³	Supported ³	Supported ³
Out-of-band environmental monitoring	Supported	Supported	Supported ²
System voltage monitoring	Supported	Supported	Supported
Battery voltage monitor	Supported	Supported	No
System temperature monitoring	Supported	Supported	Supported
Fan speed control	Supported	Supported	Supported
Fan tachometer monitor	Supported	Supported	Supported
Power good signal monitor	Supported	Supported	Supported
System reset control	Supported	Supported	Supported
NMI detection	Supported	Supported	Supported
SMI detection and generation	No	Supported	
Remind button detection	No	Supported	Supported
Auto Server Restart watchdog alert	Supported	Supported	Supported
System LED control (power, disk, alert)	Supported	Supported	Supported
Lightpath LED control	Supported	Supported	Supported

Feature	BMC (e325 and e326)	BMC (xSeries servers)	ISM processor
Notes:			
1.	This feature requires the addition of a Remote Supervisor Adapter II.		
2.	This feature is possible via the ASM interconnect (RS-485) or with the addition of a Remote Supervisor Adapter II.		
3.	In-band alerting requires that IBM Director Agent V4 or later is installed.		

2.2 BMC in the e325 and e326

Systems management via the BMC allows users to manage their servers locally or remotely. The BMC includes functionality such as IPMI compliance, text-console redirect or serial/shared LAN, remote out-of-band alerts, unattended firmware updates, and PXE.

The BMC is based on a QLogic chip and implements Version 1.5 of the IPMI specification. The spec document is available from:

ftp://download.intel.com/design/servers/ipmi/IPMIV1_5rev1_1-012904markup.pdf

2.2.1 External connections

The BMCs communicate via port 1 of the system Gigabit Ethernet. To communicate with the BMC you would attach a standard Ethernet cable. Refer to Table 2-2 for details on which Ethernet port is shared with the BMC to ensure successful communication.

Note: Unlike the BMCs in the xSeries servers, you cannot use PING to confirm that this connection is valid.

Table 2-2 Shared Ethernet ports with the BMC

Server	System Ethernet port shared with the BMC
eServer 325	Ethernet port 1
eServer 326	Ethernet port 1

See Figure 2-1 on page 10 for the location of the correct port.

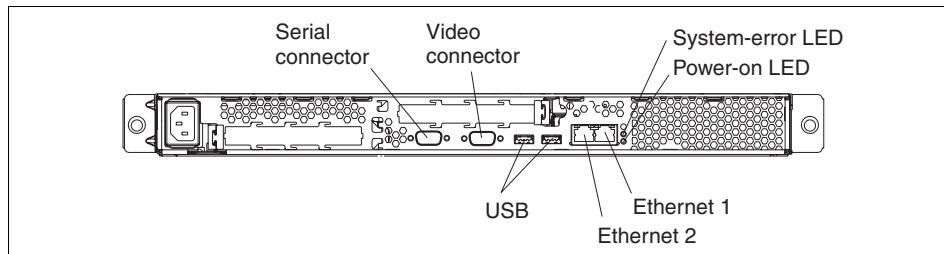


Figure 2-1 Rear connectors of the e325 and e326 servers

2.2.2 Upgrading the BMC firmware

In this section, we describe the process to upgrade the firmware of the BMC on the e325 and 326 servers.

You can download the firmware as an ISO image (which requires a CD burner to create the CD) or as an EXE file (which creates a bootable diskette). Complete the following steps to download the latest BMC firmware update:

1. Refer to the IBM technote *IBM @server xSeries BMC — Firmware and Drivers Cheatsheet*, TIPS0532, and click the link for the firmware for the appropriate server.
<http://www.redbooks.ibm.com/abstracts/tips0532.html>
Alternatively, you can navigate to the appropriate download page from:
<http://www.pc.ibm.com/support>
2. If you wish to build a diskette image, select the EXE file. If you wish to burn a CD, select the ISO file.

Note: The e325 and e326 do not have a diskette drive installed as standard. If you plan to use the EXE to create a diskette, you will need to provide a USB-attached external diskette drive to attach to the server.

3. Once the CD or diskette has been created, insert the media (attach an external USB-attached diskette drive if necessary) and restart the server.
4. If you are booting from diskette, you may need to go into the BIOS Configuration/Setup Utility program (press F1 during server startup) to configure the external USB diskette drive as a startup device.
5. Once the update has completed you are now ready to configure the BMC. Refer to 2.2.3, “Configuring the BMC” on page 11.

6. If you have already configured the BMC, remove the diskette from the drive and restart your server.

2.2.3 Configuring the BMC

The lancfg configuration utility is the method that can be used to configure this BMC. Once you have configured the network settings you are able to use IBM Director to configure user IDs, passwords, and alert-forwarding profiles. We will explore both methods below.

Configuring the BMC using lancfg

Using the lancfg configuration utility, you are able to make all the necessary configuration settings. This utility is located on the BMC firmware diskette or CD prepared earlier for upgrading the BMC firmware.

Note: You must run the LAN configuration utility (lancfg.exe) by booting to the DOS session after you start your server from the startable BMC management controller firmware update diskette/CD. Do not run the utility from a DOS window from within Windows.

1. After the BMC firmware update is completed, a command prompt is displayed. Type in `lancfg` and press Enter. The LAN configuration utility starts, and the BMC Information screen is displayed. The default values that are displayed are read only. You cannot make changes in this screen.
2. To use the LAN configuration utility, press F10 and use the arrow keys to select the menu items at the top of the window.
3. Select **LanCfg**. The LAN Configuration screen is displayed. See Figure 2-2 on page 12.

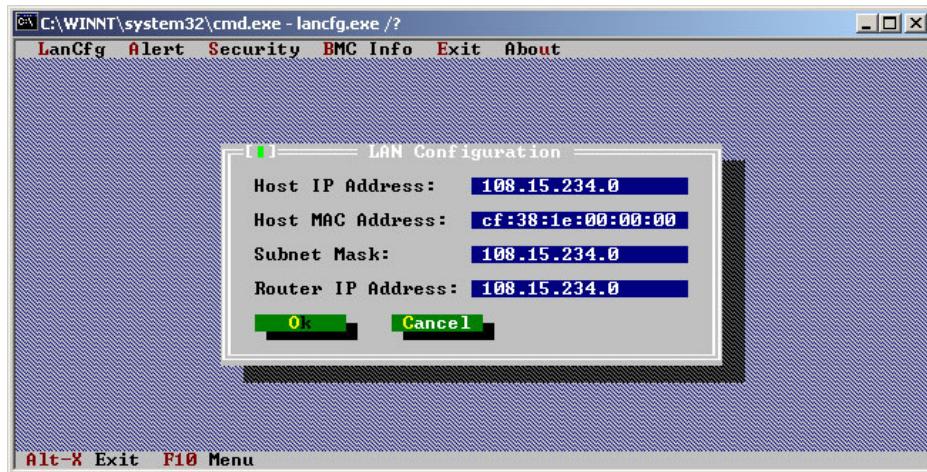


Figure 2-2 LAN configuration screen

4. Press Tab to edit the fields, type in the information requested for the BMC in the fields detailed below, and select **OK**.
 - Host IP address
 - Subnet mask
 - Router IP address

Note: The Host MAC Address field is read only and cannot be changed from the LAN configuration utility.

5. Select **OK** to close the information message.
6. Press F10 to enter the menu, then select **Alert** to enter the event destination address. The Alert Setting screen is displayed. See Figure 2-3 on page 13.

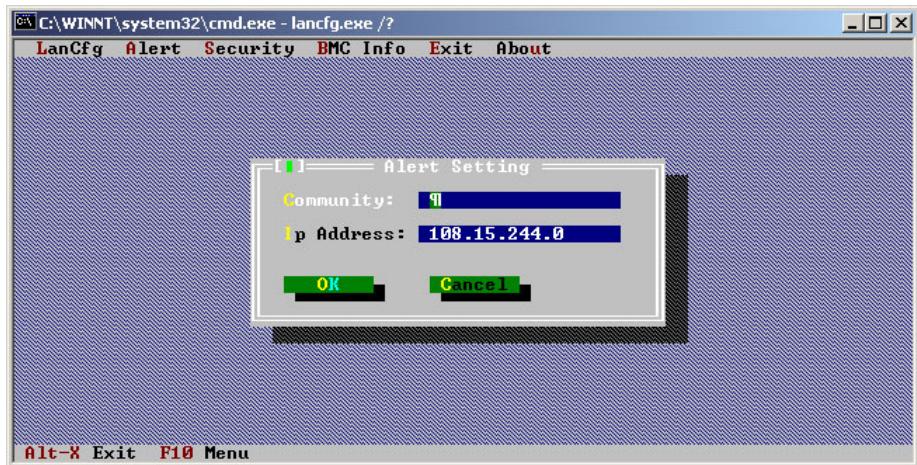


Figure 2-3 Alert Settings window

7. Type in the destination IP address where you want alerts to be sent, and also the appropriate community name in the fields. The IP address you enter is that of a Platform Event Trap (PET) listener such as IBM Director. Select **OK** to save, and select **OK** to close the information screen. LAN alerts are sent as SNMP Traps in the PET format to a specified alert destination.
8. Press F10 to enter the menu and select **Security** to view or modify the Login settings. The Security Setting screen is displayed. See Figure 2-4 on page 14.

Note: The default user ID and password are USERID and PASSW0RD (with a zero and not the letter o). This is the default user ID and password for all IBM Service processors; therefore, we will explore how to modify the user ID and password in the following sections.

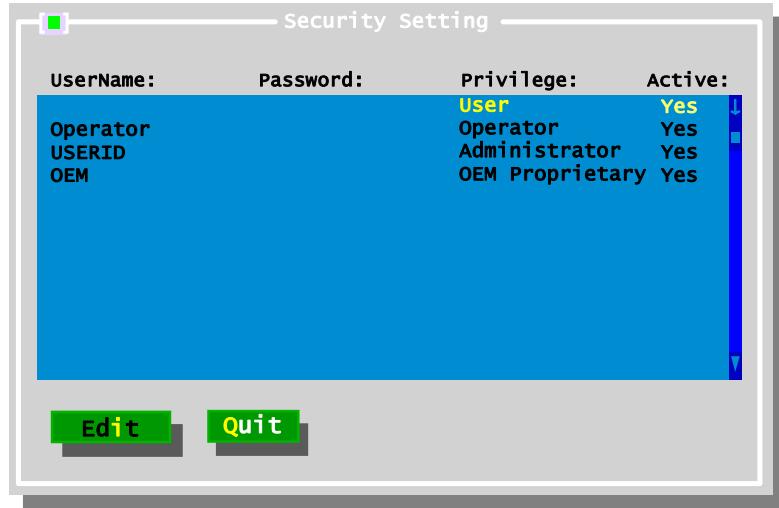


Figure 2-4 Security Settings screen

9. You can maintain the BMC user accounts on this screen. To make changes on this screen, select **Edit**, type your changes in the Edit screen, and select **OK**.
10. After you make all the changes required and before you exit the LAN configuration utility, remove the firmware update diskette from the diskette drive.
11. Select **Exit**. When you are prompted to restart the server, select **Reboot**.

Using IBM Director to configure the BMC

If you have the IBM Director server installed in your environment and the BMC network settings are configured correctly, you can use this method to configure settings on the BMC. This will also enable you to manage the BMC OOB. In this section we will describe how to configure the user ID, passwords, and alert-forwarding settings.

1. From the director console, right-click the middle pane in a blank area. Select **New → Physical Platform**.
2. You will be presented with the window shown in Figure 2-5 on page 15. Enter an appropriate name and the IP address details for the BMC you want to add, and select **OK**.

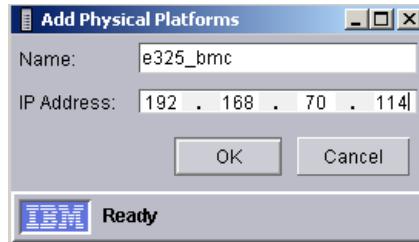


Figure 2-5 Add management processors window

3. Once the BMC is discovered it will appear as an out-of-band Physical Platform object on the IBM Director console.
4. The IBM Director console, group contents will show the BMC as shown in Figure 2-6.



Figure 2-6 IBM Director console group contents pane with BMC added

5. IBM Director attempts to access the BMC using the default USERID/PASSW0RD combination.
If you have deleted or changed the default USERID/PASSW0RD combination, then a small padlock icon will appear next to the device. Right-click the device and click **Request Access**, and enter a valid user ID and password.
6. You are now able to use the MPA Task to configure settings such as user id,passwords Alert forwarding profiles.
7. Either right-click the BMC object and select **Management Processor Assistant → Configuration** or expand the Management Processor Assistant Task in the right-hand pane, highlight **Configuration**, and then drag and drop the configuration task onto the BMC object.
8. When the Management Processor Assistant window opens, select the appropriate setting you want to modify. To change the user ID and password select **Login profiles** from the left-hand menu.
9. To add a new user, click any of the login profiles. This will highlight an entry. Select **Add an Entry**, which will add a new login profile. You can also modify any existing user by double-clicking the fields. See Figure 2-7 on page 16.

Server	Entry number	User ID	Password	Confirm password	Authority
E325_bmc	1		*****	*****	Read only ▾
E325_bmc	2	Operator	*****	*****	Operator ▾
E325_bmc	3	USERID	*****	*****	Supervisor ▾
E325_bmc	4	OEM	*****	*****	Custom ▾

Figure 2-7 Login profile settings

10. Double-click the User ID field and enter the user name.
11. Next double-click the Password field and enter and appropriate password.
12. Double-click the Confirm Password field and enter the password again
13. Specify the level of authorization you require. The choices are:
 - *Supervisor* indicates the following privileges:
 - User account management
 - Remote console access
 - Remote console and virtual media access
 - Remote server and power/restart access
 - Ability to clear event logs
 - Adapter configuration basic
 - Adapter configuration - Networking and security
 - Adapter configuration advanced
 - *Read only* indicates all data is view-only. No updates are permitted.
 - *Operator* indicates the following privileges:
 - Remote server and power/restart access
 - Ability to clear event logs
 - *Custom* indicates that you can specify what you want.

14. Once you have configured your settings, click **Apply** to confirm changes.
15. To modify the Alert-forwarding profiles select **Alert-forwarding profile** from the left-hand menu. The following pane in Figure 2-8 will appear on the right.

Server	Entry number	Status	Description	Connection type	IP address or host name
E325_bmc	4	Enabled	Not supported	IBM Director Comprehensive	192.168.70.107

Figure 2-8 Alert-forwarding profile

16. There are four profiles available to be set.

17. To add a new profile click one of the profiles already there and then click **Add an entry**. Fill in the appropriate details and then click **Apply** to confirm changes.

Note: Not all the settings displayed can be modified. Some of these settings are not applicable to the BMC. These fields will have not supported in them.

2.2.4 Installing the OSA IPMI device drivers

The device drivers are required for operating system support, and also to enable inband communication with IBM Director.

To download the available device drivers, refer to the IBM technote *IBM @server xSeries BMC — Firmware and Drivers Cheatsheet*, TIPS0532, and click the link for the drivers for the appropriate server.

<http://www.redbooks.ibm.com/abstracts/tips0532.html>

Alternatively, you can navigate to the appropriate download page from:

<http://www.pc.ibm.com/support>

Note: At the time of writing, drivers were only available for Windows (not Linux or NetWare), and only for the BMC on the eServer 325 (not the eServer 326).

For a breakdown of the device drivers required refer to Table 2-3.

Table 2-3 IPMI required device drivers

Device driver	Additional comments
IPMI device drivers	<ul style="list-style-type: none">▶ Required to support the IPMI library files▶ Required for inband communication with IBM Director
IPMI library (sp6lib)—OSA BMC mapping layer (library) files	<ul style="list-style-type: none">▶ BMC Mapping Layer (maps the dot commands to the IPMI commands)▶ Required for inband communication with IBM Director
ASR Server Restart software	<ul style="list-style-type: none">▶ Required for ASR Functionality

The device drivers must be installed in a specific order or they will fail installation. The order is as follows:

1. IPMI device driver
2. IPMI Mapping Layer files (library)

3. IPMI ASR Service

For each of these drivers, download the EXE from the above Web site, run the EXE, and follow the instructions. Reboot if you are prompted to do so. An unattended install procedure is also available. See the README.TXT file for instructions.

2.2.5 Event log

The BMC System Event Log (SEL) is accessible from BIOS and from tools such as IBM Director.

Note: The system event log has room for 128 entries. You will receive alerts if the log reaches 75 percent and 90 percent full. However, once the log is full, new entries are not saved. You will need to clear the log in this instance.

2.3 BMC in the xSeries Servers

The Baseboard Management Controller (BMC) in the xSeries servers provides the environmental monitoring for the server. If environmental conditions exceed thresholds or if system components fail, the baseboard management controller will light LEDs to help you diagnose the problem, and will also record the error in the BMC System Event/Error log.

The BMC is based on an Hitachi 2166 chip and implements Version 1.5 of the IPMI specification. The spec document is available from:

ftp://download.intel.com/design/servers/ipmi/IPMIv1_5rev1_1-012904markup.pdf

Topics covered here are:

- ▶ 2.3.1, “Functionality” on page 18
- ▶ 2.3.2, “External connections” on page 19
- ▶ 2.3.3, “Updating the BMC firmware” on page 22
- ▶ 2.3.4, “Configuring the BMC using BMC_CFG” on page 22
- ▶ 2.3.5, “Configuring the BMC in BIOS” on page 34
- ▶ 2.3.7, “Configuring the BMC with IBM Director” on page 37
- ▶ 2.3.9, “Installing the BMC device drivers” on page 40

2.3.1 Functionality

This integrated BMC has the following functionality:

- ▶ Monitoring of system voltages
- ▶ Battery voltage monitor

- ▶ System temperature monitors
- ▶ Fan speed control
- ▶ Fan tachometer monitor
- ▶ Power Good signal monitor
- ▶ System ID and planar version detection
- ▶ System power control
- ▶ System reset control
- ▶ NMI detection
- ▶ SMI detection and generation
- ▶ Serial Port text redirection
- ▶ Remind button detection
- ▶ System LEDs control (power, HDD activity, alert, etc.)
- ▶ Control of Lightpath LED

Refer to Table 2-1 on page 8 for a complete feature and functionality breakdown.

2.3.2 External connections

The BMCs communicate via one of the integrated Ethernet adapters on the server. To communicate with the BMC you would attach a standard Ethernet cable. Refer to Table 2-4 for details on which Ethernet port is shared with the BMC to ensure successful communication.

Note: You can use the PING command to confirm that this connection is valid.

Table 2-4 Shared Ethernet ports with the BMC

Server	System Ethernet port shared with the BMC
xSeries 236	Ethernet port 1
xSeries 336	Ethernet port 1
xSeries 346	Ethernet port 1
xSeries 366	Ethernet port 1
HS20 (8843)	None. BMC functions are provided through the management module.
HS40 (8839)	None. BMC functions are provided through the management module.

The following show the locations of the connectors on the above xSeries server:

- ▶ x346: Figure 2-9 on page 20
- ▶ x336: Figure 2-10 on page 20
- ▶ x236: Figure 2-11 on page 21
- ▶ x366: Figure 2-12 on page 21

Tip: If you install an RSA II SlimLine in the server, the system Ethernet port is still the one you use to access the BMC. However, you may wish to disable connectivity into the BMC for security purposes, by setting the IP address to something not valid (for example, 0.0.0.0).

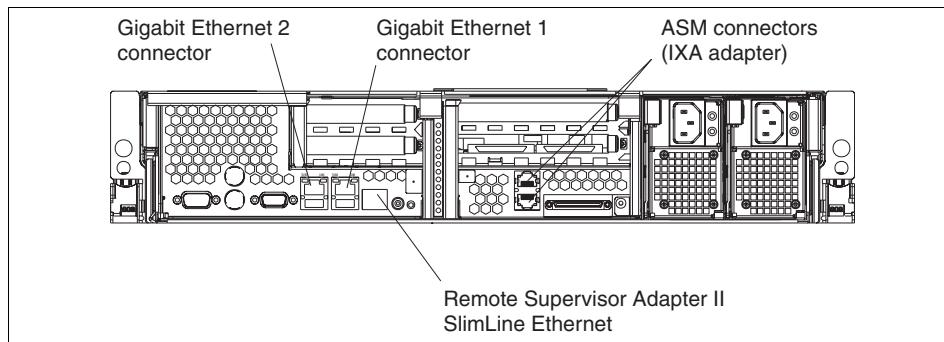


Figure 2-9 Rear ports of the xSeries 346

The Remote Supervisor Adapter II SlimLine Ethernet connector on servers such as the x346 and x366 is to connect the server to a network for systems-management information control. This connector is active only if you have installed a Remote Supervisor Adapter II SlimLine.

The ASM connectors of the x236, x346, and x366 are to connect the server to an Integrated xSeries Adapter (IXA) if one is installed in the server. They are *not* used to form an ASM interconnect network—the interconnect network is not supported.

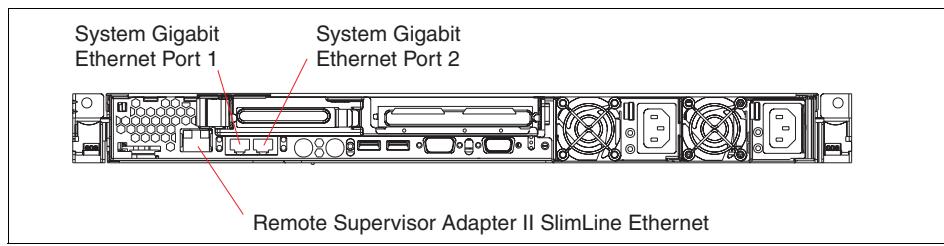


Figure 2-10 Rear ports of the xSeries 336

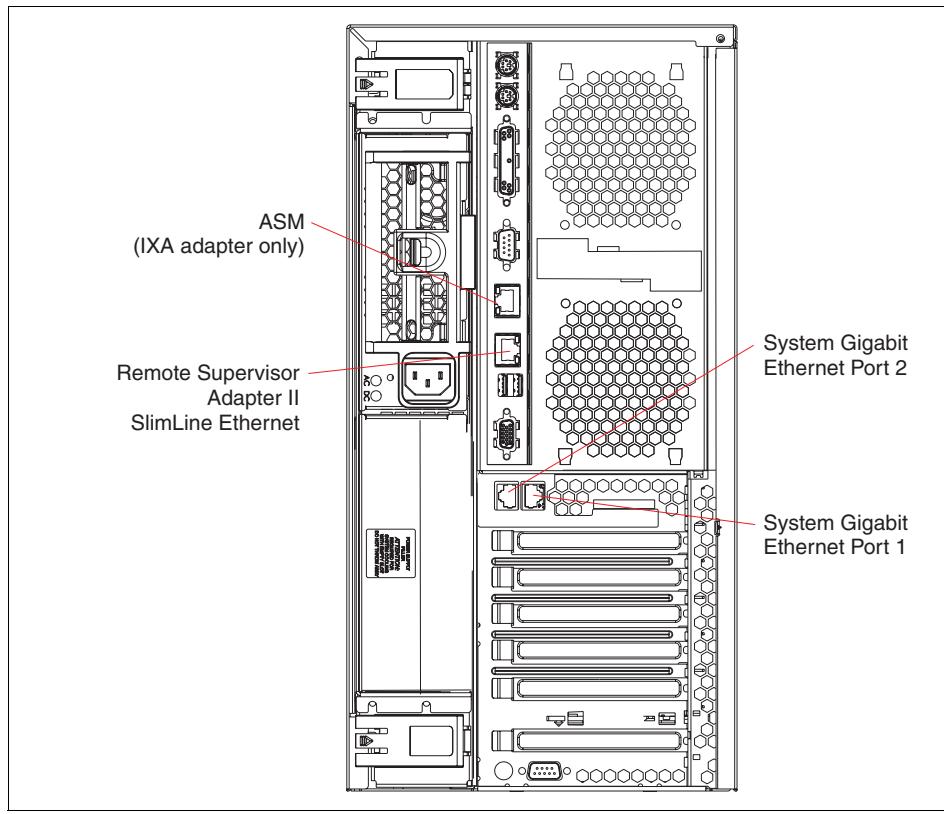


Figure 2-11 Rear ports of the xSeries 236

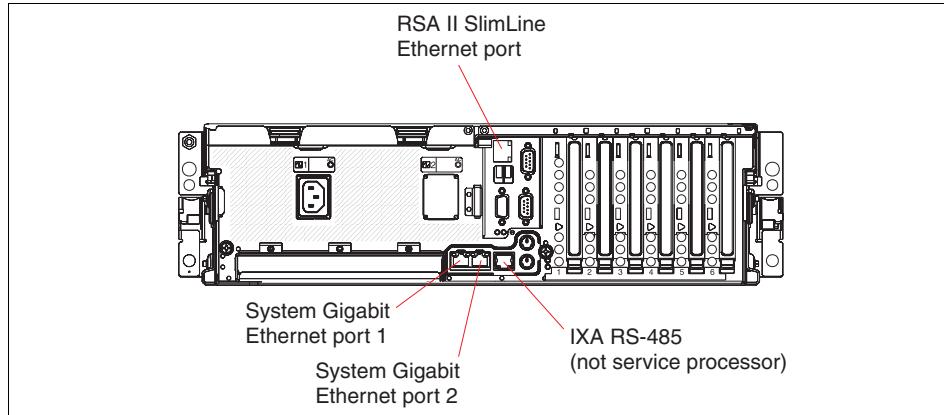


Figure 2-12 Rear ports of the x366

2.3.3 Updating the BMC firmware

This section describes the process to upgrade the BMC on the xSeries servers. It is a best practice to ensure that the BMC firmware is at the latest level to avoid any issues.

Note: Updating the firmware of the BMC does not change any user settings.

The steps are as follows:

1. Download the firmware appropriate for your server. Refer to the IBM technote *IBM @server xSeries BMC — Firmware and Drivers Cheatsheet*, TIPS0532, and click the link for the firmware for the appropriate server.
<http://www.redbooks.ibm.com/abstracts/tips0532.html>
Alternatively, you can navigate to the appropriate download page from:
<http://www.pc.ibm.com/support>
2. The BMC firmware update is usually available in bootable diskette form (an EXE file); however, it can be available as a ISO image file for CD creation. For servers such as the x336, you will need the ISO file since the server does not have a diskette drive standard. Create the diskette or CD.
3. Insert the media into the server and boot the server. You may need to use POST/BIOS setup to configure the correct boot devices.
4. Once your system starts, a Ramdrive will be created, the appropriate files will be copied to this Ramdrive, and the BMC firmware update will execute automatically.
5. When you are finished updating the BMC firmware, you can continue using the firmware update diskette or CD-ROM to configure the server. Refer to 2.3.4, “Configuring the BMC using BMC_CFG” on page 22, for details.
6. If you have already configured the BMC, remove the media and restart your system.

2.3.4 Configuring the BMC using BMC_CFG

There are two methods available to configure the initial BMC network settings (IP address, subnet mask, gateway):

- ▶ Via System Setup in BIOS (pressing F1 at boot time) and accessing BMC settings via the Advanced Options menu. This is discussed in 2.3.5, “Configuring the BMC in BIOS” on page 34.

Using Setup in BIOS is the recommended method. Once the network settings are configured, you can use the Management Processor Assistant (MPA) in

- IBM Director to configure the other required settings such as user IDs, passwords, and alert destinations.
- ▶ Using the `bmc_cfg.exe` configuration utility from the firmware update diskette. This is discussed in this section.

`Bmc_cfg` is considered primarily a debug tool, and can also be used to view or change the BMC configuration settings. Using the `bmc_cfg.exe` configuration utility, we are able to perform all the required configuration settings. This utility is located on the BMC firmware update diskette or CD as described in 2.3.3, “Updating the BMC firmware” on page 22. It is not available as a standalone tool.

Note: You can only run `bmc_cfg` by exiting to DOS after booting the server from the bootable BMC management firmware update diskette/CD. Do not run the utility from a command prompt in Windows.

If you plan to enable the BMC to communicate out-of-band, you will need to configure the following settings:

- ▶ IP Address: See “Setting the IP address” on page 24.
- ▶ Subnet mask: See “Setting the subnet mask” on page 25.
- ▶ Default gateway: See “Setting the default gateway” on page 26.
- ▶ Alert notification and alert destination settings: See “Setting the destination where BMC alerts are to be sent” on page 26.

We also suggest the you change the user ID and password from the default of `USERID` and `PASSW0RD`. To modify the security settings you will have to change the following:

- ▶ User ID and password: See “Adding or modifying users” on page 27.
- ▶ User privilege: See “Setting the access a user can have” on page 30.

Complete the following steps to start `bmc_cfg`:

1. If you have just updated the firmware of the BMC, exit the update utility to return to the DOS prompt. If not, boot from the firmware update diskette/CD, and when prompted whether you want to update the firmware, select **No**.
2. At the DOS prompt, enter `bmc_cfg`. This will display the main menu screen, Figure 2-13 on page 24.

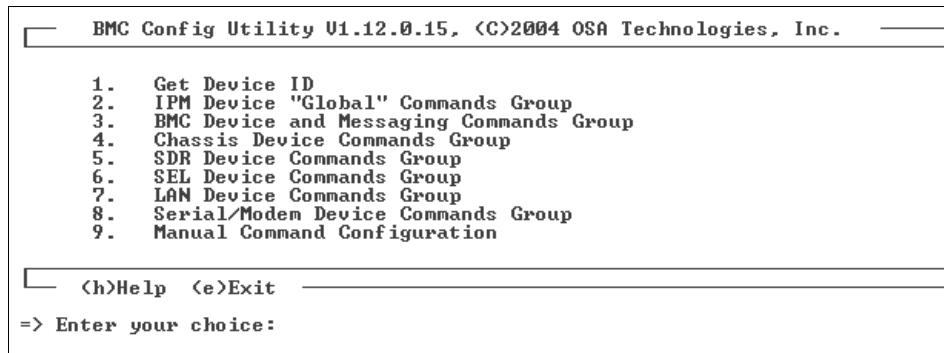


Figure 2-13 BMC_cfg main menu

Setting the IP address

Follow these steps to set the IP address for the service processor to a static address.

1. Enter 7 from the main menu to select Set LAN Device Commands Group. Figure 2-14 appears.

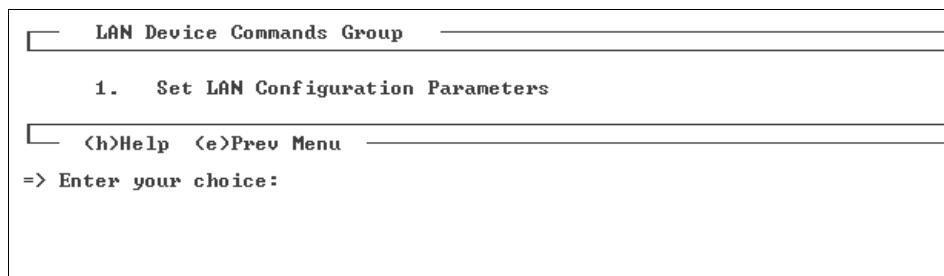


Figure 2-14 LAN Device Commands Group

2. Enter 1 to select Set LAN Configuration Parameters. Figure 2-15 on page 25 appears.

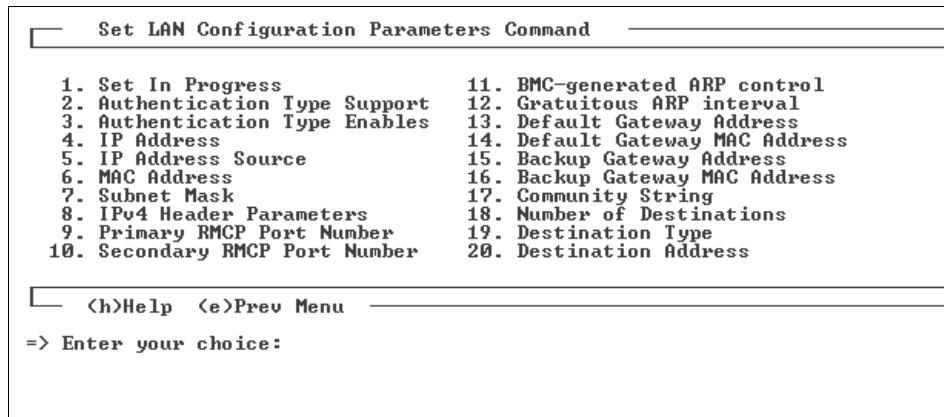


Figure 2-15 LAN configuration parameters command menu

3. Enter 4 to select IP address.
4. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
5. Enter 1 to update the IP address.
6. Type in the IP address for the BMC and press Enter.
7. Enter C to commit the changes.
8. Enter E to return to Figure 2-15.

Note: Even though option 5, IP Address Source, lets you enable DHCP, our testing has shown that this does not work. As a result, you must use a static IP address as described above.

Setting the subnet mask

Follow these steps to set the subnet mask for the service processor.

1. From Figure 2-15, enter 7 to select subnet mask.
2. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
3. Enter 1 to update the subnet mask value.
4. Type in the subnet mask for the BMC and press Enter.
5. Enter C to commit the changes.
6. Enter E to return to Figure 2-15.

Setting the default gateway

Follow these steps to set the gateway for the service processor:

1. From Figure 2-15 on page 25, enter 13 to select default gateway address.
2. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
3. Enter 1 to update the gateway value.
4. Type the address of the default gateway and press Enter.
5. Enter C to commit changes.
6. Enter E to return to Figure 2-15 on page 25.

Setting the destination where BMC alerts are to be sent

The BMC supports up to four destinations where alerts will be sent. The device that you specify to receive the alerts must be able to receive PET traps (platform event traps). A system running IBM Director Server can receive PET traps.

Follow these steps to specify where the BMC is to send alerts:

1. From Figure 2-15 on page 25, enter 20 to select default destination.
2. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
3. Enter the number of the destination you wish to modify: 1, 2, 3, or 4.
4. Type in the IP address where you want BMC alerts to be sent to and press Enter. For example, this may be your IBM Director management server.
5. Enter C to commit changes.
6. Enter E to return to Figure 2-15 on page 25.

Setting the destination type

The destination type is where you specify what type of system is to receive the alerts from the BMC. Only PET 1.0 (platform event trap, an IPMI standard) is currently supported. You will need to set the destination type for each destination you configure (up to 4).

PET is a specific format of SNMP and includes an acknowledgement to ensure the trap handler actually receives the alert. IPMI V1.5 also specifies when to retry sending the alert and how often if there is no response. IBM Director Server can receive PET 1.0 types of alerts.

Follow these steps to set the destination type for the service processor:

1. Enter 19 to select the destination type.
 2. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
 3. Enter the number of the destination you wish to modify: 1, 2, 3, or 4.
 4. Select the option you wish to modify:
 - 1 = Destination type
 - 2 = Alert acknowledgement timeout/retry interval (in seconds)
 - 3 = Number of retries
- Enter 1 to modify the settings of the destination type.
5. Enter 00 to select PET trap destination. This is the only supported choice.
 6. Enter E to go back to the previous menu.
 7. Enter C to commit changes.
 8. Enter E to return to Figure 2-15 on page 25.

Setting the SNMP community name

To set the SNMP community name:

1. Enter 17 to select community name.
2. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
3. Enter 1 to change the community name.
4. Type in the community name you require and press Enter.
5. Enter C to commit changes.
6. Enter E to return to Figure 2-15 on page 25.

Adding or modifying users

Remote access to the BMC is controlled by user ID and password. There are four user IDs, but only IDs 2, 3, and 4 can be changed. User ID 1 is a *null user*, and by IPMI specification cannot be changed.

Note: By default, user ID 2 is USERID, and the password is PASSW0RD (with the number 0, not the letter O).

To add or modify a user (IDs 2, 3, or 4 only), do the following:

1. Go back to the BMC_CFG main menu. Use the E, previous menu, selection to return to the main menu if necessary.
2. Enter 3 to select BMC Device and Messaging Commands Group.

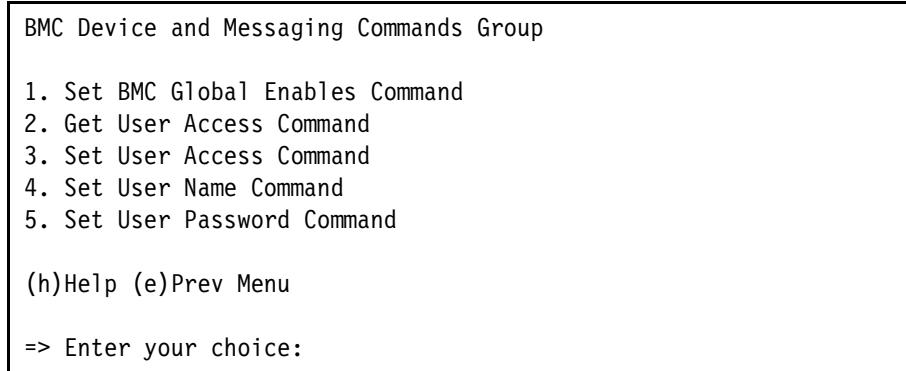


Figure 2-16 Device and Messaging Commands Group

3. Enter 4 to select Set User Name Command.
4. Select the user number you want to change: 2, 3, or 4 (you cannot change user 1).
5. Enter 1 to enter the user name. It can be up to 16 characters.
6. Enter C to commit changes to the BMC.
7. Enter E to return to the previous menu.

To set the password for a BMC user, you need to select the user you want to change, enter the password twice, then enable the user. The steps are as follows:

1. From the BMC Device and Messaging Commands Group menu, Figure 2-16, enter 5 to select Set User Password Command. See Figure 2-17 on page 29.

Set User Password command

Set_ Description_____

1. 00h User ID
2. 00h Operation
3. Password data:

(c)Commit (h)Help (s)Save Config (e)Prev Menu

=> Enter your choice:

Figure 2-17 Set User Password command window

2. Enter 1 to select the user ID field.
3. Enter the user you want to change: 2, 3, or 4. Figure 2-17 updates to reflect the selected user.
4. Enter 2 to select the operation you wish to perform.

Byte 2, Set User Password command

Current Byte Value= 00h

Mod/Set_ Description_____

00h operation

- | | | |
|------------------|--|-------------------|
| 00. disable user | | 01. enable user |
| 02. set password | | 03. test password |

(v)Modify (+)Enable (-)Disable

(h)Help (d)Discard (e)Prev Menu

=> Enter your choice:

Figure 2-18 Selecting an operation to perform on the user password

The options, as shown in Figure 2-18, are:

- 00 = disable user
- 01 = enable user
- 02 = set password
- 03 = test password

5. Enter 02 to select the operation to set the password.
6. Enter E to return to the previous menu.

7. Enter 3 to enter a new password.
8. Type in your password (it can be up to 16 characters) and press Enter.
9. Enter C to commit the changes to the BMC.
10. Enter 2 to select a different operation. Figure 2-18 on page 29 appears again.
11. Type 01 to select the operation to enable the user.
12. Enter E to return to the previous menu.
13. Enter C to commit changes to the BMC.
14. Enter E to return to the previous menu.

Setting the access a user can have

The BMC lets you specify what type of access a user can have, from no access to full access.

1. In the BMC Device and Messaging Command Group menu, Figure 2-16 on page 28, enter 3 to select Set User Access Command. Figure 2-19 appears.

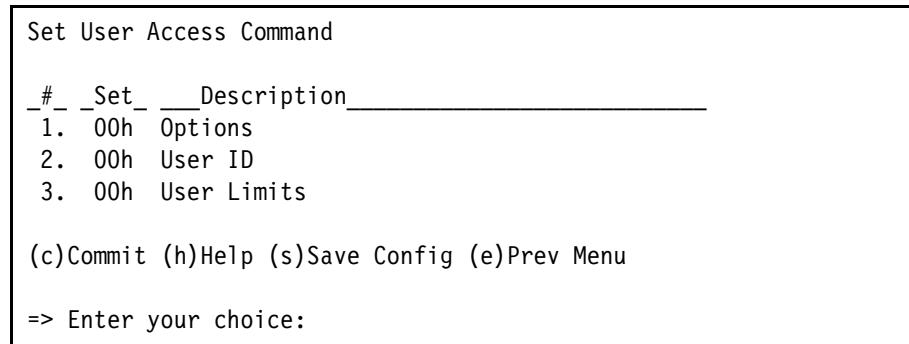


Figure 2-19 Set User Access Command menu

2. The first step is to select a channel via the Options menu. Enter 1 to change the options.

```

Byte 1, Options

Current Byte Value= 00h

#_ _Mod/Set_ _Description_____
7.      -   Enable changing the following bits in the byte
6.      -   User Restricted to Callback
5.      -   User Link authentication enable
4.      -   User IPMI Messaging enable
3.    00h   Channel Number

(v)Modify (+)Enable (-)Disable

(h)Help (d)Discard (e)Prev Menu

=> Enter your choice:

```

Figure 2-20 Set User Access Command menu

3. Enter 3 to change the channel number.
 4. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial
- Figure 2-20 now changes to reflect the selected channel number.
5. Enter E to return to the previous menu.
 6. Enter 2 to select the user.
 7. Enter the user you want to change: 2, 3, or 4. Figure 2-17 on page 29 updates to reflect the selected user.

```

Set User Access Command

#_ _Set_ _Description_____
1. 01h Options
2. 02h User ID
3. 00h User Limits

(c)Commit (h)Help (s)Save Config (e)Prev Menu

=> Enter your choice:

```

Figure 2-21 Set User Access Command menu

8. Enter 3 to change the access privilege of this user.

Byte 3, User Limits																							
Current Byte Value= 00h																							
<table><tr><td><u>#</u></td><td><u>Mod/Set</u></td><td><u>Description</u></td><td>_____</td></tr><tr><td colspan="4">00h User Privilege</td></tr><tr><td colspan="2">01. Callback</td><td colspan="2">02. User</td></tr><tr><td colspan="2">03. Operator</td><td colspan="2">04. Administrator</td></tr><tr><td colspan="2">05. OEM Proprietary</td><td colspan="2">0f. NO ACCESS</td></tr></table>				<u>#</u>	<u>Mod/Set</u>	<u>Description</u>	_____	00h User Privilege				01. Callback		02. User		03. Operator		04. Administrator		05. OEM Proprietary		0f. NO ACCESS	
<u>#</u>	<u>Mod/Set</u>	<u>Description</u>	_____																				
00h User Privilege																							
01. Callback		02. User																					
03. Operator		04. Administrator																					
05. OEM Proprietary		0f. NO ACCESS																					
(v)Modify (+)Enable (-)Disable																							
(h)Help (d)Discard (e)Prev Menu																							
=> Enter your choice:																							

Figure 2-22 Specifying the user access

Options available are. See Table 2-5.

Table 2-5 BMC user authority levels

User access	Description
01 - Callback	This is the lowest privilege level. Only commands necessary to support initiating a callback are allowed.
02 - User	Only commands that can read data and display status are allowed. Commands that alter the configuration or change status are not allowed.
03 - Operator	All commands such as power control and clearing the event log are allowed. Commands that are not allowed are those that modify the Ethernet and serial interfaces and the ability to change user access privileges.
04 - Administrator	All BMC commands are allowed.
05 - OEM proprietary	Reserved.
0f - No access	The user cannot perform any actions.

9. Enter one of these to specify the privilege level you require.
10. Enter E to return to the previous menu.
11. Enter C to commit the changes to the BMC.

Verifying what access a user has

To verify what access a user has, do the following.

1. From the BMC Device and Messaging Commands Group menu, Figure 2-16 on page 28, enter 2 to select Get User Access Command.
2. Enter 1 for the channel number. The channel numbers are as follows:
 - 1 = LAN
 - 2 = Serial

Figure 2-2 on page 12 appears.

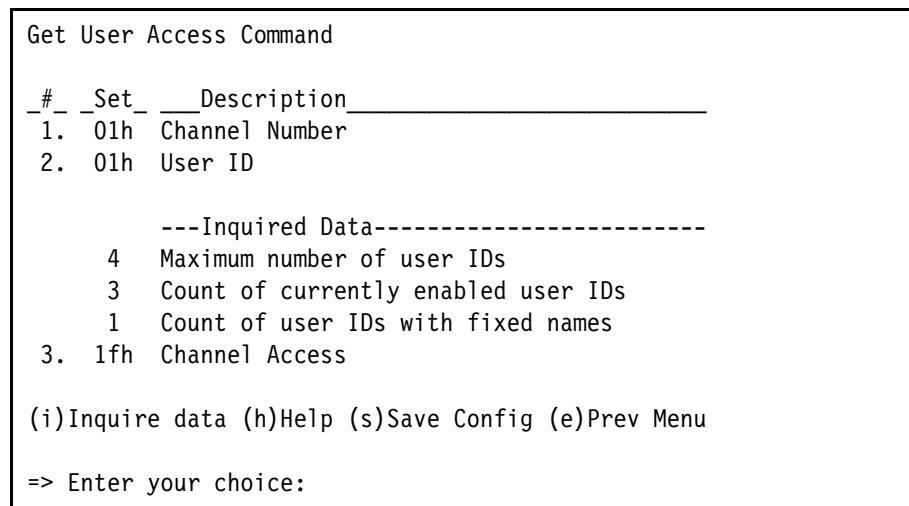


Figure 2-23 Requesting an existing user's access

3. Enter 2 to select a user. Enter 1, 2, 3, or 4.
4. Enter I to send the inquiry request to the BMC.
5. Enter 3 to display the access in textual format. A screen similar to Figure 2-24 on page 34 appears.

In this example, the user privilege is 04h, which corresponds to Administrator.

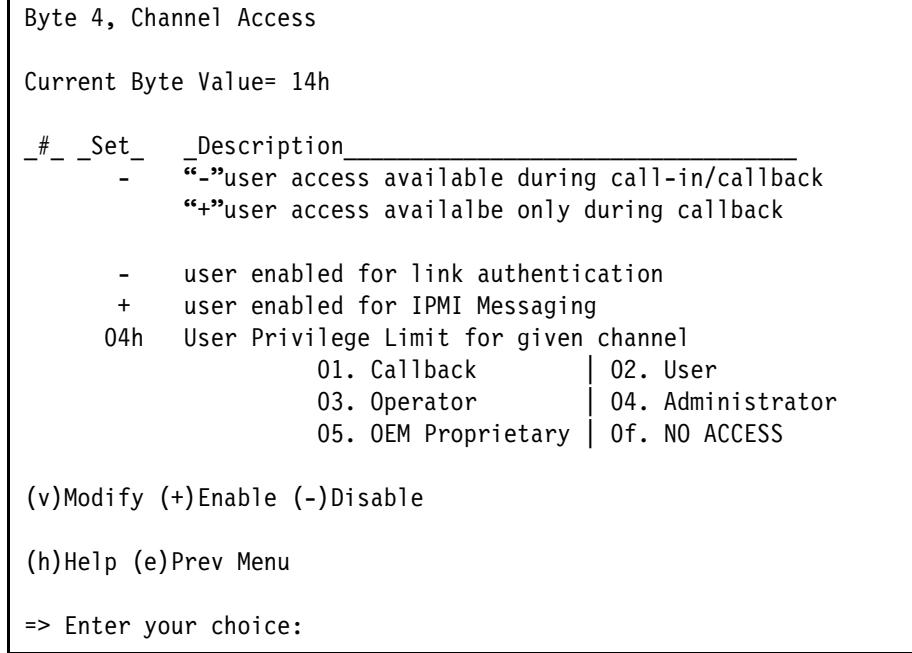


Figure 2-24 Displaying the user access

6. Enter E to exit this menu.

2.3.5 Configuring the BMC in BIOS

Within the system BIOS you are able to configure the following settings:

- ▶ IP address
- ▶ Subnet mask
- ▶ Default gateway

If you want to modify the default user ID and password, you are required to either use bmc_cfg (see 2.3.4, “Configuring the BMC using BMC_CFG” on page 22) or IBM Director (see 2.3.7, “Configuring the BMC with IBM Director” on page 37).

To configure the BMC using the Bios follow these steps:

1. Reboot the server if currently running. During post press F1 to enter the Configuration and Setup utility.
2. Select **Advanced Setup**.
3. Select **Baseboard Management Controller (BMC) Settings**. The menu is as shown in Figure 2-25 on page 35.



Figure 2-25 BMC Settings panel in BIOS

4. Select **BMC Network Configuration**.

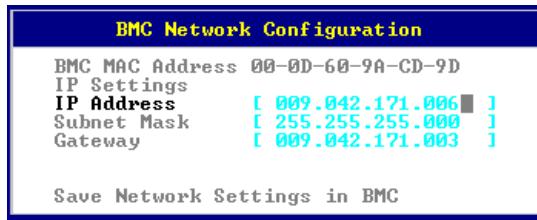


Figure 2-26 BMC network settings in BIOS

5. Enter the appropriate IP address, subnet mask, and gateway addresses, then select **Save Network Settings in BMC**.

Further parameters will need to be adjusted if you plan to use console redirection and Serial over LAN. This can be used with a tool such as OSA SMBridge. See 6.4, “OSA SMBridge utility” on page 192.

2.3.6 Event Log

You can access the BMC System Event Log (SEL) via the menu shown in Figure 2-25 or using tools such as OSA SMBridge. This event log records all the hardware alerts for the server. The event log displays one event per screen. Use the Get Next Entry and Get Previous Entry links to page through the events.

You may notice that some events have a date stamp of 2070. When power is removed from the server and later restored, the BMC clock resets to 1970 (which the BIOS displays as 2070). As soon POST completes and the operating system is passed control, the BMC clock is updated with the correct time from BIOS.

Note: The incorrect time does not affect the timestamps of the events as received by IBM Director. The events as seen in the IBM Director Event Log have the correct time—the time the events were received—as long as the IBM Director Management Server has the correct time.

```
*****
*                                BMC System Event Log
*****
*  Get Next Entry          **
*  Get Previous Entry       **
*  Clear BMC SEL           *
*
*  Entry Number*   00001 / 00031      *
*  Record ID*    0001                *
*  Record Type*   02                 *
*  Timestamp*    2070/01/01 00:00:14  *
*  Entry Details: Generator ID* 0020  *
*                      Sensor Type* 08    *
*                      Assertion Event   *
*                      Power Supply      *
*                      Sensor Specific Type  *
*                      Presence detected   *
*                      Sensor Number* 70      ?*
*****
<F1> Help            <><?> MMove
<Esc> Exit           <Enter> Select
```

Figure 2-27 BMC System Event Log

Note: The system event log has room for 512 entries. You will be alerted if the log reaches 75 percent or 90 percent full. However, unlike the RSA II or BladeCenter management module, once the log is full, new entries are not saved. You will need to clear the log in this instance using tools such as SMBridge.

When an RSA II SlimLine is installed in the server, all events in the BMC System Event Log are also made available to the RSA II. The RSA II also maintains a separate log, and when viewed by accessing the RSA II, you will see both RSA II and BMC-based events. However, the reverse is not true. You cannot view the RSA II event log by viewing the event log in BIOS. The BIOS event log only shows BMC-based events.

2.3.7 Configuring the BMC with IBM Director

If you have the IBM Director Server installed in your environment and the BMC network settings are configured correctly, you can use this method to configure settings on the BMC. This is the IBM preferred method of configuring the BMC, and also enables out-of-band management of the BMC.

In this section we describe how to configure the user ID, passwords, and alert-forwarding settings.

Adding the BMC to IBM Director Console

To add the BMC to Director as a managed object, do the following:

1. From the Director console right-click the middle pane in a blank area.
2. Click **New → Physical Platform**.

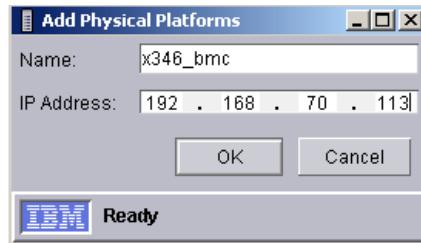


Figure 2-28 Add physical platforms window

3. Enter the appropriate details for the BMC you want to add and select **OK**.
4. Once the BMC is discovered it will appear as an out-of-band (OOB) Physical Platform object on the Director console, and will appear as shown in Figure 2-29.



Figure 2-29 IBM Director console group contents pane with BMC added

5. IBM Director attempts to access the BMC using the default USERID/PASSW0RD combination.
If you have deleted or changed the default USERID/PASSW0RD combination, then a small padlock icon will appear next to the device. Right-click the device and click **Request Access**, and enter a valid user ID and password.

Adding users

You are now able to use the MPA task to configure the user ID and password, as follows.

Note: The maximum number of login profiles is four.

1. Either right-click the BMC object and select **Management Processor Assistant** → **Configuration**, or Expand the Management Processor Assistant Task in the right-hand pane, and drag the Configuration subtask and drop it on the BMC object.
2. Once MPA starts, click **Login profiles** from the left-hand menu (Figure 2-30).

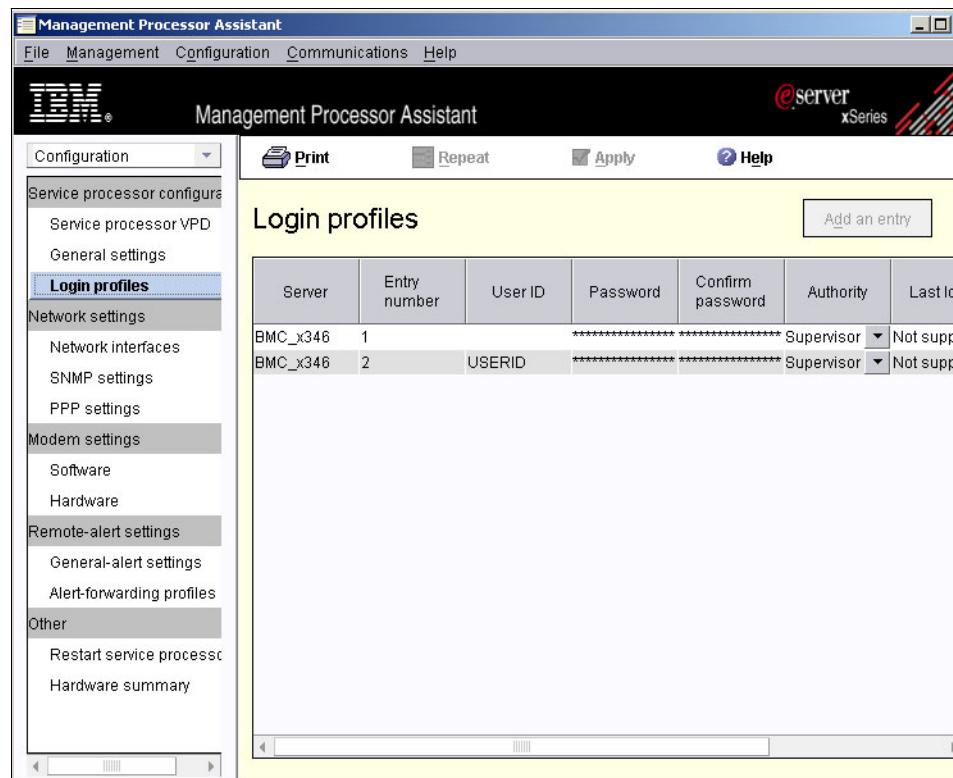


Figure 2-30 Management Processor Assistant Configuration window

3. To add a new user, highlight the first login profile and click **Add an Entry**. This adds a new row to the display table, as shown in Figure 2-31 on page 39.

Server	Entry number	User ID	Password	Confirm password	Authority	Last login	Dial-back	
							Dial-back number	Dial-back enabled
BMC_x346	1		*****	*****	Supervisor	Not supported	Not supported	Not supported
BMC_x346	2	USERID	*****	*****	Supervisor	Not supported	Not supported	Not supported
BMC_x346	3	USER1	*****	*****	Supervisor	Not supported	Not supported	Not supported

Figure 2-31 Add a new security entry to the BMC

4. Double-click the **User ID** cell and enter the details for your user.
5. Double-click the **Password** cell and enter the appropriate password.
6. Double-click the **Confirm Password** cell and enter the password again to confirm.
7. Next specify the level of authorization you require. The levels are as follows:

Supervisor has the following privileges:

- User account management
- Remote console access
- Remote console and virtual media access * If applicable
- Remote server and power /restart access
- Ability to clear event logs
- Adapter configuration basic
- Adapter configuration - Networking and security
- Adapter configuration advanced

Read only has viewing privileges only. No changes can be made.

Operator has the following privileges:

- Remote server and power/restart access
- Ability to clear event logs

No Access disables access to the BMC for this user.

8. Once you have entered all of the correct details, click **Apply** to save the changes.

Configuring alert forwarding

You can also modify the Alert-forwarding profiles by selecting **Alert-forwarding profile** from the left-hand menu. The alert forwarding settings will appear on the right, similar to Figure 2-32.

Server	Entry number	Status	Description	Connection type	IP address or host name
BMC_x346	4	Enabled	Not supported	IBM Director Comprehensive	192.168.70.107

Figure 2-32 Alert notification settings for BMC

9. To add a new profile, highlight the existing profile and then click **Add an entry**.
10. Enter the IP address of your IBM Director management server to verify that the connection type is IBM Director Comprehensive.
11. Click **Apply** to commit the changes to the BMC.

Note: Not all the settings displayed can be modified. Some of these settings are not applicable to the BMC. These fields will have Not Supported in them.

2.3.8 Remote control

The BMC supports remote control using the OSA SMBridge utility and Serial over LAN. This provides a text-only console interface that lets you control BIOS screens and specific operating system consoles. Both Linux and Windows provide such text-only consoles. See 6.4, “OSA SMBridge utility” on page 192.

2.3.9 Installing the BMC device drivers

The device drivers are required to provide operating support and inband communication with IBM Director. This section describes how to install the IPMI device drivers on Windows and Linux platforms. The required device drivers are listed in Table 2-6.

Table 2-6 IPMI required device drivers

Device driver	Additional comments
IPMI device drivers.	<ul style="list-style-type: none"> ▶ Required for in-band communication with IBM Director
IPMI Library (sp6lib) - This is the OSA BMC IPMI mapping layer.	<ul style="list-style-type: none"> ▶ BMC Mapping Layer (maps the dot.commands to IPMI commands) ▶ Required for in-band communication with IBM Director
ASR Server Restart software.	<ul style="list-style-type: none"> ▶ Required for ASR functionality

The device drivers must be installed in a specific order or they will fail installation. The order is as follows:

1. IPMI device driver
2. IPMI mapping layer (library) files
3. IPMI ASR service

To download the drivers appropriate for your server, refer to the IBM technote *IBM @server xSeries BMC — Firmware and Drivers Cheatsheet*, TIPS0532, and click the link for the firmware for the appropriate server.

<http://www.redbooks.ibm.com/abstracts/tips0532.html>

Alternatively, you can navigate to the appropriate download page from:

<http://www.pc.ibm.com/support>

Installing the device drivers on Windows

This section describes how to install the drivers under Windows.

IPMI device driver

To install the OSA IPMI device driver, follow these steps:

1. Run Setup.exe. After the usual initial windows, you will be prompted to select a driver parameter, as in Figure 2-33.

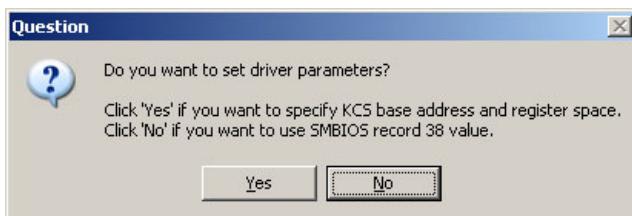


Figure 2-33 Driver parameters

2. Click **No**.

Clicking No means that you want the driver to query SMBIOS record 38 for the necessary device driver parameters. Clicking Yes means that you will manually set these parameters, and this should only be used in unusual situations as directed by IBM support. If you manually set an invalid parameter, you may cause Windows to blue screen or reboot.

3. Click **Next** to begin the installation. When it completes you will be prompted to reboot the server, but the installer will not do this automatically.

IPMI mapping layer (library) files

To install the IPMI mapping layer (library) files, do the following:

1. Ensure that the IPMI device driver is installed before installing this software.
2. Download the EXE from the above Web site and run it.
3. Follow the on-screen instructions.
4. Reboot the server if the installation procedure prompts you to do so.

IPMI ASR service

To install the ASR service, do the following:

1. Ensure that the IPMI device driver and IPMI library files are installed before installing this software.
2. Download the EXE from the above Web site and run it.
3. Follow the on-screen instructions.
4. Reboot the server if the installation procedure prompts you to do so.

Installing the device drivers on Linux

This section describes how to install the drivers under Linux.

IPMI device driver

To install the OSA IPMI device driver, launch a UNIX shell and enter the following command to build and install the driver module on your system:

```
rpm -i osa_ipmi-x.x.x-x.i386.rpm
```

If you upgrade your Linux kernel, you should uninstall and then recompile/re-install the OSA IPMI device driver. To rebuild the driver, change to directory /usr/osa/osa_ipmi-x.x.x-x and enter:

```
sh build_osadrv
```

Notes:

- ▶ You should install the necessary source code packages on your system. We recommend that you install them in /usr/src.
- ▶ Make sure you have gcc 3.2 available. You may also need to upgrade the binutils package.
- ▶ When installing on 32-bit SUSE LINUX 8.2, which has gcc Version 3.3 20030226 (pre-release) installed, **insmod** does not work without the -f option. You should manually add the -f option to the **insmod** command in the /sbin/ipmi_load script for the force loading. You may, however, receive a warning that the kernel is tainted. Other gcc versions may cause the same problem.

To uninstall the OSA IPMI device driver, enter one of the following:

```
rpm -e osa_ipmi-x.x.x-x  
rpm -e osa_ipmi
```

See the README.TXT file available with the driver for more information.

IPMI mapping layer (library) files

The IBM mapping layer software is installed and removed via the Linux® RPM package management tool. Ensure that you have first installed the IPMI driver.

If this is an upgrade to an existing software package, remove the old version first, with the command:

```
rpm -e ibmsp6a
```

Depending upon your system's configuration, you may see messages about missing files. These may be ignored.

To install the IPMI mapping layer (library) files, issue the following commands.

EM64T and AMD64 note: On x86_64 kernels this RPM will build a 64-bit shared object, and a 32-bit compatibility shared object. Before installing the RPM on an x86_64 kernel, make sure the 32-bit compatibility development packages are installed.

```
rpmbuild --rebuild ibmsp6a-x.xx-y.src.rpm
```

Followed by:

```
cd /usr/src/package-dir/RPMS/architecture  
rpm -ivh ibmsp6a-x.xx-y.architecture.rpm
```

Where:

- ▶ *package-dir* is the distribution-specific name of the RPM build directory (usually "redhat" or "packages").
- ▶ *architecture* is the architecture of the kernel in use (i386, i586, or x86_64).

For example, to install the rpm on an x86_64 SUSE LINUX, the commands are:

```
rpmbuild --rebuild ibmsp6a-x.xx-y.src.rpm  
cd /usr/src/packages/RPMS/x86_64  
rpm -ivh ibmsp6a-x.xx-y.x86_64.rpm
```

IPMI ASR service

This section describes how to install the ASR (ibmipmiasr) RPM.

Before installing, make sure your server has both the IPMI device driver and the IBM Mapping Layer Software installed.

The system that the source rpm file is to be run on must have Linux development/build capability.

If this is an upgrade to an existing software package, remove the old version first, with the command:

```
rpm -e ibmipmiasr
```

Depending upon your system's configuration, you may see messages about missing files—these may be ignored.

To install the source rpm, execute the following command:

```
rpm -ivh ibmipmiasr-x.xx-y.i386.rpm
```

Once the installation is complete, check the log file /var/log/message. A successful installation will write the following message to the log:

```
IBM IPMI ASR application loaded
```

To uninstall the binary rpm, execute the following command:

```
rpm -e ibmipmiasr
```

RPM will unload the ASR application, and remove all ibmipmiasr-related files from your system.

2.3.10 Ports used by the BMC

The BMC uses several TCP/UDP ports for communication. If the communication with the BMC passes firewalls, it is important to know which ports you have to enable on the firewalls to communicate properly.

Table 2-7 TCP/IP ports used by the BMC

Port number	Description
623	IPMI communications to SMBridge and Director
664	IPMI communications (secondary)
161	SNMP get/set commands
162	SNMP traps and PET alerts to Director

2.4 Integrated system management processors

Refer to the Table 1-1 on page 2 for the details on which servers have integrated ISM processors as standard.

2.4.1 Features

The ISM Processor has the following functionality:

- ▶ Intrusion alert
- ▶ Monitoring of system temperature/CPU temperature
- ▶ Monitoring of fans, memory, power supplies, voltages
- ▶ Auto Server Restart watchdog failure alert
- ▶ RS-485 Interconnecting capability
- ▶ Remote firmware updates
- ▶ Alert forwarding via RS-485 interconnect network
- ▶ Control of light path diagnostics
- ▶ Alert Standard Format (ASF) compatibility

The xSeries 345 is a typical ISM Processor-based server. Figure 2-34 on page 45 shows the locations of the key connectors.

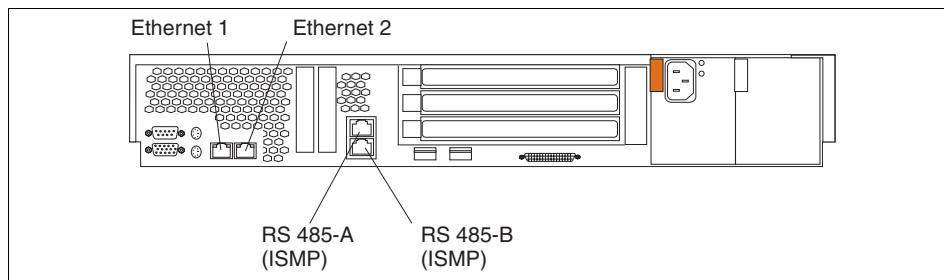


Figure 2-34 Connections on the xSeries 345

The RS-485 connectors are used to connect the server to an ASM interconnect network.

2.4.2 Limitations

The ISM Processor-based servers do not have the ability to forward alerts out-of-band from the service processor unless they are interconnected via the ASM network to an RSA I, RSA II, or RSA II-EXA service processor and that service processor is configured to be the gateway. See 3.3, “Advanced Systems Management network” on page 55.

You can also forward alerts in-band from the ISM Processor by installing IBM Director Agent on the server.

For more information on inband communication with IBM Director please refer to *Implementing Systems Management Solutions using IBM Director*, SG24-6188, or the following documents:

- ▶ *IBM Director Installation and Configuration Guide:*
<http://www.ibm.com/pc/support/site.wss/MIGR-50460.html>
- ▶ *IBM Director Systems Management Guide:*
<http://www.ibm.com/pc/support/site.wss/MIGR-50461.html>

2.4.3 Configuration

There is no configuration required at the BIOS level for the ISM Processors.

If you wish to receive alerts from an ISM Process, you will need to configure an RSA or RSA II in your ASM interconnect network to be the gateway and configure alerts on that RSA or RSA II. See 3.3.1, “Specifying the ASM Gateway” on page 58.



Remote Supervisor Adapter II

The Remote Supervisor Adapter II (RSA II) is the top-of-the-line systems management adapter for xSeries. It provides many options for alerting, monitoring, and remote management of xSeries servers.

In this chapter we explain the different models of the Remote Supervisor Adapter II, their features, and common usage. We do not cover every detail of all available functions, just what you need for implementation of hardware-based systems management of IBM @server xSeries servers. You will find more details in the product publication *Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide*.

The RSA II replaces the older Remote Supervisor Adapter (which we refer to as the RSA I) and Advanced System Management PCI Adapter (ASMA). Despite their different features, they can all be connected in an Advanced System Management network. This chapter contains:

- ▶ 3.1, “Functions and features” on page 48
- ▶ 3.2, “Overview of the Remote Supervisor Adapter family” on page 49
- ▶ 3.3, “Advanced Systems Management network” on page 55
- ▶ 3.4, “Basic configuration of Remote Supervisor Adapter II” on page 59
- ▶ 3.5, “Remote console and remote media” on page 67
- ▶ 3.6, “Ports used by Remote Supervisor Adapter II” on page 85

3.1 Functions and features

The most useful functions and features of the RSA II are:

- ▶ Automatic notification and alerts

The RSA II automatically sends different types of alerts and notifications to another server like IBM Director, SNMP destination, or as e-mail directly to a user by using SMTP.

- ▶ Continuous health monitoring and control

The RSA II monitors all important system parameters like temperature, voltage, etc. continuously. If a fan fails, for example, the RSA II forces the remaining fans to increase speed to compensate for the failing fan.

- ▶ Event log

You can get access to the event logs of the server and the power-on-self-test (POST) log and export them while the server is up and running.

- ▶ LAN and Advanced Systems Management (ASM) interconnect remote access

The RSA II has an LAN interface that you can connect with integrated system management processors (ISMPs) to an ASM interconnect network. The RSA II is the focal point of the ASM network and can forward all alerts of the connected ISMPs, and provides access to them over an Ethernet.

- ▶ Operating system failure screen capture

When the operating system hangs, for example, with a blue screen, you can do a screen capture for support purposes. Additionally, the RSA II stores the last failure screen in memory so you can refer to it later.

- ▶ Remote media

As a part of the remote control feature, the remote media capability lets you use diskette drives, diskette images, optical drives such as DVD or CD-ROM drives, or optical drive images of the system where the Web interface of RSA II is running on the remote PC, and make them appear to be local drives on the server.

Note: At the time of writing, support for optical images (ISO files) was being rolled out to all servers that support RSA II for Windows only. Linux support will come at a later date.

- ▶ Remote power control
The RSA II supports remote power control to power on, power off, or restart the server with or without operating system shutdown over LAN or even WAN connection.
- ▶ Server console redirection
The servers console is available in the RSA II Web interface for remote administration.

3.2 Overview of the Remote Supervisor Adapter family

There are three different RSA II adapters for xSeries servers:

- ▶ Remote Supervisor Adapter II (see page 50)
- ▶ Remote Supervisor Adapter II-EXA (see page 52)
- ▶ Remote Supervisor Adapter II SlimLine (see page 53)

Table 3-1 shows the adapters are supported in each xSeries server. The servers listed here are the supported servers at the time of writing this book. Older servers are not supported. For newer ones check the current list of supported servers. See the technote *Service Processors Supported in IBM Netfinity and IBM @server xSeries Servers*, TIPS0146, available from:

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

For the RSA II, the PCI slot where the adapter must be installed is noted (the RSA II SlimLine does not occupy a slot). The table also lists the system board connection, and if the supplied mini-USB cable must be installed for that server.

Tip: The RSA II-EXA is only used with the x445 server.

Table 3-1 RSA II and supported servers

Server	RSA II	RSA II SlimLine	PCI slot	System board connector	Connect mini-USB cable
xSeries 205	Optional	No	1	CN20	Required
xSeries 206	Optional	No	2	CONN2	Required
xSeries 225 (8649)	Optional	No	1	JMGT1 ^a	No
xSeries 226	Optional	No	2	JMGT1 ^a	No
xSeries 235	Optional	No	1	J27	Required

Server	RSA II	RSA II SlimLine	PCI slot	System board connector	Connect mini-USB cable
xSeries 236	No	Optional	-	-	No
xSeries 255	Optional	No	1	J16	Required
xSeries 305	Optional	No	1	CN12	Required
xSeries 306	Optional	No	2	CN18	Required
xSeries 335	Optional ^b	No	1	J2	Required
xSeries 336	No	Optional	-	-	No
xSeries 345	Optional	No	5	J2	Required
xSeries 346	No	Optional	-	-	No
xSeries 365	Standard	No	-	Standard	No
xSeries 366	No	Optional		I/O board	No
xSeries 445	Standard ^c	No	-	Standard	Required ^d
xSeries 460	No	Optional		I/O board	No
eServer 326	Optional	No	2	JMGT1 ^a	No

- a. Use the 26-pin cable with USB signalling.
- b. The xSeries 335 supports the Remote Supervisor Adapter II; however, the C2T function of the x335 will not work with the RSA II because the adapter's video disables the onboard video. Customers will need to install an RSA II in every x335, if they want to use the remote video functionality of the RSA II. See <http://www.pc.ibm.com/support?page=MIGR-54747> for more information.
- c. The RSA II-EXA is standard on some models of the x445. On other models, the RSA I is standard, and the RSA II-EXA (part 13N0382) can be installed in its place. The RSA II (part 59P2984) is not supported in the x445.
- d. If RSA II-EXA is installed, the breakout cable contains the USB connector.

3.2.1 Remote Supervisor Adapter II

The Remote Supervisor Adapter II (world wide part number 59P2984) is a third-generation system management adapter for IBM xSeries servers. It is based on the IBM PowerPC® 405 32-bit RISC processor operating at 200 MHz. It is a half-length PCI adapter running at 66 MHz/32-bit speed.

It comes as a standard feature within the x365 and is preinstalled in PCI slot 1. For many other servers, it is available as an optional feature.

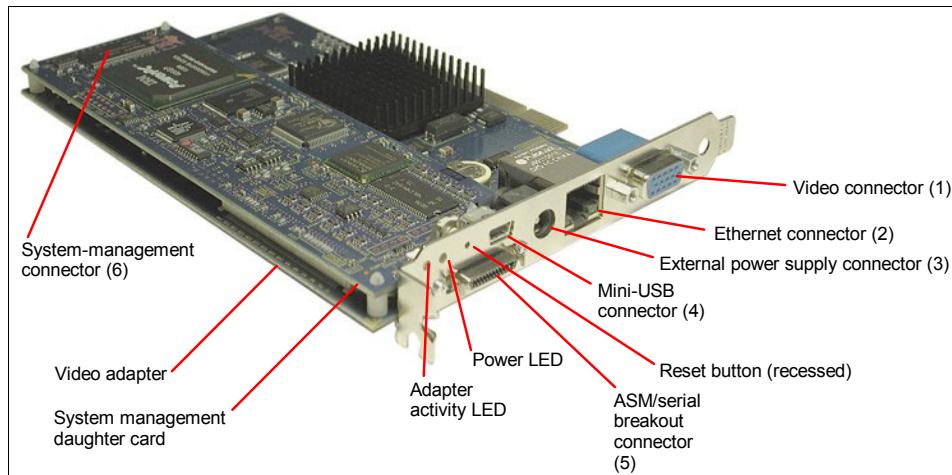


Figure 3-1 External connectors and indicators of the RSA II

The RSA II has the following connectors (the numbers refer to Figure 3-1):

- ▶ Video connector (1 in Figure 3-1). The RSA II contains an additional video subsystem on the adapter. If you install the RSA II in a server, it will automatically disable the onboard video. You should connect the server's monitor to the RSA II video connector.
- ▶ 10/100 Ethernet connector (2). For connection to a 10 Mbps or 100 Mbps Ethernet-based client LAN or management LAN.
- ▶ Power connector (3). You still can access the RSA II if the server is powered down when you use the external power supply (supplied when the adapter is purchased as an option). Connect the power supply to a different power source as the server (for example, a separate UPS).

Tip: The external power supply is not supported for servers with a RSA II installed as standard, such as the x365.

- ▶ Mini-USB connector (4). This port provides the ability for remote keyboard and mouse when using the remote control feature. Connect this to a USB port of the server, except for the following servers where the cable should not be connected (the USB signal is transmitted inside these servers).
 - x225
 - x226
 - x365
 - eServer 326

- ▶ Breakout connector (5). To use the RSA II as focal point for an ASM network or for connecting a modem, a breakout cable is supplied, which has the ASM and serial connections, as shown in Figure 3-2. The breakout cable has one or two serial connectors (earlier RSA II adapters had only one serial port) and two RJ45 connectors for daisy chaining the ASM RS-485 interconnect network.

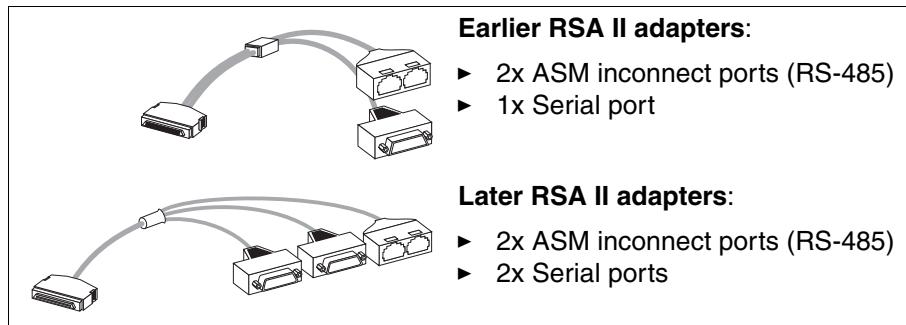


Figure 3-2 Breakout cable of RSA II

- ▶ A 20-pin connector for the connection to the server's motherboard (6). Table 3-1 on page 49 lists the connector on the planar where the supplied cable should be connected.

3.2.2 Remote Supervisor Adapter II-EXA

The RSA II-EXA (part number 13N0382) is an option for the x445 only or is preinstalled in current models. It has identical functions to the RSA II. The adapter can only be installed in the x445 and only by a service technician (because it requires temporary removal of many of the server components).

The RSA II-EXA does not occupy a PCI slot—you find it horizontally underneath the six PCI slots.

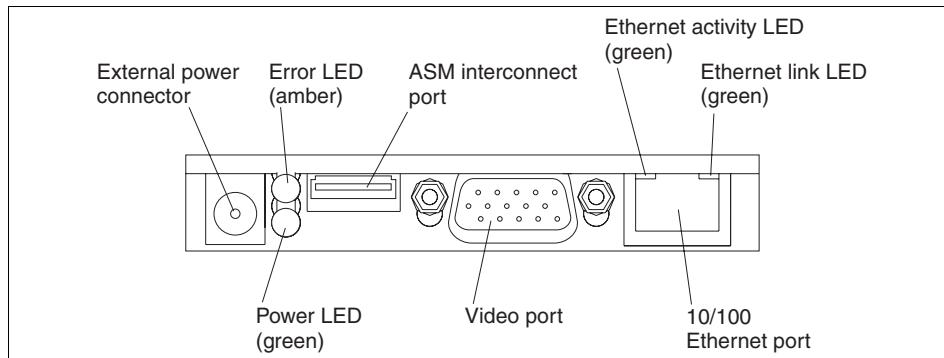


Figure 3-3 Connectors of RSA II-EXA

Tip: If you are not sure which Remote Supervisor Adapter is installed in your x445, check for a video connector on the adapter. If there is one, it is an RSA II-EXA, if not it is an RSA I.

The functionality of RSA II and RSA II-EXA is the same although the connectors are different. The breakout cable of the RSA II-EXA also contains the USB connector (which you connect to the server's USB port) and a second serial port, as shown in Figure 3-4.

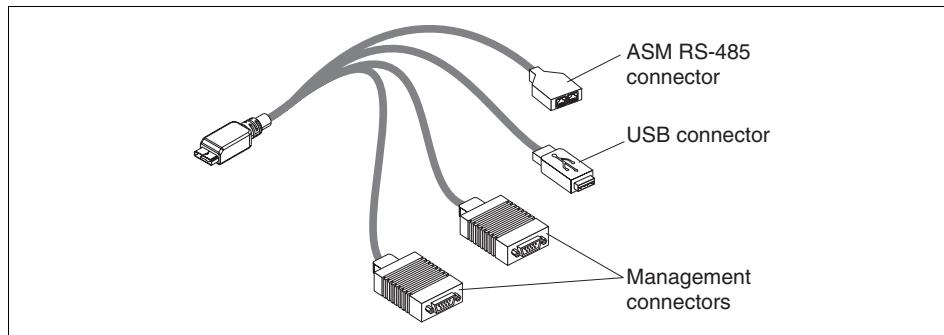


Figure 3-4 RSA II EXA breakout cable

3.2.3 Remote Supervisor Adapter II SlimLine

Some of the current range of xSeries servers and future xSeries Servers have the RSA II SlimLine adapter (part number 73P9341) as an option (see Table 3-1 on page 49). The ServerProven® Web site lists the full line of supported servers:

<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

This new member of the RSA II family does not occupy a PCI slot. It is a small circuit board that looks like the system management daughter card of the Remote Supervisor Adapter II PCI adapter.

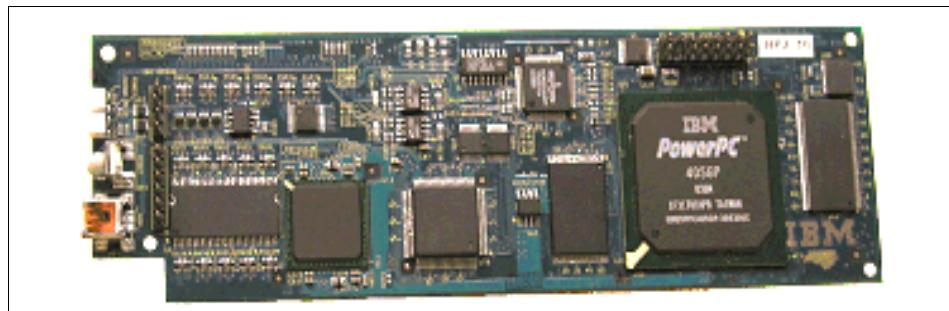


Figure 3-5 RSA II SlimLine adapter

The RSA II SlimLine has no external connectors and no video card, unlike the PCI version of RSA II (the connectors you can see on the left-hand side in Figure 3-5 on page 54 are not used). Servers where SlimLine is supported have a dedicated Ethernet connector for the RSA II SlimLine.

The RSA II SlimLine in the current xSeries servers has the following limitations:

- ▶ No alphanumeric or numeric pager alerts.
- ▶ No character-based console redirection out the server's serial port. Graphical console redirection is supported, and character-based Serial Over LAN redirection is supported by the BMC using OSA SMBridge.

Refer to the *Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide* or the *Installation Guide* for your server for current limitations.

The RSA II SlimLine coexists with the integrated Baseboard Management Controller (BMC) of the server. For details of BMC, see Chapter 2, “Baseboard Management Controller” on page 7.

When the RSA II SlimLine adapter is installed in a BMC-based server, the BMC remains enabled. Consequently, if you have already configured the BMC with an IP address, that access will still be available to those users defined in the BMC's user access list. In addition, out-of-band communications via the BMC cannot be made secure with encryption as the RSA II can.

For consistent and secure management, we recommend that you reconfigure the BMC and change its IP address to 0.0.0.0. This will ensure that all out-of-band

communication will be via the RSA II SlimLine adapter, which can be made secure, as described in Chapter 5, “Security and authentication” on page 129.

Note: Unlike the RSA II and RSA II-EXA, the RSA II SlimLine does not support the ASM interconnect network. Instead, the service processor connects directly to the customer’s Ethernet network, and not via a separate management network.

3.3 Advanced Systems Management network

The Advanced Systems Management network is for interconnectivity of legacy service processors with the Remote Supervisor Adapter II. Service processors that can form this ASM network are:

- ▶ Remote Supervisor Adapter II
- ▶ Remote Supervisor Adapter
- ▶ Integrated Systems Management Processor
- ▶ Advanced Systems Management PCI Adapter
- ▶ Advanced Systems Management Processor

The last two devices are not covered in this book. See section 6.1.5 of the IBM Redbook *Implementing Systems Management Solutions using IBM Director*, SG24-6188, for details.

With this ASM network, these service processors can route alerts and management functions and can share Ethernet and modem connections.

Important: The ASM network is to connect legacy service processors. Many current and future xSeries servers (using the BMC or RSA II SlimLine controllers) will no longer support or need the ASM network. Instead, alerts and management functions are performed directly with the service processor via one of the server’s Gigabit Ethernet ports.

For a table showing which servers support the ASM network (also known as the ASM interconnect network), see:

<http://www.redbooks.ibm.com/abstracts/tips0146.html>
<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

The RSA II works as a gateway for the ASM network. It can provide access to the connected management processors (that have no Ethernet connection) from the LAN and is the gateway for the management processors to the LAN.

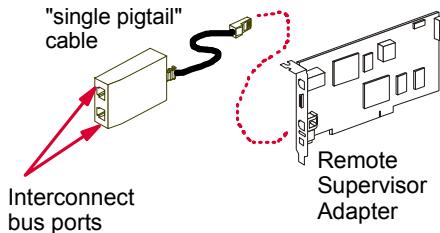
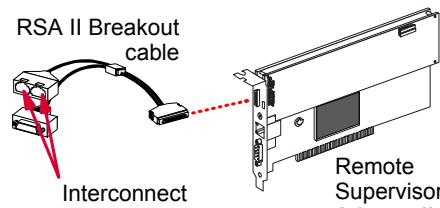
You need the following components to build an ASM network:

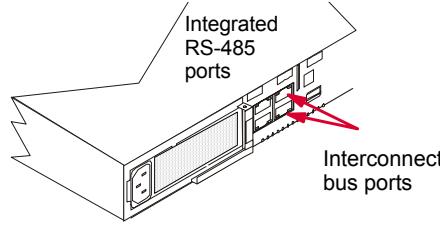
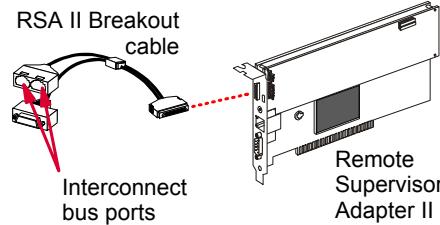
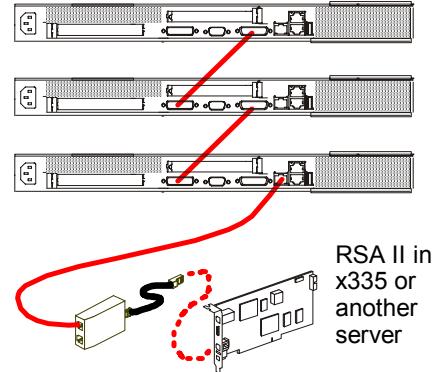
- ▶ At least one gateway device (an RSA II)
- ▶ Member devices (for example, ISMPs, RSA Is, and RSA IIs)
- ▶ Category 5 Ethernet cables (not crossover cables)
- ▶ ASM interconnect/serial port breakout cable for the RSA II (Figure 3-2 on page 52) or RSA II-EXA (Figure 3-4 on page 53)
- ▶ Terminators—one for each end of the network

Joining each server to the interconnect bus requires two RS-485 ports so that you can connect the server to two other partners in the daisy chain. You can achieve this requirement in one of two ways:

- ▶ Use the ASM interconnect/serial port breakout cable for the Remote Supervisor Adapter II.
- ▶ Directly, when the server has two RS-485 ports on the rear of the chassis.

Table 3-2 Hardware required to form the ASM interconnect network

Configuration	Models	Location of the interconnect ports
Servers with either no onboard service processor and the addition of a Remote Supervisor Adapter, or the Remote Supervisor Adapter standard in the server: ▶ Use the single pigtail cable that ships with the adapter.	x205 x225 x220 x305 x360 x440 x445 x450 x455	 <p>"single pigtail" cable</p> <p>Interconnect bus ports</p> <p>Remote Supervisor Adapter</p>
Servers with no onboard service processor, with the addition of a Remote Supervisor Adapter II or the Remote Supervisor Adapter II standard in the server: ▶ Use the breakout cable that ships with the adapter.	x205 x206 x225 x226 x305 x306 x365 x445 e326	 <p>RSA II Breakout cable</p> <p>Interconnect bus ports</p> <p>Remote Supervisor Adapter II</p>

Configuration	Models	Location of the interconnect ports
<p>Servers with integrated ISM processor and with RS-485 ports on the rear of the server chassis:</p> <ul style="list-style-type: none"> ▶ No additional cables are required. <p>Note: Ensure that the latest service processor firmware is loaded.</p>	x232 x235 x255 x342 x345	 <p>Integrated RS-485 ports</p> <p>Interconnect bus ports</p>
<p>Servers with an ISM processor, with an optional Remote Supervisor Adapter II:</p> <ul style="list-style-type: none"> ▶ Use the breakout cable that ships with the adapter. <p>Note: In this situation, the Remote Supervisor Adapter II takes over the role as service processor. The ISM processor is disabled.</p>	x235 x255 x335 x345	 <p>RSA II Breakout cable</p> <p>Interconnect bus ports</p> <p>Remote Supervisor Adapter II</p>
<p>Servers using Cable Chaining Technology (C2T):</p> <ul style="list-style-type: none"> ▶ When the server only has the onboard ISM processor, the ASM interconnect is made using the C2T cabling only. Connection to other servers is via the ISM port on the last x335. ▶ When the server also has an RSA II installed, or the x335s are connected to another server with an RSA II, the ISM port is connected to the ASM port of the RSA breakout cable, as shown here. <p>Do not use an RSA II in a x335 within a C2T chain unless you have made a special support agreement with IBM. Therefore, contact an IBM representative. A better solution is to install the RSA II in another server than the x335. However, remote video is not supported over the C2T. Refer this table's footnote b on page 50.</p> <p>Note: Even though C2T allows up to 42 servers to be connected, only 24 can form a single ASM interconnect network. See the <i>Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide</i> for information about cabling in this instance.</p>	x335	 <p>RSA II in x335 or another server</p>

For details on older servers, systems management adapters, and processors refer to Chapter 6 of the IBM Redbook *Implementing Systems Management Solutions using IBM Director*, SG24-6188.

3.3.1 Specifying the ASM Gateway

The concept of a ASM interconnect *gateway* is relevant only for ISM processors.

Service processors other than the ISM processor are able to communicate with all other service processors on the ASM interconnect bus and determine what type of device each is and what resources (modems and Ethernet connections) each has.

ISM processors, on the other hand, are unable to determine what type other service processors are or what resources they have attached to them.

As a result, ISM processors need to be “told” where to send alerts so that those alerts can be forwarded to intended recipients. The device to which the ISM processors send alerts is called the *ASM gateway*.

Any RSA or RSA II (not RSA II SlimLine) can be the gateway. You can tell which device is the current gateway via the RSA Web interface—in the Access Remote ASM menu selection, the gateway has (G) listed, as shown in Figure 3-6.

Remote ASM Access 			
System Health	ASM Name	ASM Interconnect Connection	Direct LAN Connection
 (G)	chicago-rsa	login	9.24.104.114
	Lenzburg	login	9.24.104.181
	Oslo-RSA	login	9.24.104.154

Figure 3-6 The gateway has a (G) in the System Health column

When an event occurs, the reporting ISMP sends the alert only to the gateway. The gateway then either sends out the alert or forwards it to another RSA to be delivered to the intended recipient.

Important: The gateway RSA or RSA II *must* have alert recipients configured. If not, when it receives an alert from an ISM processor, it will neither send the alert to the recipient nor forward it to another RSA.

As the gateway service processor must have alert recipients configured, it is often convenient to force a particular RSA to be the gateway. This can be

achieved by clicking the **Make this ASM the Gateway** button in the Alerts section of the service processor configuration Web page.

Once you make the RSA or RSA II the gateway, it will remain the gateway until it goes offline. At that point, the remaining RSA and RSA II devices will negotiate which one is to be the gateway. If the original gateway comes back online, it will become the gateway again.

Important: If the gateway service processor goes offline and the new elected gateway does not have any remote alert recipients configured, then alerts from ISM processors will *not* be sent. For this reason, you should configure alerting on all potential gateway devices (that is, all RSA and RSA II service processors). You should also ensure all potential gateway devices have alert recipients defined consistently.

Compare the ISM processor with the other service processors, such as the Remote Supervisor Adapter, ASM processor, and ASM PCI adapter. These others do not need a gateway to send alerts. If an RSA cannot send an alert itself, it will find another RSA on the RS-485 network that can send the alert, then forward its alert to that RSA.

No one service processor “owns” the ASM interconnect network. All service processors (other than ISM processors) either send alerts themselves or know which other one can send if they cannot. The information about the capabilities of other service processors on the network is part of the heartbeat messages that they send to each other every 45 seconds or so.

The ISM processors ignore this information from the other service processor and always simply send their alerts to the gateway device. The gateway, knowing what resources are where on the network, then sends the alerts itself or sends them to the appropriate service processor that does the sending.

3.4 Basic configuration of Remote Supervisor Adapter II

To use the functionality of the RSAs, you first have to configure the adapter. In this section, we describe the basic configuration steps. For more configuration options refer the *Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User’s Guide* and Chapter 7, “Scenarios and best practices” on page 233 in this book.

3.4.1 Installing the RSA II

The RSA II is installed in a specific slot, as listed in Table 3-1 on page 49. If you use the RSA II SlimLine, install it in the connector designed for it on the system planar of the server. For the location of the connector, refer the documentation that came with your server.

Important: Update the server's BIOS and BMC firmware to the latest level *before* installing the RSA II.

To install the RSA II adapter, do the following:

1. Connect the 20-pin (26-pin for x225/x226) ribbon cable to the RSA II and the onboard or riser card connector. Refer to the server's documentation for location of this connector.
2. Connect the mini USB cable to the RSA II and one USB port of the server, except if the server is an x225, x226, or x365—for these servers, the ribbon cable contains the USB signal. For x445, install the breakout cable, which includes the USB cable.

Note: If you plan a new installation of Red Hat Linux on a x235 or x345 using a locally attached PS/2® mouse, connect the mini USB cable *after* installing the operating system. During the installation process Red Hat can use only one type of mouse and will use USB if present. Refer to RETAIN® tip H177279 at:

<http://www.pc.ibm.com/support?page=MIGR-50413>

3. Disconnect the video cable from the video connector of the onboard video card and connect it to the RSA II.
4. Attach an Ethernet cable to the Ethernet port of the RSA II.
5. If you want to create an ASM interconnect network or plan to connect a modem to the RSA II, attach the ASM breakout cable. For x445 it is necessary to attach the breakout cable, because it contains the USB connector for the server's USB port.
6. To connect the RSA II SlimLine to the Ethernet network, plug an Ethernet cable into the dedicated Ethernet port of your server. For the location of this port please refer the server's documentation.

3.4.2 Network settings

After installing the adapter in your server, you have to configure the network settings to connect to the RSA II using the Web interface or telnet. Ensure that

you have upgrade the adapter to the latest firmware and that it is the firmware for this particular server.

To configure the network settings, do the following:

1. Boot your server and press F1 to go to the BIOS settings.
2. Select **Advanced Setup → RSA II Settings**.

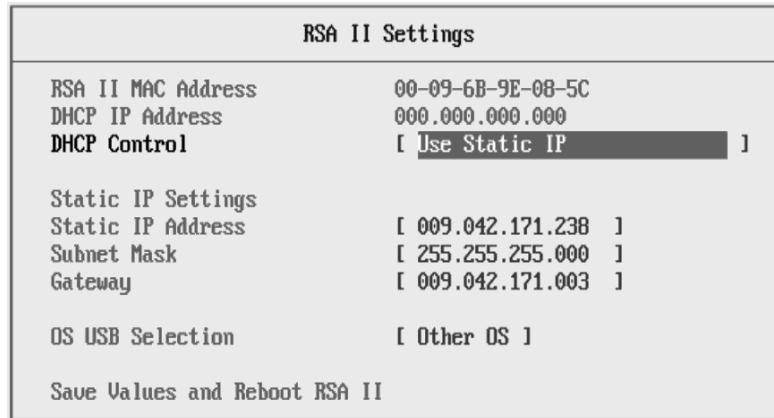


Figure 3-7 RSA II Settings in server BIOS

3. Change the DHCP control to Use Static IP by using the right and left arrow keys. We recommend that you use a static IP address for the RSA II so that you can still get access even if DHCP problems occur.
4. Fill in the IP address you want to assign to the RSA II, the network's subnet mask, and the standard gateway. Contact your network administrator for details.
5. Select **Other OS** for Windows operating system or **Linux OS** as OS USB Selection. Use the right and left arrow keys for selection.

The purpose of this selection is to prevent a known problem with Linux and its generic human interface device (HID) driver. Linux cannot establish USB communication with the RSA II using the generic HID (which Windows uses). By selecting **Linux OS** here, it makes the RSA II appear as an OEM HID instead of generic HID, which then functions properly.

Now select **Save the Values and Reboot RSA II** with the arrow keys and press Enter. Exit the utility.

Tip: To check the network connection of RSA II use the PING command from another system connected to the network.

3.4.3 Update firmware

The next step is to update the firmware of the RSAII to the most recent version.

Tip: Other methods to remotely update firmware are described in 7.8, “Remote BIOS and firmware updates” on page 256.

The firmware of the RSA II is specific to the server the adapter is installed in, so ensure that you download the correct version. Download the firmware via the appropriate link on the *Remote Supervisor Adapter II Family — Firmware and Drivers Cheatsheet*, TIPS0532:

<http://www.redbooks.ibm.com/abstracts/tips0534.html>

Alternatively, go to <http://www.pc.ibm.com/support> and navigate to your server and find the link under **Advanced Systems Management** for your server.

As you can see from the cheatsheet, there are up to three ways to update the firmware of the RSA II:

- ▶ Locally on the server running Windows
- ▶ Locally on the server running Linux
- ▶ From the RSA II Web browser interface using packet (PKT) files

We will be using the PKT files to update the firmware.

Note: If you are planning to move the RSA II to another server:

- ▶ If you plan to use the Windows or Linux-based firmware update utilities, you should install the adapter in the new server first, then update the RSA II firmware. You may get some error messages during POST, but these can be ignored and will go away as soon as the firmware is updated.
- ▶ If you plan to use the Web browser interface to flash the adapter, do the firmware update first using the **Advanced Options** link, then move the adapter.
- ▶ On some servers, there may still be leftover VPD data from the old server even after the firmware update. For example, on the RSA II Vital Product Data page, the Diagnostics VPD section may show values from the old server. However, the RSA II will still function correctly.

1. Click the Packet files link for your server from the Cheatsheet URL above.
2. Download the EXE file and save it to a local directory.
3. Run the EXE to extract the files. After extracting the file take a few minutes to read the readme.txt. The following files should be in your directory. Note that

there are two PKT files—you will need to perform the firmware update procedure twice, once for each file.

Name	Size	Type
26r0562.zip	1,327 KB	PKZIP File
RAETBRUS.PKT	65 KB	PKT File
RAETMNJS.PKT	1,286 KB	PKT File
readme.txt	13 KB	Text Document
RTALERT.MIB	34 KB	MIB File
RTRSAAG.MIB	268 KB	MIB File

Figure 3-8 Files of RSA II firmware update package

Tip: The firmware package suitable for update via a Web browser is delivered as a ZIP file, and the ZIP file contains only two PKT files.

Now Connect to your RSA II using a browser. Now log on to your RSA II with standard user USERID and PASSW0RD (with a zero, not the letter O) as the password, unless you have changed it. For security reasons you should change the standard password after first logon.

If you plan to install an RSA II that was previously installed and flashed in another server, you can do this, although you need to click **Advanced Options** in step 4 on page 64 below. We recommend that you flash the adapter with the new firmware before transferring the adapter to the new server. Otherwise, you may get some error messages during POST.

1. In the navigation frame click **Tasks → Firmware Update**.

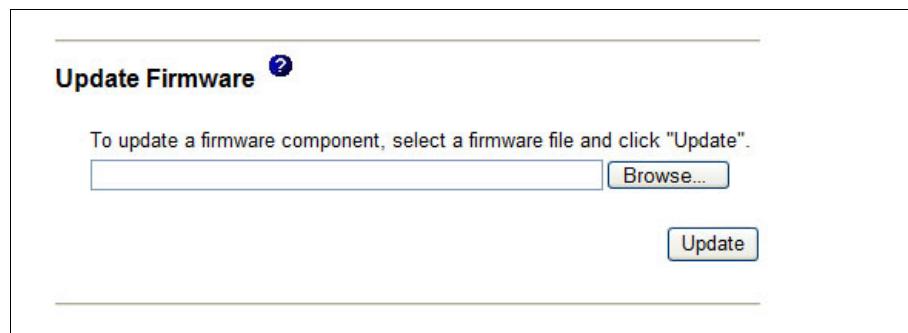


Figure 3-9 RSA II firmware update

2. Click **Browse** to select the first of two files for firmware update.

You should select the files in the correct order for updating the firmware. First select RAETBRUS.PKT (RSA Boot ROM) then RAETMNUS.PKT (RSA Main Application). Restart RSA only after applying both files.

3. To update click **Update**. The file is now transferred to the RSA II.
4. Click **Continue** to flash the RSA II, or if you are flashing the adapter with firmware for another server, do the following:
 - a. Click **Advanced Options**.

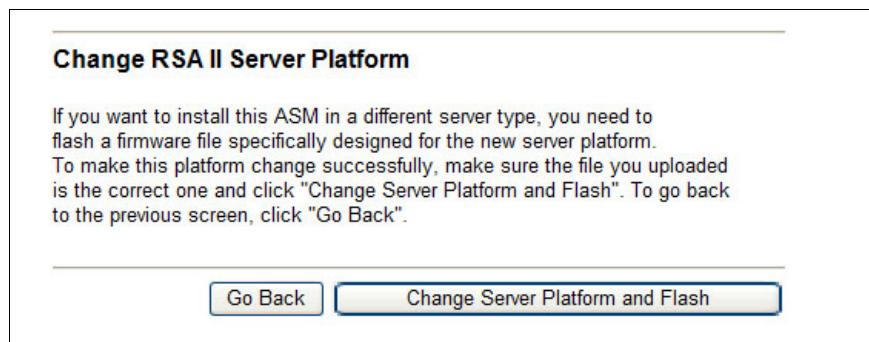


Figure 3-10 Advanced Options window

- b. Click **Change Server Platform and Flash**.
- c. Click **OK** to confirm the action.
5. Repeat step 1 to 4 for the second PKT file.
6. Restart the adapter by clicking **ASM Control** → **ASM Restart**.

Tip: If you update an RSA II in an x205, x235, x255, or x345 and the display shows stripes, you will also have to update the video BIOS of the RSA II. Download this at the same location as the firmware but select **BIOS (adapter)** in the category filter. Extract the file to a diskette and boot your server with it. Follow the instructions.

Now you can configure other options of RSA II as described in the remainder of this chapter.

3.4.4 Installing the device driver

The operating system you run on your server needs a driver for the RSA II adapter.

Tip: This RSA II driver you download from the Web is a different one from the driver for the older service processors. The RSA II driver installs as a Windows service or Linux daemon.

Download the driver via the appropriate link on the *Remote Supervisor Adapter II Family — Firmware and Drivers Cheatsheet*, TIPS0532:

<http://www.redbooks.ibm.com/abstracts/tips0534.html>

Alternatively, go to <http://www.pc.ibm.com/support> and navigate to your server and find the link under **Advanced Systems Management** for your server.

Windows service installation

The installation of the RSA II server software package is unlike the driver installations of older systems management adapters. It is done by executing the downloaded executable file.

Attention: Before installing the RSA II software, if a USB cable is needed (see Table 3-1 on page 49), make sure it is connected between the RSA II and a USB port on the server. Also, for Windows, make sure the RSA II is configured for *Other OS* in the system BIOS (Figure 3-7 on page 61).

The installation is as follows:

1. Execute the downloaded EXE file on the server with the RSA II.
2. Optionally click **Change** to specify an alternate temporary folder for the installation files.
3. The installation process starts automatically after the files are copied.
4. Follow the instructions.
5. When installation finishes you can delete the files in the temporary folder.

To determine if the installation was successful, check the services for the IBM Remote Supervisor Adapter II:

1. In the taskbar click the button **Start**.
2. Then click **All Programs** → **Administrative Tools** → **Services**.

Scroll down to the service IBM Remote Supervisor Adapter II and verify that the status is started.

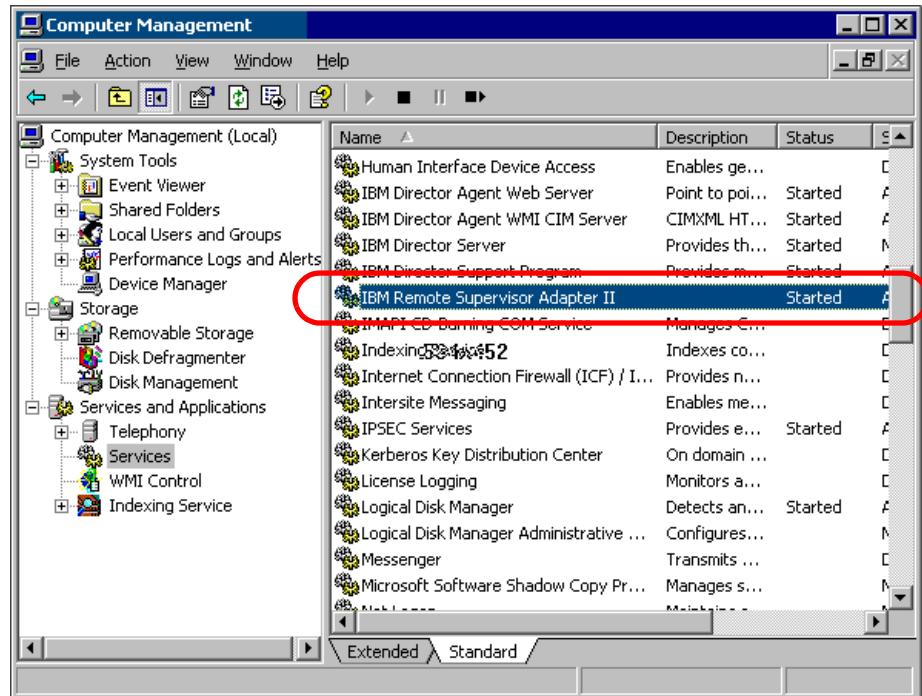


Figure 3-11 RSA II service in Windows 2003

Linux daemon installation

To install the Linux deamon for the RSA II, first download it from the IBM support Web site. Use the steps in 3.4.4, “Installing the device driver” on page 64.

1. Select the correct rpm package for your Linux distribution (Red Hat or SUSE LINUX).
2. Review the appropriate readme file of the rpm package for prerequisites and installation steps.

Attention: Before installing the RSA II software, if a USB cable is needed (refer Table 3-1 on page 49), make sure it is connected between the RSA II and a USB port on the server. Also make sure the RSA II is configured for Linux OS in the server's BIOS (Figure 3-7 on page 61).

3. Copy the downloaded file to a folder of the Linux server, for example, /tmp/inst.
4. Install the daemon (for example, SUSE, where xx is the version):

```
rpm -ivh ibmusbasm-1.xx.i386.rpm
```

Now you can check for the daemon running. Use the **ps** command as shown in Example 3-1.

Example 3-1 Command to verify the RSA daemon is running

```
linux:~ # ps -ef | grep ibmasm
root      11056      1  0 10:47 pts/1    00:00:00 /sbin/ibmasm
root      11060  11056  0 10:47 pts/1    00:00:00 /sbin/ibmasm
root      11062  10996  0 10:48 pts/1    00:00:00 grep ibmasm
linux:~ #
```

If /sbin/ibmasm appears in the list, the daemon is running. The ibmasm daemon is started automatically during boot process of the operating system.

To start the daemon manually use the command **ibmspup**. To stop the daemon, enter **ibmspdown**.

3.4.5 MIB files

The RSA II supports SNMP from many management tools including IBM Director. If you require MIB files, these can be found on the RSA II firmware update for your server, in the ZIP file that also includes the PKT files. See the xSeries software matrix to download the ZIP file:

<http://www.ibm.com/pc/support/site.wss/MIGR-4JTS2T.html>

3.5 Remote console and remote media

To manage servers from a remote location, you need more than just keyboard-video-mouse (KVM) redirection. For example, for the installation of an operating system or patches, you need remote media to connect a CD-ROM or diskette to the server.

Tip: It is possible to mount more than one remote drive concurrently. For example, you could mount a CD-ROM and a diskette or diskette image.

Using remote media requires USB support from the operating system while the OS is up and running or during installation of OS. Remote media works with the following operating systems:

- ▶ Windows Server 2003
- ▶ Windows 2000 Server with Service Pack 4 or later
- ▶ Red Hat Enterprise Linux AS 3, but not for OS installation
- ▶ SUSE LINUX Enterprise Server 8, but not for OS installation

A Java™ runtime is required, which can be installed by going to:

<http://www.java.com/en/download/manual.jsp>

Restriction: Remote media is not supported during the installation of Red Hat and SUSE LINUX because the installers have problems recognizing or mounting/unmounting the remote CD-ROM. This is due to be corrected in future versions of the Linux distributions.

For the most recent information for your specific combination of RSA II and xSeries, check the IBM ServerProven Web site and click the relevant checkmark in the table:

<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

When you launch a remote console for the first time in your browser a security warning window will pop up. This warning comes from the Java applets that remote control uses. It is quite usual to see these warnings, and you can trust this certificate from IBM and click **Yes** or **Always**.



Figure 3-12 Security warning

For more details on this warning click **More Details** or to continue click **Yes**.

Tip: This window will pop up every time you enter remote control unless you click **Always**.

In the remote control window, there is a set of buttons that simulate specific keystrokes and the video speed selector, as shown in Figure 3-13. The slider is used to limit the bandwidth that is devoted to the remote console display on your computer.

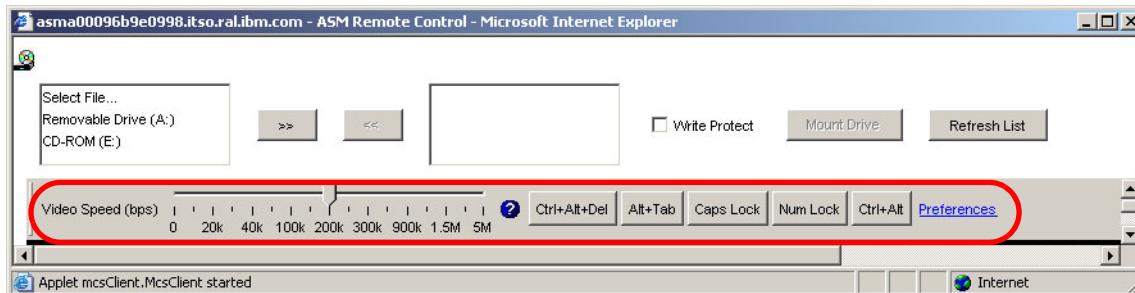


Figure 3-13 RSA II - Remote control buttons

Reducing the video speed can improve the rate at which the remote console display is refreshed by limiting the video data that must be displayed. You can reduce, or even stop, video data to allow more bandwidth for remote disk, if desired. Move the slider left or right until you find the bandwidth that achieves the best results.

Each of the buttons represents a key or a combination of keys. If you press a button, the corresponding key stroke sequence will be sent to the server. If you require additional buttons, click **Preferences**, where you can modify or create new key buttons.

Tip: The BladeCenter management module Web interface for remote console looks very similar, but it does not have the ability to modify or create user-defined remote control buttons.

The button bar can be detached by clicking anywhere in the grey background and dragging. Drop the button bar to create a separate window.



Figure 3-14 Detached button bar

The Preferences link also lets you specify your keyboard and enable mouse synchronization (that is, ensure the mouse pointer on the remote system precisely follows the local mouse pointer). The following keyboard types are supported:

- ▶ US 104-key keyboard
- ▶ Belgian 105-key keyboard
- ▶ French 105-key keyboard
- ▶ German 105-key keyboard
- ▶ Italian 105-key keyboard
- ▶ Japanese 109-key keyboard
- ▶ Spanish 105-key keyboard
- ▶ UK 105-key keyboard

3.5.1 Linux support for remote control

When using the remote control feature with a Linux distribution, there are some additional configuration steps needed in the operating systems to make the remote mouse and keyboard work. These steps are necessary because the local keyboard and mouse are usually devices with PS/2 connectors. The remote control uses USB devices, and these must be added manually.

Complete the following steps to configure the USB mouse and keyboard in Linux:

1. Log in to a text screen (press Ctrl+Alt+F1 if you are in GUI mode).
2. Change the video driver to a VESA driver.

In the /etc/X11/XF86Config (/etc/X11/XF86Config-4 for Red Hat) file, search for the word *radeon* and replace it with *vesa*.

3. Color depth and window size.

Edit the file /etc/X11/XF86Config to look as follows:

Section “Screen”

```
DefaultDepth 16
SubSection "Display"
    Depth 16
    Modes "1024x768"
EndSubSection
...
```

Be sure that the Depth value is 16 (add the Depth line above, if necessary) and the Modes value is 1024x768 only. Delete the other mode values.

For Red Hat, change ‘dmbs’ to ‘off’ in the ‘Monitor’ section.

4. Enable PS/2 and USB mouse support.

To configure the mousedev module and usb-storage module (for USB storage support) to load at startup, edit the /etc/init.d/boot.local file, and at the end of the file, add these lines:

```
/sbin/modprobe mousedev
/sbin/modprobe usb-storage
```

To activate this support without rebooting, you can also enter both these commands at the command prompt.

5. Add the new input device to the X Window System configuration file.

- For SUSE LINUX, add the following lines to file /etc/X11/XF86Config:

```
Section "InputDevice"
    Driver "mouse"
    Identifier "USB Mouse"
    Option "Device" "/dev/input/mice"
    Option "Name" "AutoDetected"
    Option "Protocol" "IMPS/2"
    Option "Vendor" "AutoDetected"
EndSection
```

Add the second mouse and specify that it sends core events:

```
Section "ServerLayout"
    Identifier "Layout[all]"
    InputDevice "Keyboard[0]" "CoreKeyboard"
InputDevice "Mouse[1]" "SendCoreEvents"
InputDevice "USB Mouse" "CorePointer"
    Screen "Screen[0]"
EndSection
```

Change
"CorePointer" to
"SendCoreEvents"

Add this new
line

- For Red Hat Linux, add the following lines to file /etc/X11/XF86Config-4:

```
Section "InputDevice"
    Identifier "USB_Mouse"
    Driver "mouse"
    Option "Protocol" "IMPS/2"
    Option "Device" "/dev/input/mice"
EndSection
```

Add the second mouse and specify that it sends core events:

```
Section "ServerLayout"
    Identifier "Anaconda Configured"
    Screen 0 "Screen0" 0 0
InputDevice "USB Mouse" "CorePointer"
InputDevice "Mouse0" "SendCoreEvents"
EndSection
```

Add this
new line

Change
"CorePointer" to
"SendCoreEvents"

6. After these changes, restart the X Windows system by pressing Ctrl+Alt+Backspace.

7. To provide the correct resolution information to the mouse handler if your resolution is not 1024 x 768, do the following:
 - a. Type `init 3` at the Linux command prompt.
 - b. Unload the mouse driver module. Type `rmmmod mousedev` to do this.
 - c. Add the following statement to the file `/etc/modules.conf`:


```
options mousedev xres=X, yres=Y
```

 Where *X* and *Y* specify the video resolution.
 - d. Reload the mouse driver module with the command `insmod mousedev`.
 - e. Change back to runlevel 5, by typing `init 5`.
8. To synchronize the local and the remote mouse during remote control sessions (so that the two mouse pointers move in unison), the settings for the graphical login screen (XDM) and for your preferred GUI (such as KDE or GNOME) must be changed.

Tip: We only describe KDE and GNOME here. If you are using WindowMaker, MWM, or TWM, refer to *IBM Remote Supervisor Adapter II Technical Update for Linux, 2nd Edition (November 2003) - 88P9248*, which came with the RSA II. You can download this document at <http://www.pc.ibm.com/support>. Search for the document number.

- For XDM do the following:
 - i. Change to run mode 3 by typing `init 3`.
 - ii. For SUSE LINUX, add the following line just before the `exit 0` line to the file `/etc/X11/xdm/Xsetup`:


```
$xset m 1 1
```
 - iii. For Red Hat, add the following line just before the `exit 0` line to the file `/etc/X11/xdm/Xsetup_0`:


```
xset m 1 1
```
 - iv. Save the file and change to runmode 5 by entering `init 5`.
- For KDE, complete the following steps to set the mouse acceleration and threshold values if you are using the KDE:
 - i. Using the keyboard, press Alt+F1 or Ctrl+Esc to open the menu on the desktop.
 - ii. From the menu, click **Preferences** → **Peripherals** → **Mouse**.
 - iii. Select the **Advanced** tab and change the Pointer Acceleration and Threshold values to 1.

- iv. Log out from this session and be sure to check the **Save current setup** check box in the Log out window.

The next time you log in, the remote and local mouse are synchronized.

- For GNOME, complete the following steps to set the mouse acceleration and threshold values:
 - i. Using the keyboard, press Alt+F1 or Ctrl+Esc to open the menu on the desktop.
 - ii. From the menu, select **Programs → Settings → Session → Session Properties & Startup Programs** or **Extras → Preferences → Sessions** (depending on the Linux version).
 - iii. Select the **Startup Programs** tab; then select **Add** to open another window.
 - iv. On the command line, type `xset m 1 1`, and click **OK** to save this command.
 - v. Click **Apply** and then click **OK** to exit this window. Log out from this session and be sure to check the **Save current setup** check box on the Log out window.

The next time you log in, the remote and local mouse are synchronized.

Tip: To synchronize the local and remote mouse pointer (bring the local and remote mouse arrows on top of each other) for the first time, move the pointer in one of the corners of the display so that the local and remote mouse pointer are at the same position.

On the next restart of the operating system, new hardware will be detected.

Attention: At the next reboot of the system the hardware detection programs of Linux will detect new hardware. Read the following instructions carefully.

► For SUSE LINUX:

On the next restart of the server, the SUSE LINUX operating system hardware detection service program (YaST2) will detect hardware changes. *Do not* let YaST2 make any configuration changes, because you manually added devices (for example, the USB mouse) that are only seen by the operating system, when remote console is connected to the server. Click **Cancel** when prompted.

- ▶ For Red Hat:

On the next restart of the server, the Red Hat Linux operating-system hardware detection service program (Kudzu) will detect hardware changes. The following table lists the Kudzu queries and suggested user responses.

Table 3-3 Kudzu messages and recommended user action

Kudzu query	User response
ATI Rage XL has been removed	Select Keep Configuration .
Generic USB mouse has been added	Select Ignore .
ATI RADEON has been added	Select Ignore .
Generic USB keyboard has been added	Select Ignore .

3.5.2 Using remote media

Before using remote media support, check the available bandwidth of the network connection. It works well in a 100 Mbps LAN environment. If you have a low bandwidth WAN connection, the performance may be unsatisfactory.

You can use remote media during the booting process or when the operating system is up and running (see the restrictions described in 3.5, “Remote console and remote media” on page 67). With this feature of the RSA II, a complete installation of the server from a remote location, including operating system and patches, is possible. This includes:

- ▶ BIOS update of server (diskette based)
- ▶ Update of diagnostics (two diskettes plus one diskette of BIOS update for booting)
- ▶ Firmware upgrade of ServeRAID™ adapters and RAID configuration when booting ServeRAID CD

Tip: When using a remote diskette or CD-ROM with Red Hat Enterprise Linux AS 3 or SUSE LINUX Enterprise Server 8, the system may hang or not recognize the remote device. This issue will be corrected in future Linux versions. Refer to RETAIN tip H181968 at:

<http://www.ibm.com/pc/support/site.wss/MIGR-55671.html>

The work around for the above restriction is to stop the daemon while you are using the remote console with remote media; then once completed, restart the daemon. The steps are as follows:

1. From the Linux command prompt unload the ibmasm daemon using the command:
`ibmspdown`
2. Mount the remote device manually. For details refer to:
 - 3.5.3, “Remote diskette” on page 77
 - 3.5.4, “Remote CD-ROM and DVD” on page 80
 - 3.5.5, “Remote file” on page 82
3. Use remote media in conjunction with the remote console to perform your management tasks, as described below.
4. Once you have finished, restart the ibmasm daemon with the command:
`ibmspup`

To use remote media, do the following:

1. Open a browser window and access the RSA II Web interface.
2. Click **Tasks → Remote Control**.
3. Select single or multi-user mode. There are two options to start a remote console:
 - Single user mode, where no other person can use remote control on this RSA II until you end your session. You would normally use this mode. Click **Start Remote Control in Single User Mode**.
 - Multi-user mode, where other users can access remote consoles during your session. You would typically use this mode only if you want two administrators to have control of the mouse, keyboard, and display at the same time. This can create a “race condition,” whereby each user is “fighting” for control over the mouse and keyboard. Click **Start Remote Control in Multi User Mode**.
4. At the remote console window, you can mount remote media to your server by selecting the device (file, diskette, or CD-ROM) and clicking **>>**.
5. Select other devices if you need more than one.
6. Optionally click **Write Protect** to prevent writing to any device.
7. Click **Mount Drive**.

8. If you are running Windows on your server, you should now be able to access the media as a drive letter. For Linux, you will need to mount the drive as described in:
 - 3.5.3, “Remote diskette” on page 77
 - 3.5.4, “Remote CD-ROM and DVD” on page 80
 - 3.5.5, “Remote file” on page 82

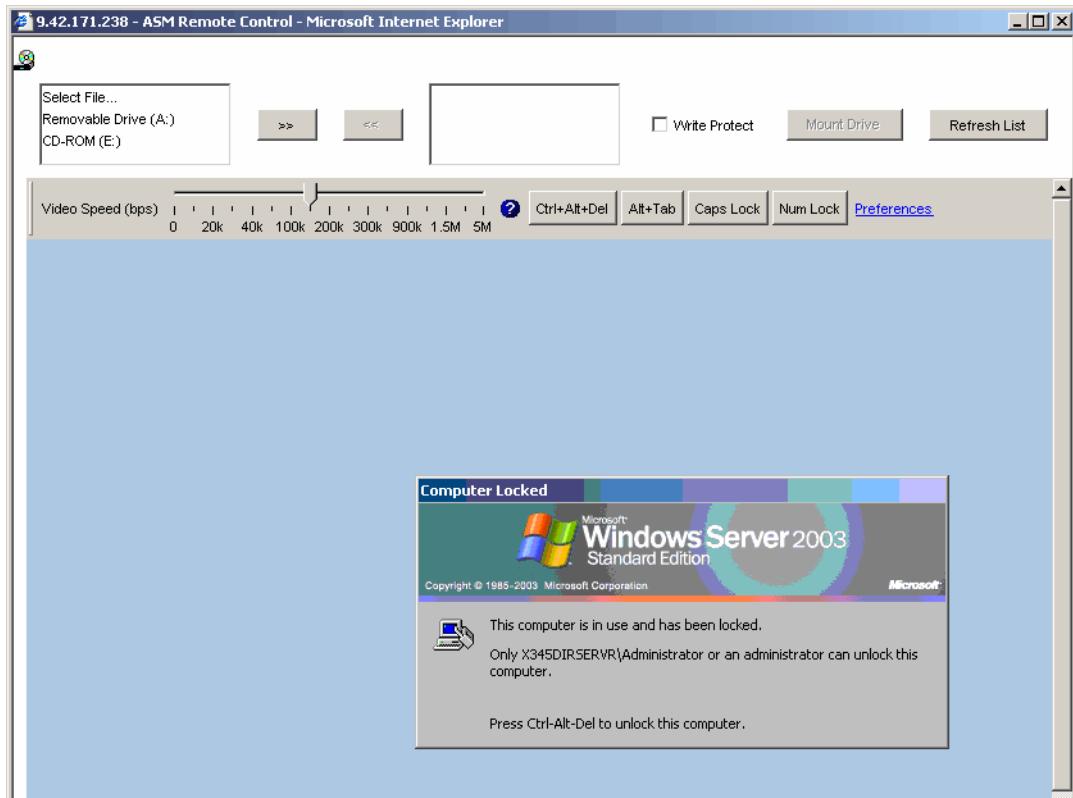


Figure 3-15 Remote console and remote media

9. To unmount remote media do the following:

For Windows:

- a. Double-click the Safely Remove Hardware icon in the task bar of your remote console.



Figure 3-16 Safely removing hardware via the Windows task bar

- b. In the opened window click **USB Mass Storage Device** and **Stop**.

- c. Click **IBM Remote Disk USB device** and **OK**. A message will appear that it is now safe to remove the hardware.
- d. Click **Close** to close the window.

For Linux, unmount the remote drive with the **umount** command at operating system level. For example, if your mount command was **mount /dev/sdb /media/floppy**, then use **umount /media/floppy** now. Generally use the second parameter of the mount command (which represents the mountpoint) for unmounting.

10. Click **Unmount Drive** (the button Mount Drive changed to Unmount Drive during mount process), then << to remove it from the drives list.

3.5.3 Remote diskette

When you use remote disk, you can mount the local diskette drive to the server with the RSA II you are connected to. To use remote diskette complete the following steps:

1. Choose **Removable Drive (A:)** and click **>>**.
2. When you are asked to upload the content of the diskette drive as an image to the RSA II, you are presented with the dialog shown in Figure 3-17, where you have two options.

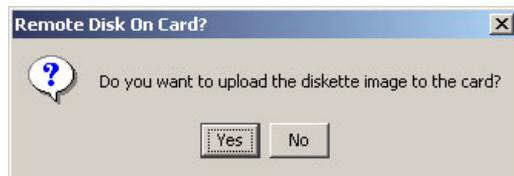


Figure 3-17 RSA II - Upload remote diskette

If you click **Yes**, the RSA II loads the diskette to its memory. A progress indicator appears. It is not necessary to click **Mount Drive**, because the mount works automatically. When completed, it is available as an additional drive or device in the operating system.



Figure 3-18 RSA II - Remote Disk On Card

If you do not want to upload the diskette image file click **No**. To make it available in the operating system click **Mount Drive**.

When booting the server and the RSA II contains a diskette image or a diskette or diskette image is mounted while remote media Web interface is still open, the server will try to boot from it. If the media is bootable but it does not work, check the boot sequence in the BIOS.

Tip: If you use the upload option, unmount the drive if no longer needed, because on next reboot the server will boot from the diskette image in the RSA II's memory if there is still one. It stays there until you click **Unmount Drive**, the RSA II is restarted, or the firmware is updated.

Windows-specific steps

In Windows, the remove media usually appears as the B drive.

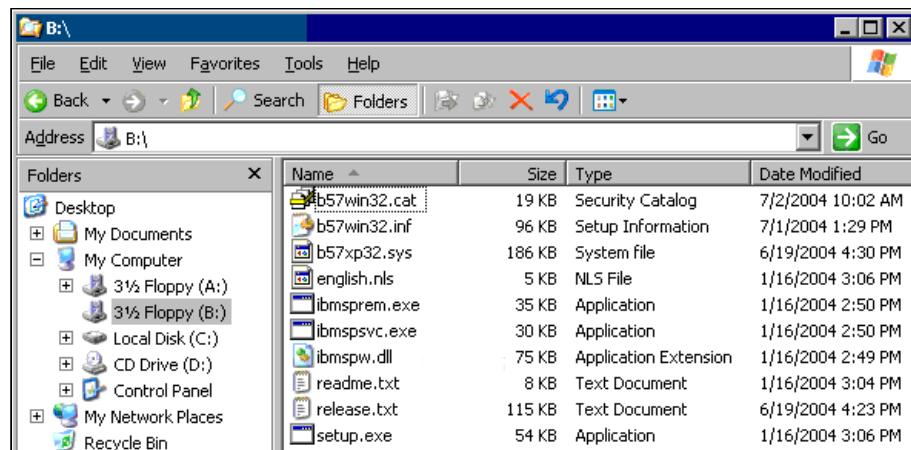


Figure 3-19 RSA II - Remote diskette on remote Windows

To unmount, launch the remote media Web interface, and follow step 9 on page 76.

Linux-specific steps

After you click the **Mount Drive** button the Linux operating system knows the drive, but depending on your Linux distribution, you may have to mount the drive manually to get access to it. The name of the device to mount can be different from server to server, and if you used remote file before. Sometimes it is /dev/sda, sometimes /dev/sdb.

SUSE LINUX

For SUSE LINUX, after clicking the **Mount Drive** button, review the file /etc/fstab for the name of the device to mount. In Figure 3-20 on page 79, it is /dev/sda.

/dev/hda2	/	reiserfs	defaults 1 1
/dev/hda1	/data1	auto	noauto,user 0 0
/dev/hdc1	/data2	auto	noauto,user 0 0
/dev/hdc2	/data3	auto	noauto,user 0 0
/dev/hdc5	/data4	auto	noauto,user 0 0
/dev/hdc6	/data5	auto	noauto,user 0 0
/dev/hdc7	/data6	auto	noauto,user 0 0
/dev/hda3	swap	swap	pri=42 0 0
/dev/hdc3	swap	swap	pri=42 0 0
devpts	/dev/pts	devpts	mode=0620,gid=5 0 0
proc	/proc	proc	defaults 0 0
usbdevfs	/proc/bus/usb	usbdevfs	noauto 0 0
/dev/cdrom	/media/cdrom	auto	ro,noauto,user,exec 0 0
/dev/sda	/media/sda	auto	noauto,user,exec 0 0 #HOTPLUG

Figure 3-20 SUSE LINUX - File /etc/fstab and the remote drive

In the last line (circled), you can see the hotplugged remote media /dev/sda.

Important: Remote media with SUSE LINUX Enterprise Server 8 works only if SUSE Service Pack 3 is installed.

Now you can mount the remote diskette with the following command:

```
mount /media/sda
```

Or use **mount /dev/sda /media/floppy** if you also want to specify an additional mountpoint name.

After using the remote diskette, unmount the remote media. To do this, launch the remote media Web interface, and follow step 9 on page 76.

Red Hat

When using Red Hat Linux, the remote diskette is not mentioned in the file /etc/fstab. As a result, you will have to try sda, sdb, sdc, etc. until you successfully connect to the remote device.

In Figure 3-21 on page 80, we used the **mount** command and tried /dev/sda first, then /dev/sdb second.

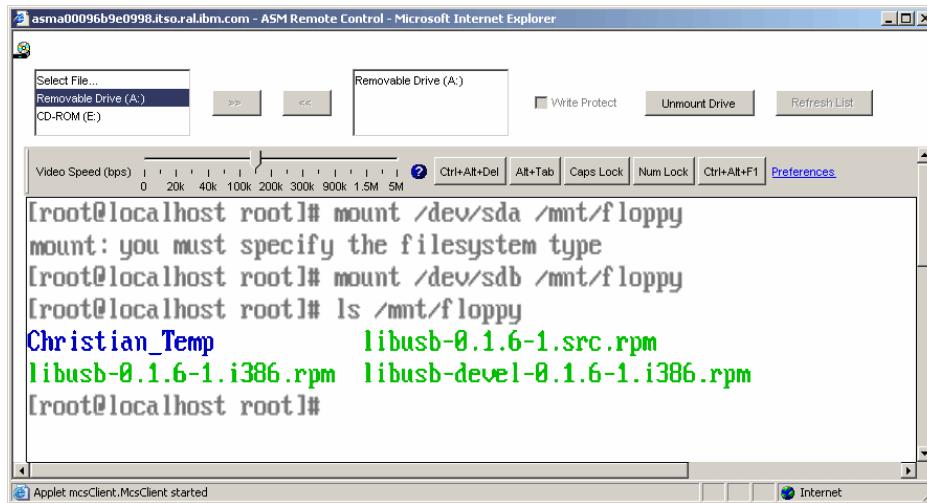


Figure 3-21 RSA II - Using remote diskette with Red Hat Linux

To unmount the device, launch the remote media Web interface, and complete the steps beginning with step 9 on page 76.

3.5.4 Remote CD-ROM and DVD

Remote CD-ROM works very similarly to remote diskette. The only difference is that the RSA II will not load the content of the CD-ROM to its memory. You can boot from a remote CD-ROM or use it as a drive letter in the operating system. Remote CD-ROM also works with DVD drives and media.

The mount is only active while the remote media Web interface is open. If you close it, you automatically unmount the media.

To use remote CD-ROM complete the following steps:

1. Choose **CD-ROM({driveletter}:)** then click **>>**.
2. When clicking **Mount Drive**, the process of mounting the CD-ROM to the remote server starts. After a short time you can use the remote CD-ROM in your operating system

Windows-specific steps

In Windows operating systems the remote CD-ROM shows as a drive letter in the operating system shortly after you press the **Mount Drive** button. Here you see it as drive E:.

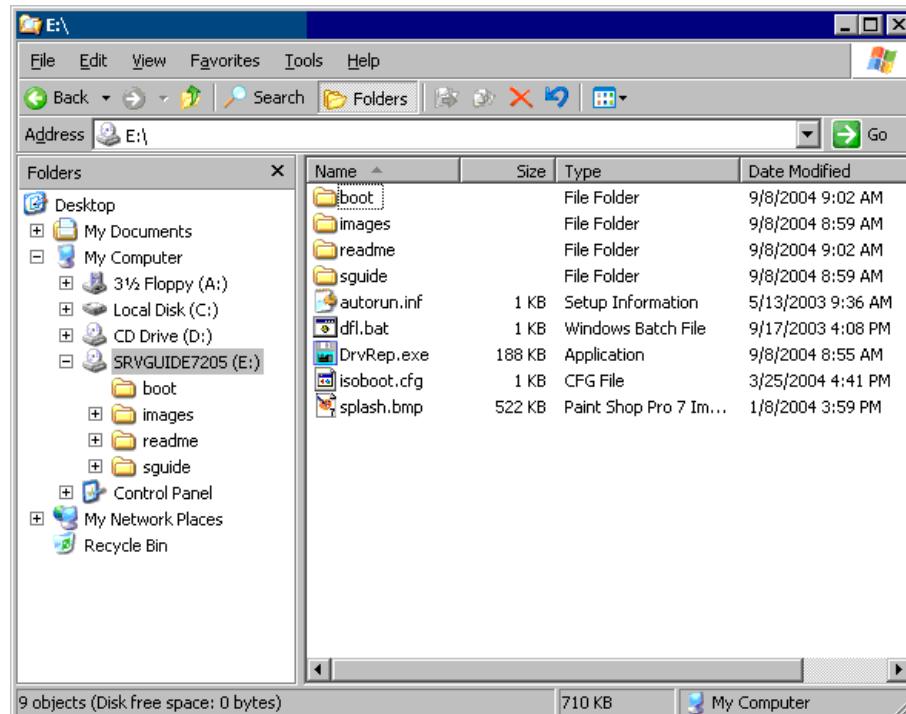


Figure 3-22 RSA II - Remote CD-ROM on remote Windows

To unmount follow the steps beginning with step 9 on page 76.

Linux-specific steps

In Linux operating systems the remote media is not mounted automatically; you have to mount it. Remote CD-ROM will be shown in the file /etc/fstab for SUSE and for Red Hat.

SUSE

Check the /etc/fstab in the operating system. You will find the device /dev/sr0. To mount it, type the following command:

```
mount /dev/sr0 /media/cdrom
```

After using remote diskette, unmount the remote media. To do this launch the remote media Web interface, and follow step 9 on page 76.

Red Hat

The following is the example for the file /etc/fstab of Red Hat Linux.

LABEL=/	/	ext3	defaults	1 1
LABEL=/boot	/boot	ext3	defaults	1 2
none	/dev/pts	devpts	gid=5,mode=620	0 0
none	/proc	proc	defaults	0 0
none	/dev/shm	tmpfs	defaults	0 0
/dev/sda3	swap	swap	defaults	0 0
/dev/cdrom	/mnt/cdrom	udf,iso9660	noauto,owner,kudzu,ro	0 0
/dev/fd0	/mnt/floppy	auto	noauto,owner,kudzu	0 0
/dev/cdrom1	/mnt/cdrom1	udf,iso9660	noauto,owner,kudzu,ro	0 0

Figure 3-23 Red Hat Linux - File /etc/fstab and the remote drive

In the last line, you can see the remote media /dev/cdrom1. Mount the drive in your operating system:

```
mount /mnt/cdrom1
```

To unmount, follow the steps beginning with step 9 on page 76.

3.5.5 Remote file

With the remote file feature, you can use diskette and CD-ROM images as a drive to mount. It works similar to remote diskette/CD-ROM. The drive image file must be an uncompressed byte-for-byte copy of a diskette, such as standard IMG or BIN files, or an ISO file.

Restrictions: The restrictions are:

- ▶ ISO image support requires RSA II firmware dated March 2005 onwards.
- ▶ ISO files need to be in ISO9660 format.

To mount a file do the following:

1. Click **Select File...**, then click the >> button.

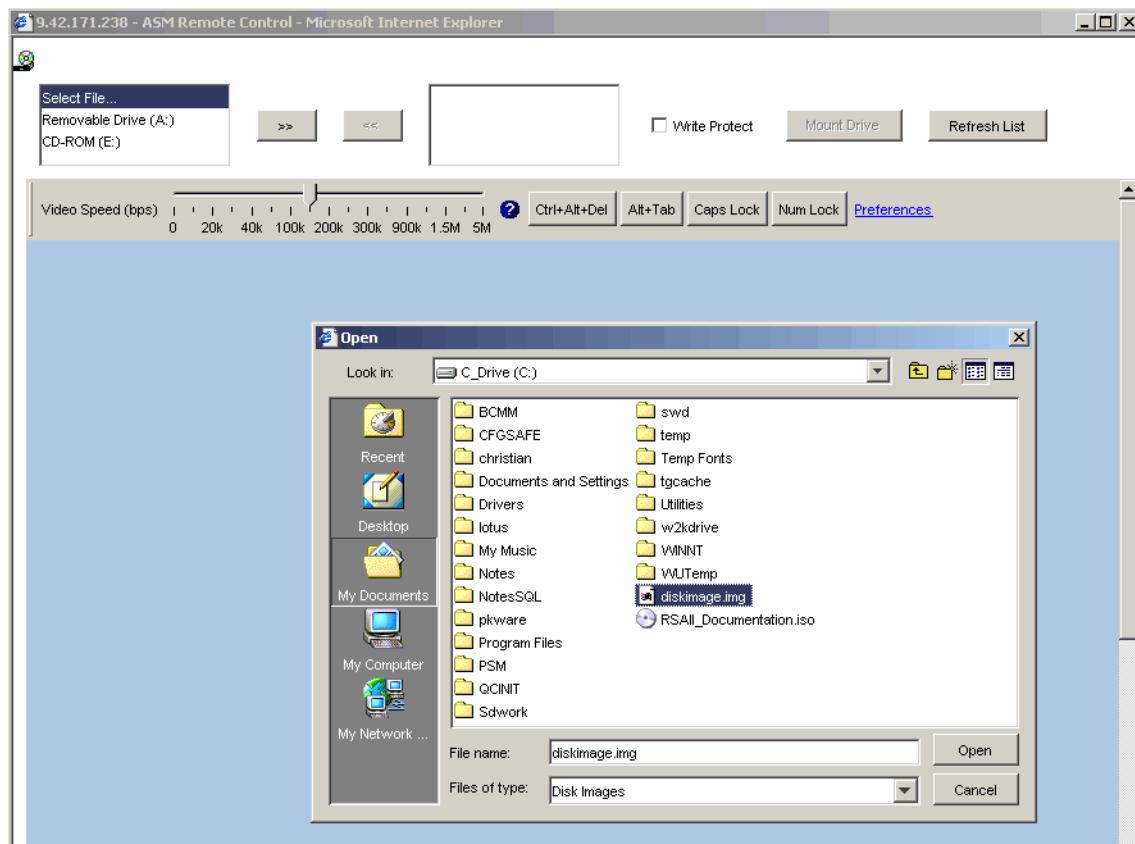


Figure 3-24 RSA II remote media - File

2. Once you have selected the diskette image to use, click **Open**. You are prompted as follows.



Figure 3-25 RSA II - Upload remote file

If you click **Yes**, the file is uploaded to the RAM of the RSA II adapter on the server. To upload the image it must not be bigger than 1.44 MB. This may take some time depending on the network connection. A progress indicator appears showing you how long the upload process will take.



Figure 3-26 RSA II - Remote Disk On Card

Tip: The image will remain accessible to the server until you unmount it using the **Unmount** button, the RSA II is restarted, or the firmware is updated.

If you click **No**, you additionally have to click **Mount Drive** to mount the drive to the remote server. The file is not uploaded, and is accessed remotely from your local PC via the network. Subsequent file access from this remote file will be at network speed. It is automatically unmounted when you close the remote console window.

Windows-specific steps

If the server is running Windows, the diskette image file is now available as a drive letter to the operating system. Check in the Windows Explorer for the new drive.

To unmount, launch the remote media Web interface, and complete the steps beginning with step 9 on page 76.

Linux-specific steps

If the server is running Linux, you now need to mount the drive in the operating system.

SUSE

Before and after pressing the **Mount Drive** button check the file /etc/fstab for the new device.

/dev/sda2	/	reiserfs	defaults	1 1
/dev/sda1	swap	swap	pri=42	0 0
devpts	/dev/pts	devpts	mode=0620,gid=5	0 0
proc	/proc	proc	defaults	0 0
usbdevfs	/proc/bus/usb	usbdevfs	noauto	0 0
/dev/cdrom	/media/cdrom	auto	ro,noauto,user,exec	0 0
/dev/fd0	/media/floppy	auto	noauto,user,sync	0 0
/dev/sdb	/media/sdb	auto	noauto,user,exec	0 0 #HOTPLUG
B3Fu.c+j0WmpZdK6				

Figure 3-27 File /etc/fstab and the remote file

In the last line you can see the device for the remote file. Mount it with the following command:

```
mount /dev/sdb /media/usb floppy
```

To unmount, follow the steps beginning with step 9 on page 76.

Red Hat

When using Red Hat Linux, the remote diskette is not listed in the file /etc/fstab. As a result, you will have to try sda, sdb, sdc, etc. until you successfully connect to the remote device.

In Figure 3-21 on page 80, we used the **mount** command and tried /dev/sda first, then /dev/sdb second.

Start with the following command to mount the remote diskette:

```
mount /dev/sda /mnt/floppy
```

If it does not work and you get the error message **mount: you must specify the file system**, the device name is /dev/sdb. Type **mount /dev/sdb /mnt/floppy** now to mount the drive.

To unmount, launch the remote media Web interface, and complete the steps beginning with step 9 on page 76.

3.6 Ports used by Remote Supervisor Adapter II

The RSA II is using several tcp/udp ports for communication. If the communication with the RSA II passes firewalls, it is important to know which ports you have to enable on the firewalls to communicate with the RSA. Below you will find a table with the default ports. Remember when you change the ports in the RSA you have to change them in the firewalls too.

Table 3-4 User configurable TCP/IP ports used by the RSA II

Port name	Port number	Description
http	80 (default)	Web server HTTP connection - TCP
https	443 (default)	SSL connection -TCP
telnet	23 (default)	Telnet command-line interface connection -TCP
SSH	22 (default)	Secure Shell (SSH) command-line interface - TCP
SNMP Agent	161 (default)	SNMP get/set commands - UDP
SNMP Traps	162 (default)	SNMP traps - UDP

Some other ports are fixed and cannot be changed.

Table 3-5 Fixed TCP/IP ports used by the RSA II

Port number	Description
427	SLP connection - UDP
1044	Remote disk function - TCP
1045	Persistent remote disk (disk on card) - TCP
2000	Remote Console video redirect - TCP
6090	IBM Director commands - TCP
7070-7074	Partition management - TCP



BladeCenter management module

The BladeCenter management module has similar capabilities to the RSA II, which is discussed in Chapter 3, “Remote Supervisor Adapter II” on page 47. There are some additional BladeCenter-specific features such as the integrated KVM switch.

The BladeCenter management module acts like a global RSA II for all the installed blade servers in the chassis. In this chapter we describe the differences between and similarities of the BladeCenter management module and the RSA II and some management module-specific issues.

This chapter contains:

- ▶ 4.1, “Features and functions” on page 88
- ▶ 4.2, “Basic configuration of the management module” on page 91
- ▶ 4.3, “Redundant management modules” on page 97
- ▶ 4.4, “Remote console and remote media” on page 100
- ▶ 4.5, “Basic configuration of blade-specific features” on page 119
- ▶ 4.6, “Ports used by the management module” on page 126
- ▶ 4.7, “Resetting the management module back to factory defaults” on page 127

4.1 Features and functions

The management module manages the BladeCenter chassis itself with all its networking modules (for example, Gigabit Ethernet or SAN) and all blade servers installed in the chassis.

The management module has an integrated KVM switch and an integrated network switch for internal IP connections to all the modules such as Ethernet switch modules (ESMs), Fibre Channel switch modules, etc. to manage the blade servers. Additionally, it acts like a RSA II for every installed blade server.

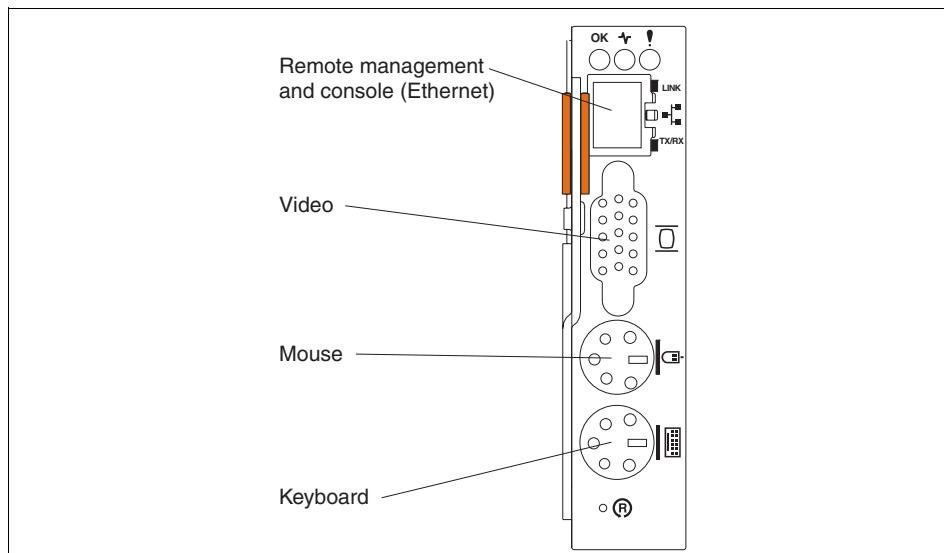


Figure 4-1 *BladeCenter Management Module connectors*

Like the RSA II, the management module communicates with the service processor integrated into every blade server.

Note: The BladeCenter Management Module does not support the ASM interconnect network.

The BladeCenter management module is supported in a BladeCenter or BladeCenter T. The BladeCenter T is a special chassis that is Network Equipment Building Standard (NEBS) compliant, especially for the telecommunication industry, and fits in racks that are shallower in depth than the standard server racks. Most of the blade servers and BladeCenter options are

supported in both BladeCenter chassis. Check the IBM ServerProven Web site for details:

<http://www.pc.ibm.com/us/compat/>

Table 4-1 is an overview of the features of the management module, broken down into subheadings monitoring, blade server tasks, I/O module tasks, and management module control. It shows the required user authority you need to execute these features.

Table 4-1 Features and required authority of BladeCenter management module

		Authority required to change information or execute tasks								
		Supervisor	Blade server Remote Console Access	Blade server remote console and remote media access	Blade and I/O module Power/Restart Access	Ability to clear event logs	Basic configuration (MM, I/O modules, blades)	Network and security configuration	Advanced configuration (MM, I/O modules, blades)	User account management
Window										
Monitors										
System Status	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Event Log (view)	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Event Log (clear)	✓				✓					
LEDs	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Hardware VPD	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Firmware VPD	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Blade tasks										
Power/restart	✓				✓					
On demand	✓				✓					
Remote control (remote console)	✓	✓	✓							
Remote control (remote media)	✓			✓						
Firmware update	✓							✓		

	Authority required to change information or execute tasks							
	Supervisor	Blade server Remote Console Access	Blade server remote console and remote media access	Blade and I/O module Power/Restart Access	Ability to clear event logs	Basic configuration (MM, I/O modules, blades)	Network and security configuration	Advanced configuration (MM, I/O modules, blades)
Window								
Configuration	✓					✓		✓
Serial over LAN	✓					✓	✓	
I/O module tasks								
Power/restart	✓			✓				
Management	✓					✓	✓	
Firmware update	✓						✓	
Management module control								
General settings	✓					✓		✓
Login profiles	✓						✓	✓
Alerts	✓				✓		✓	
Port assignments	✓					✓	✓	
Network interfaces	✓					✓	✓	
Network protocols	✓					✓	✓	
Security	✓					✓	✓	
Configuration file	✓						✓	
Firmware update	✓						✓	
Restore defaults	✓						✓	
Restart MM	✓						✓	

4.2 Basic configuration of the management module

To use the functionality of the management module, you first have to configure it. In this section, we describe the basic configuration steps. For more information, refer to 7.3, “Provide remote access to all BladeCenter modules” on page 239, and the product publication *BladeCenter Management Module User’s Guide*.

4.2.1 Installation in a BladeCenter

When you install a BladeCenter it comes with one management module preinstalled in the upper management module bay (bay 1). The BladeCenter also supports a second redundant management module, which can be installed in bay 2, as shown in Figure 4-2.

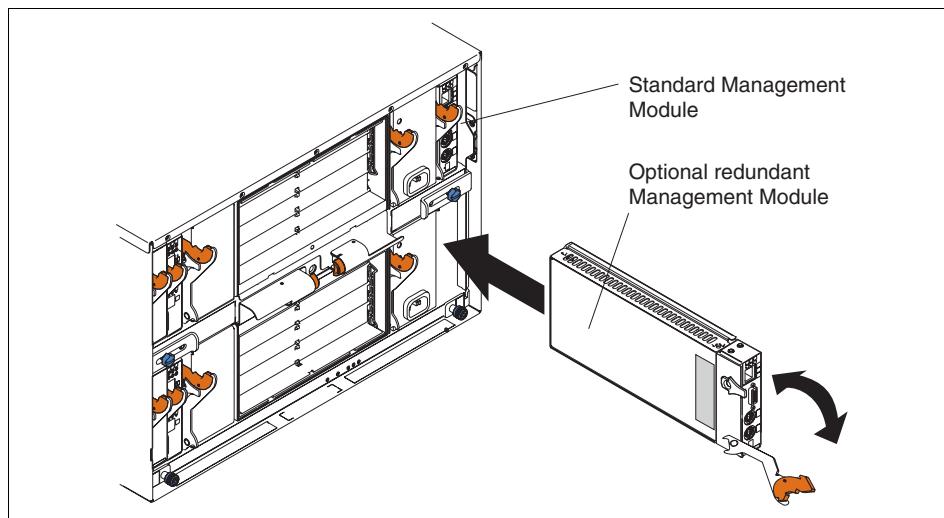


Figure 4-2 Installation of a redundant management module

We discuss the use of the redundant management module in 4.3, “Redundant management modules” on page 97.

Note: All modules with an orange release latch are hot swappable. You do not have to power down the BladeCenter. Before you replace a module, take care because it could have active connections to running servers and applications.

4.2.2 Network settings

The management module will automatically attempt to set its IP address as follows:

1. The management module searches for an active DHCP server to receive an IP address with subnet mask and default gateway.
2. If there is no response from a DHCP server within two minutes, the management module will use the default IP address 192.168.70.125 with subnet mask 255.255.255.0. The host name will be MMxxxxxx, where xxxxxxxx is the MAC address of the management module. The MAC address is printed on a label in the lowest position, as shown in Figure 4-3.

If the subnet of the BladeCenter has an active DHCP server or a DHCP relay agent, check the DHCP servers' leases for the MAC address of the management module.

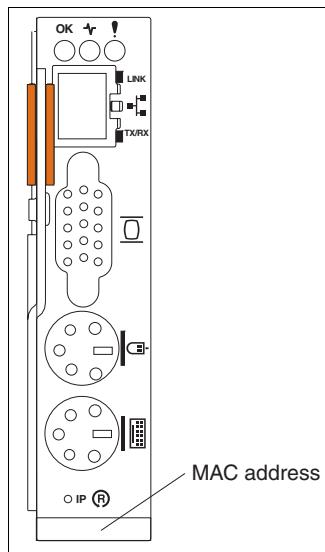


Figure 4-3 MAC address of BladeCenter management module

Tip: We recommend that you use static IP addresses for all xSeries systems management hardware to get access to the devices even if there are problems with the DHCP server.

We recommend that you use a static address. However, to change it from dynamic to static, you need to connect to the management module to change the setting. There are two ways to obtain the dynamically assigned address:

- ▶ Obtain the address from the DHCP server:

Check your DHCP server using the MAC address of the management module and obtain the dynamic IP address that was assigned to it. Use any PC with an Ethernet connection to the same LAN as the management module and launch the Web browser with the IP address of the management module.

- ▶ Without DHCP

If you do not have a DHCP server or the first method is unavailable to you, disconnect the management module from the Ethernet network and power on the BladeCenter. This will force the management module to take the default address of 192.168.70.125. Use a cross-over Ethernet cable to connect the management module to a standalone PC or notebook. This PC must have an IP address in the 192.168.70.0/24 subnet.

The PC needs a supported browser and Java 1.4 installed. Refer to 6.5, “Web interface” on page 219, for detailed specifications.

Tip: Do not use one of the IP addresses below for your PC or notebook when you connect it with a cross-over Ethernet cable to the management module, because these are the pre-defined IP addresses of the BladeCenter.

- ▶ 192.168.70.125 - Management module external port
- ▶ 192.168.70.126 - Management module internal port
- ▶ 192.168.70.127 - Module bay 1 internal port
- ▶ 192.168.70.128 - Module bay 2 internal port
- ▶ 192.168.70.129 - Module bay 3 internal port
- ▶ 192.168.70.130 - Module bay 4 internal port

Use the browser on your connected PC and launch the Web interface of management module to do the basic network configuration:

1. Log on with standard user USERID and PASSW0RD (with a zero, not the letter O) as password.

Tip: For security reasons you should plan to change the standard password as soon as possible.

2. When the Web interface starts, click **Continue**. It is not necessary to change the time-out value now, but you can if you want.

3. Click **MM Control** to expand the submenus, then **Network Interfaces** in the left-hand navigation frame.
4. Select **Disabled - Use static IP configuration** from the DHCP pull-down in the section External Network Interface (eth0).
5. Insert the host name for the management module.
6. Fill in the IP address you want to assign to the management module, the network's subnet mask, and the standard gateway. Contact your network administrator for these details.
7. Scroll down and click **Save**.
8. Click **OK** on the dialog explaining that the changes only take effect when you restart the management module.
9. Click **Restart MM** in the MM Control menu of the navigation frame.
10. In the Restart MM section click **Restart**.
11. Click **OK** to restart the management module.
12. A browser window with the message of the reset of the management module pops up. Shortly after this click **Yes** in the window to close the browser.

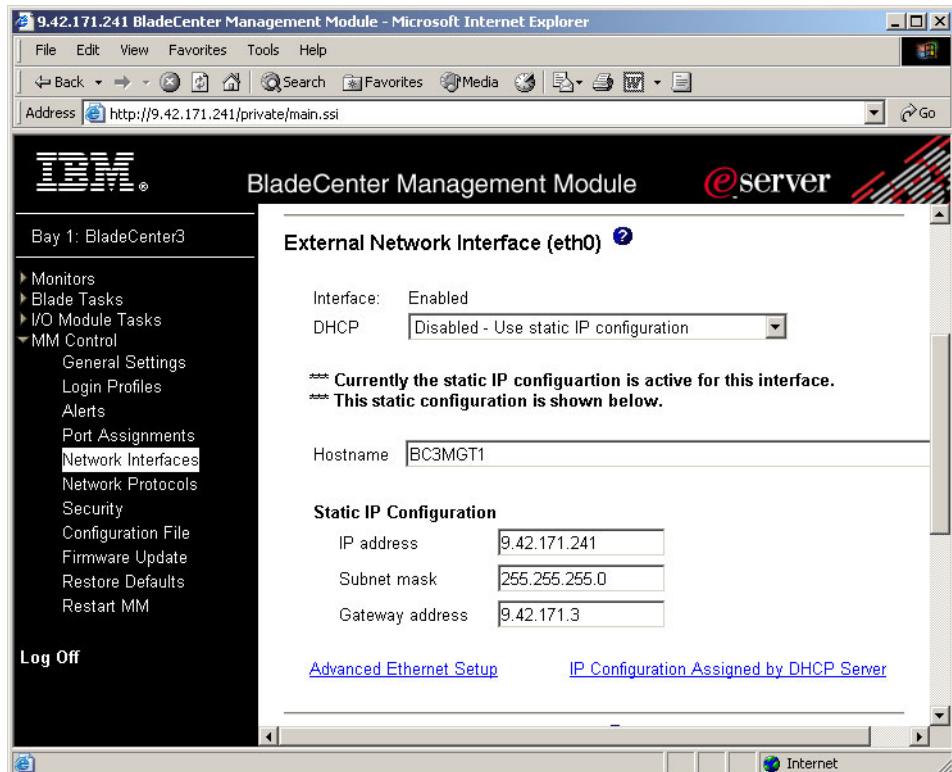


Figure 4-4 Network interfaces

The restart of the management module takes a minute. This is the right time to connect the management module to your Ethernet network if you used a cross-over Ethernet cable connected to a standalone PC.

Tip: To check the network connection of the management module, use the **ping** command from another system connected to the network.

4.2.3 Update firmware

The next step is to update the firmware of the management module to the most recent version. You can download it from one of the following URLs:

- ▶ BladeCenter: <http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
- ▶ BladeCenter T: <http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>

After extracting the file take a few minutes to read the **readme.txt**. The following files should be in your directory.

Name	Size	Type	Modified
26r0697.zip	1,796 KB	PKZIP File	10/28/2004 6:35 PM
cnetbrus.pkt	65 KB	PKT File	9/30/2004 12:27 PM
cnetmnus.pkt	1,678 KB	PKT File	9/30/2004 12:50 PM
cnetrgus.pkt	68 KB	PKT File	9/30/2004 12:27 PM
mmalert.mib	37 KB	MIB File	9/30/2004 12:20 PM
mmblade.mib	488 KB	MIB File	9/30/2004 12:22 PM
readme.txt	12 KB	Text Document	9/30/2004 1:25 PM

Figure 4-5 Files of firmware update package

Note: To update the firmware of the BladeCenter management module you can also use the management processor command line interface (MPCLI). See 7.8.1, “Using MPCLI to upgrade firmware” on page 257, for details.

Do the following steps to update the firmware and restart the management module using the Web interface:

1. In the navigation frame, click **Tasks → Firmware Update**.

Update MM Firmware ?

To update a firmware component on the MM, select a firmware file and click "Update". If there is a redundant MM installed, the firmware on the redundant MM will be automatically updated to the same level.

Note: To ensure proper operation of the management module, make sure you update all MM firmware components to the same level.

Figure 4-6 Firmware Update of BladeCenter Management Module

2. Click **Browse** to select the first of three files for firmware update.
3. To update click **Update**. The file is now transferred to the management module.
4. When file transfer is finished click **Continue** to begin the flash process.
5. Repeat these steps for the remaining two files.
6. Restart the adapter by clicking **ASM Control → ASM Restart** when finished.

Now you can use or configure other options of the management module. Some of these are discussed in the remainder of this chapter.

Tip: After basic configuration of the management module you should do the same for the installed switch modules. Refer to 4.5.3, “I/O Module tasks” on page 124, for details.

4.2.4 MIB files

The management module supports SNMP from many management tools including IBM Director. If you require MIB files, these can be found in the ZIP file for the management module firmware update:

- ▶ Management Module Firmware for BladeCenter
<http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
- ▶ Management Module Firmware for BladeCenter T
<http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>

4.3 Redundant management modules

The whole BladeCenter concept is based on complete redundancy. Even the management module can be redundant. If the primary and active module fails or if you initiate a switch over, the redundant management module will get the active one, and the former active will get the failed or redundant module.

4.3.1 Installation and cabling

After installation in the BladeCenter, all the configuration data of the primary module is automatically transferred to the redundant module. If you change configuration data, the primary module transfers the changes automatically to the redundant module.

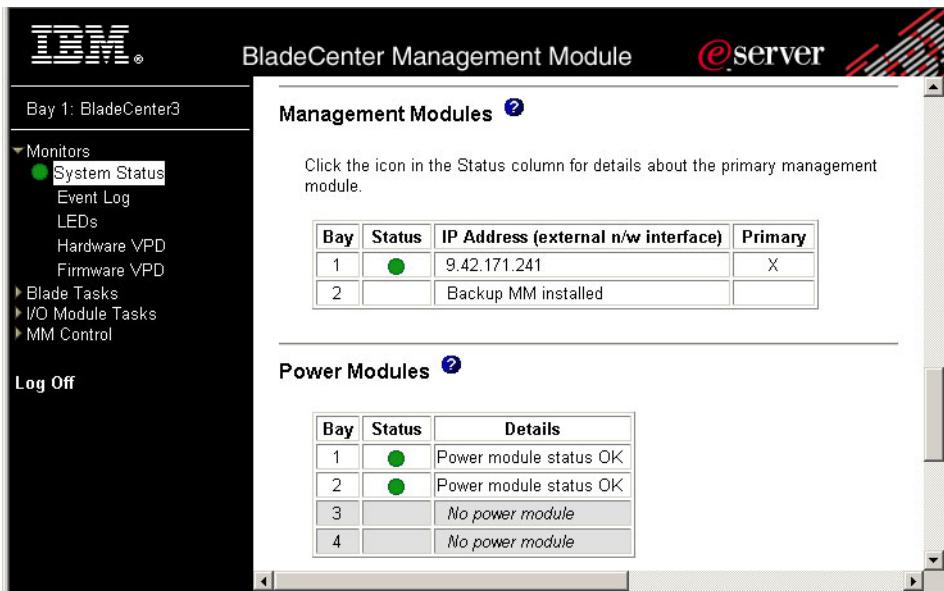


Figure 4-7 Redundant management module

Firmware updates

When you update the firmware of the primary management module, the updated files are automatically transferred to the redundant management module. To activate the new firmware on the redundant module, it will have to be restarted.

You can restart the redundant module by manual switch over. Refer to 4.3.2, “Manual switch over” on page 99. This feature was added in firmware Version 1.15 (BRET73E).

Note: If the redundant management module has much older firmware than the primary module, then the transfer of the update may not be successful with the message:

Transfer of MM main application image from MM1 to MM2 failed: Could not write new firmware image to the device to be updated.

The work-around in this instance is to manually failover and then update the firmware.

Ethernet interface

Connect the Ethernet port of the redundant management module to your LAN. The IP settings of the primary module are available, but the Ethernet port is

disabled until a switch over occurs. You can reach the Web interface of the active management module shortly after the switch over with the same IP address.

KVM connections

You will need to connect a mouse, keyboard, and monitor to the redundant management module. Connect the KVM ports ether with a console switch or a dedicated keyboard, monitor, and mouse. When the redundant module becomes the primary module, you have to use its KVM connection.

4.3.2 Manual switch over

When you implement a failover solution you should test it to be sure that it works in case of a failure. To test the switch over of the management modules of the BladeCenter, launch the Web interface and log on.

1. On the navigator bar click **MM Control**.
2. Click **Restart MM**.
3. Click **Switch Over**.
4. Click **OK**.

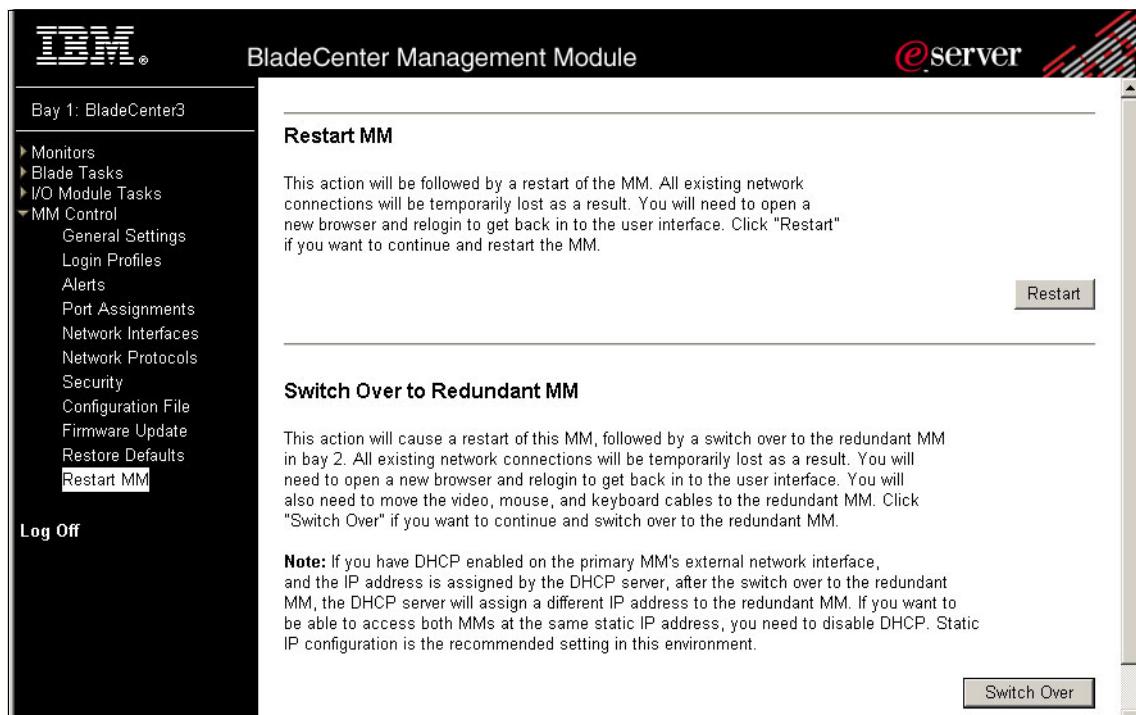


Figure 4-8 Switch over to redundant management module

The redundant management module will become the primary. The previous active module reboots and is then the redundant module. Until the redundant module is active there is no management module to manage the BladeCenter. So the fans will both work at 100 percent, and the orange error LED is turned on. After the process completes and the management modules have finished changing their roles, the status of the BladeCenter is healthy again.

4.4 Remote console and remote media

The features remote console and remote media work very similar to the RSA II. You will find additional functions regarding the blade servers and the media tray of the BladeCenter.

Using remote media requires USB support from the operating system while the OS is up and running or during installation of OS. Remote media works with the following operating systems:

- ▶ Windows Server 2003
- ▶ Windows 2000 Server with Service Pack 4 or later
- ▶ Red Hat Enterprise Linux AS 3, but not for OS installation
- ▶ SUSE LINUX Enterprise Server 8, but not for OS installation

A Java runtime is required, which can be installed by going to:

<http://www.java.com/en/download/manual.jsp>

Restriction: Remote media is not supported during the installation of Red Hat and SUSE LINUX because the installers have problems recognizing or mounting/unmounting the remote CD-ROM. This is due to be corrected in future versions of the Linux distributions.

To launch a remote console, open the Web interface, log on, and click **Blade Tasks → Remote Control** in the navigation frame.

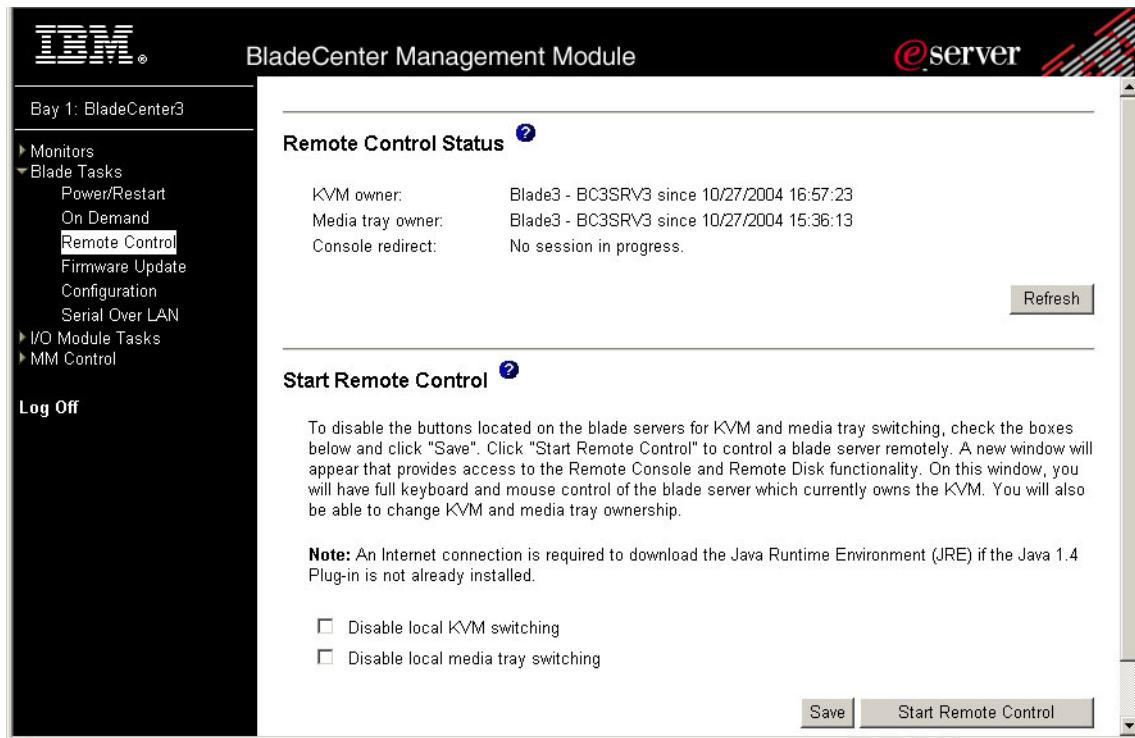


Figure 4-9 Launch remote control

In the Remote Console Status section, you can see which blade server is the KVM owner and which is the media tray (CD/DVD-ROM and diskette drive) owner. In the Start Remote Control section, you can choose to disable local manual switching of KVM and media tray at the blade servers.

Tip: If you do not disable local switching of the KVM and the media tray using the above options, you risk the possibility that someone else may switch the KVM or media tray at the BladeCenter to another blade server during your product installation. If this happens, your installation will fail.

Click **Start Remote Control** to launch the remote control window. You may see a security warning window pop up. This warning comes from Java applets remote control uses. It is normal to see these warnings, and you can trust this certificate from IBM and click **Yes**.



Figure 4-10 Security warning

For more details on this warning click **More Details**, or to continue click **Yes**.

Tip: This window will pop up every time you enter remote control unless you click **Always**.

Once loaded, you see the console of the blade server that currently owns the KVM.

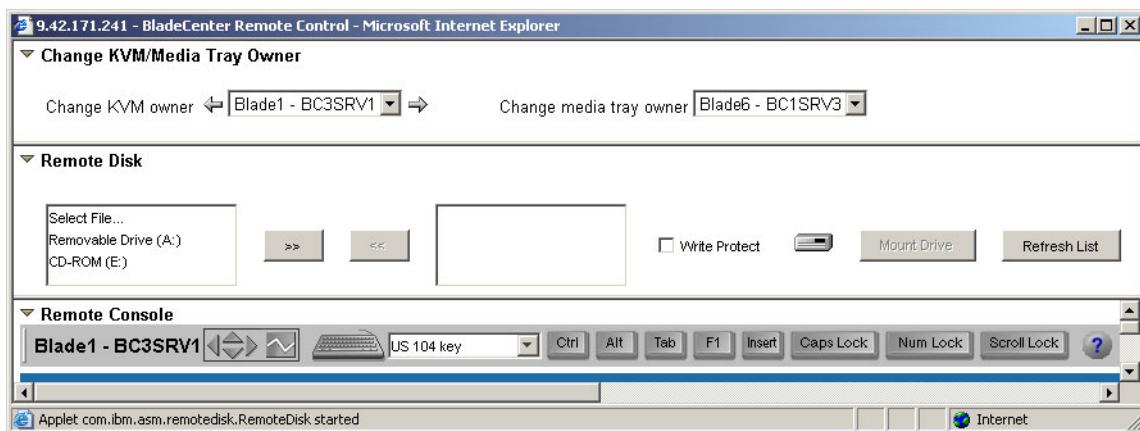


Figure 4-11 Remote control of BladeCenter

In the remote control window, Figure 4-11 on page 102, there are three control panels above the remote console.

- ▶ The Change KVM/Media Tray Owner panel lets you select which of the blade servers to control remotely. The blade server that owns the KVM is the one you can control remotely. You can also specify here which blade server is to own the media tray (both diskette and CD/DVD-ROM drive).
- ▶ The Remote Disk panel is where you enable the use of a disk on your local PC or notebook remotely to the blade server.
- ▶ The Remote Console panel provides the following functions:
 - The screen alignment control  specifies where the video should be displayed in the applet window. Due to video display variations, the video for each blade server may be aligned slightly differently. Use the screen alignment control to align the upper left corner of the video in the upper left corner of the applet video display area. Accurate mouse operation requires proper video alignment.
 - The phase calibration button  forces automatic calibration of the analog video on the remote server. This button should be pressed if you notice fuzzy or corrupted video. While phase calibration is being performed, remote updates are not sent. The remote user should insure that the server display is static while the phase adjustment is active.
 - The keyboard selector  allows you to specify the keyboard type that should be emulated.

The key icons are used to send keystrokes directly to the remote server. To send Alt or Ctrl key combinations, click the Alt and/or Ctrl key icon before pressing another key. For instance, to send the Ctrl-Alt-Del key combination, click , click , then click the Delete key on your keyboard. When you press Delete, all three keystrokes are sent to the server. When you click the Alt or Ctrl icon and make it active, it remains active until you press a keyboard key or until you click the icon again. To send any of the other keys shown, use the icons in place of the keyboard keys. Use the Caps Lock, Num Lock, and Scroll Lock icons instead of the lock keys on your computer.

Tip: To see a larger part of the remote console of the remote server you can collapse these three panels by clicking the small triangle in front of each heading.

4.4.1 Linux support for remote control

When using the remote control feature with a Linux distribution, there are some additional configuration steps needed in the operating systems to make the remote mouse and keyboard work.

1. To provide the correct resolution information to the mouse handler if your resolution is not 1024 x 768, do the following:
 - a. Type `init 3` at the Linux command prompt.
 - b. Unload the mouse driver module. Type `rmmmod mousedev` to do this.
 - c. Add the following statement to the file `/etc/modules.conf`:

```
options mousedev xres=X, yres=Y
```

Where *X* and *Y* specify the video resolution.
 - d. Reload the mouse driver module with the command `insmod mousedev`.
 - e. Change back to runlevel 5 by typing `init 5`.
2. To synchronize (to move in unison) the local and the remote mouse during remote control sessions, the settings for the graphical login screen (XDM) and for your preferred GUI (such as KDE or GNOME) must be changed.
 - For XDM do the following:
 - i. Change to run mode 3 by typing `init 3`.
 - ii. For SUSE LINUX, add the following line just before the `exit 0` line in the file `/etc/X11/xdm/Xsetup`:

```
$xset m 1 1
```
 - iii. For Red Hat, add the following line just before the `exit 0` line in the file `/etc/X11/xdm/Xsetup_0`:

```
xset m 1 1
```
 - iv. Save the file and change to runmode 5 by entering `init 5`.
 - For KDE, complete the following steps to set the mouse acceleration and threshold values if you are using the KDE:
 - i. Using the keyboard, press Alt+F1 or Ctrl+Esc to open the menu on the desktop.
 - ii. From the menu, click **Preferences → Peripherals → Mouse**.
 - iii. Select the **Advanced** tab and change the Pointer Acceleration and Threshold values to 1.
 - iv. Log out from this session and be sure to check the Save current setup check box in the Log out window.

The next time you log in, the remote and local mice are synchronized.

- For GNOME, complete the following steps to set the mouse acceleration and threshold values:
 - i. Using the keyboard, press Alt+F1 or Ctrl+Esc to open the menu on the desktop.
 - ii. From the menu, select **Programs** → **Settings** → **Session** → **Session Properties & Startup Programs** or **Extras** → **Preferences** → **Sessions** (depending on the Linux version).
 - iii. Select the **Startup Programs** tab; then select **Add** to open another window.
 - iv. On the command line, type `xset m 1 1` and click **OK** to save this command.
 - v. Click **Apply** and then click **OK** to exit this window. Log out from this session and be sure to check the Save current setup check box on the Log out window.

The next time you log in, the remote and local mouse are synchronized.

Tip: To synchronize the local and remote mouse pointer (bring the local and remote mouse arrows on top of each other) for the first time, move the pointer in one of the corners so that the local and remote mouse pointers are in the same position.

4.4.2 Using remote media

Before using remote media support, check the available bandwidth of the network connection. This works well in a 100 Mbps LAN environment. If you have a low bandwidth WAN connection, the performance may be unsatisfactory.

You can use remote media during the booting process or when the operating system is up and running (see the restrictions described in 4.4, “Remote console and remote media” on page 100). With this feature a complete installation of the server, including operating system and patches, from a remote location is possible.

Tip: In order to use both diskette drives (local and remote, because they are both USB devices) with Linux and not get confused when using one mount point for both, you should create a new mount point for remote diskette. Type `mkdir /media/usb floppy` at the SUSE Linux command line (`mkdir /mnt/usb floppy` for Red Hat).

The local devices in the media tray (diskette and CD-ROM) will create entries in the file `/etc/fstab` for SUSE LINUX and for Red Hat Linux.

The process of mounting remote media will take a little while. Wait until the media symbol in the remote media section of the Web interface stops flashing before you check the Windows Explorer or the /etc/fstab in Linux.

Important: Remote media with SUSE Linux Enterprise Server 8 works only if SUSE Service Pack 3 is installed.

To use remote media, do the following:

1. Open a browser window and access the Web interface.
2. Click **Blade Tasks** → **Remote Control**.
3. Click **Start Remote Control**.
4. At the remote console window, you can mount remote media to your server by choosing the type (file, diskette, or CD-ROM), clicking **>>**, then **Mount Drive**. Optionally, you can select write-protected.
5. If you are running Windows on your server, you should now be able to access the media as a drive letter. For Linux, you will need to mount the drive as described in:
 - 4.4.3, “Remote diskette” on page 108
 - 4.4.4, “Remote CD-ROM and DVD” on page 112
 - 4.4.5, “Remote file” on page 115

Tip: At this time it is not possible to have write access to remote media image files.

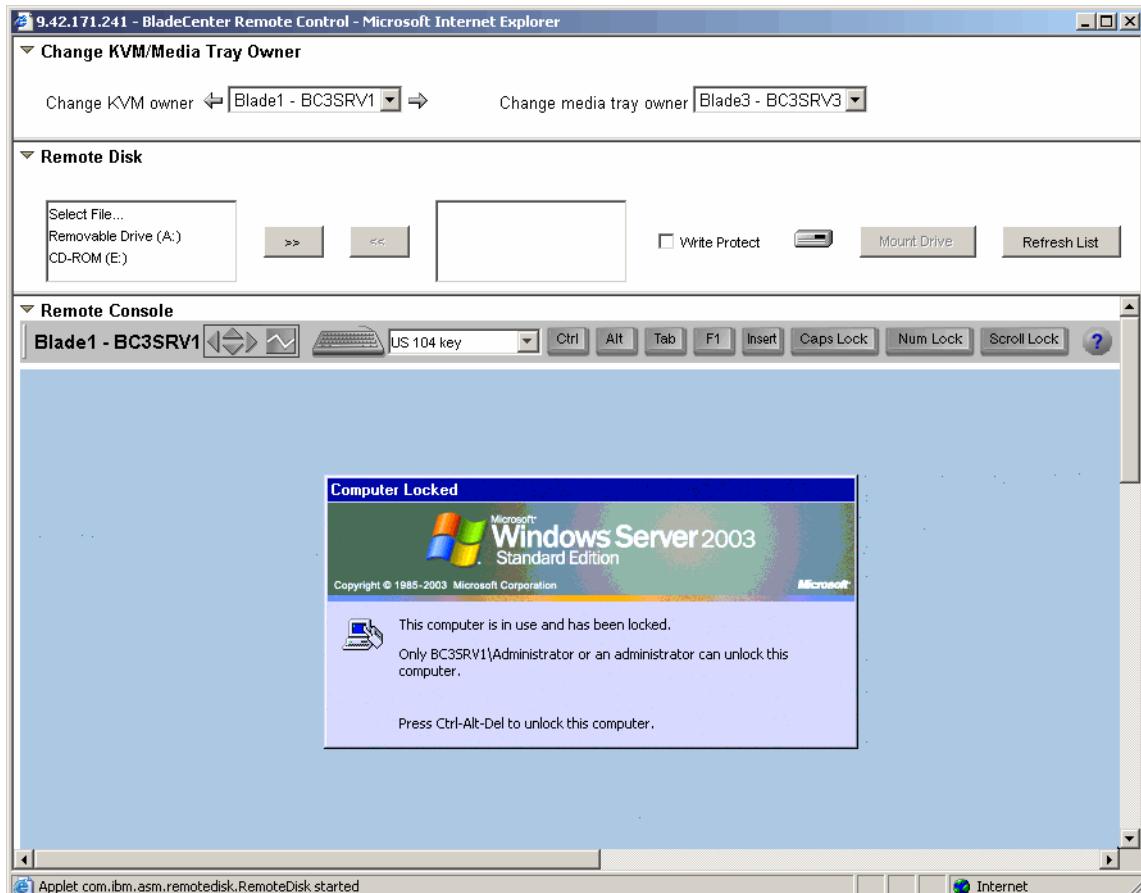


Figure 4-12 Remote console and remote media

6. To unmount remote media do the following:

For Windows:

- a. Double-click the Safely Remove Hardware icon in the task bar of your remote console.



Figure 4-13 Safely remove hardware icon in Windows task bar

- vi. In the open window click **USB Mass Storage Device** and **Stop**.
- b. Click **IBM Remote Disk USB device** and **OK**. A message will appear that it is now safe to remove the hardware.

- c. Click **Close** to close the window.

For Linux, unmount the remote drive with the **umount** command at operating system level. For example, if your mount command was **mount /dev/sdb /media/floppy**, then use **umount /media/floppy** now. Generally use the second parameter of the mount command (which represents the mount point) for unmounting.

7. Click **Unmount Drive** (the button mount drive changed to unmount drive during mount process), then << to remove it from the drives list.

4.4.3 Remote diskette

When you use a remote disk you can mount the local diskette drive to the blade server you are connected.

1. Choose **Removable Drive (A:)** and click **>>**.
2. When you are asked to upload the content of the diskette drive as an image to the management module, you have two options.

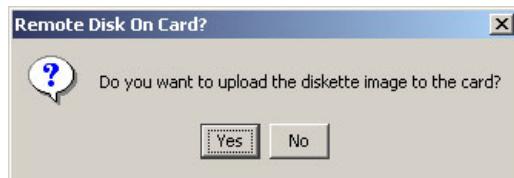


Figure 4-14 Upload remote diskette

If you click **Yes**, the management module loads the diskette image to its memory. A progress indicator appears. It is not necessary to click Mount Drive, because the mount works automatically when the diskette image is loaded to the memory of the management module. When completed, it is available as an additional drive in the operating system.



Figure 4-15 Remote Disk On Card

If you do not want to upload the diskette image file click **No**. To make it available in the operating system click **Mount Drive**.

When booting the server, and the management module contains a diskette image or a diskette or a diskette image is mounted while the remote media Web

interface is still open, the server will try to boot from it. If the media is bootable but it does not work, check the boot sequence in the BIOS.

Tip: If you use the upload option, unmount the drive if no longer needed, because on the next reboot the server will boot from the diskette image in the management module's memory if there is still one.

Windows-specific steps

In Windows operating systems you will probably find it as a new B drive.

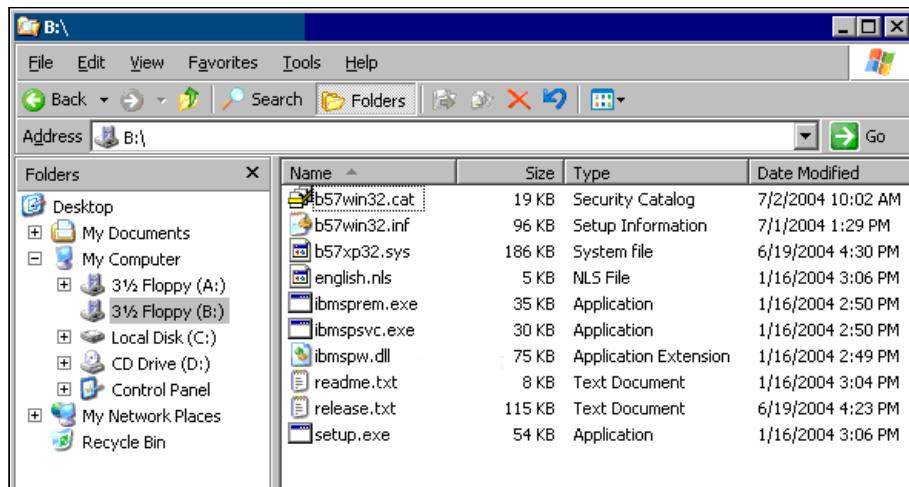


Figure 4-16 RSA II - Remote diskette on remote windows

To unmount, launch the remote media Web interface and follow step 6 on page 107.

Linux-specific steps

Unlike Windows, where the operating system automatically mounts the remote drives to a drive letter, remote media with Linux is a little additional manual work to do. After you click the **Mount Drive** button, the Linux operating system knows the device, but you have to mount the drive manually to get access to it.

SUSE LINUX

In SUSE LINUX the remote media and the local media tray (diskette and CD-ROM) create 'HOTPLUG' entries in the file /etc/fstab when connected. To mount them, check the /etc/fstab for the correct device names. The device /dev/cdrom is not used within SUSE LINUX on BladeCenter.

Tip: Check the file /etc/fstab before and after you click the **Mount Drive** button in the Web interface, to know which is the device is the remote media device.

In Figure 4-17 you can see the file /etc/fstab before the Mount Drive button was clicked. The devices of the media tray are /dev/sda (diskette) and /dev/sr0 (CD-ROM).

Note: The device /dev/cdrom is not used with SUSE LINUX and blade server.

/dev/hda2	/	reiserfs	defaults	1 1
/dev/hda1	/data1	auto	noauto,user	0 0
/dev/hdc1	/data2	auto	noauto,user	0 0
/dev/hdc2	/data3	auto	noauto,user	0 0
/dev/hdc5	/data4	auto	noauto,user	0 0
/dev/hdc6	/data5	auto	noauto,user	0 0
/dev/hdc7	/data6	auto	noauto,user	0 0
/dev/hda3	swap	swap	pri=42	0 0
/dev/hdc3	swap	swap	pri=42	0 0
devpts	/dev/pts	devpts	mode=0620,gid=5	0 0
proc	/proc	proc	defaults	0 0
usbdevfs	/proc/bus/usb	usbdevfs	noauto	0 0
/dev/cdrom	/media/cdrom	auto	ro,noauto,user,exec	0 0
/dev/sr0	/media/sr0	auto	ro,noauto,user,exec	0 0 #HOTPLUG B3Fu.dJ1EZns+fE6
/dev/sda	/media/sda	auto	noauto,user,exec	0 0 #HOTPLUG B3Fu.odWa+wJ1Pb2

Figure 4-17 SUSE LINUX - File /etc/fstab before remote drive

In Figure 4-18 on page 111 you can see that the remote diskette is recognized as new device /dev/sdb. Use the mount command shown in the figure below or use a meaningful name for a mount point, for example:

```
mount /dev/sdb /media/usb floppy
```

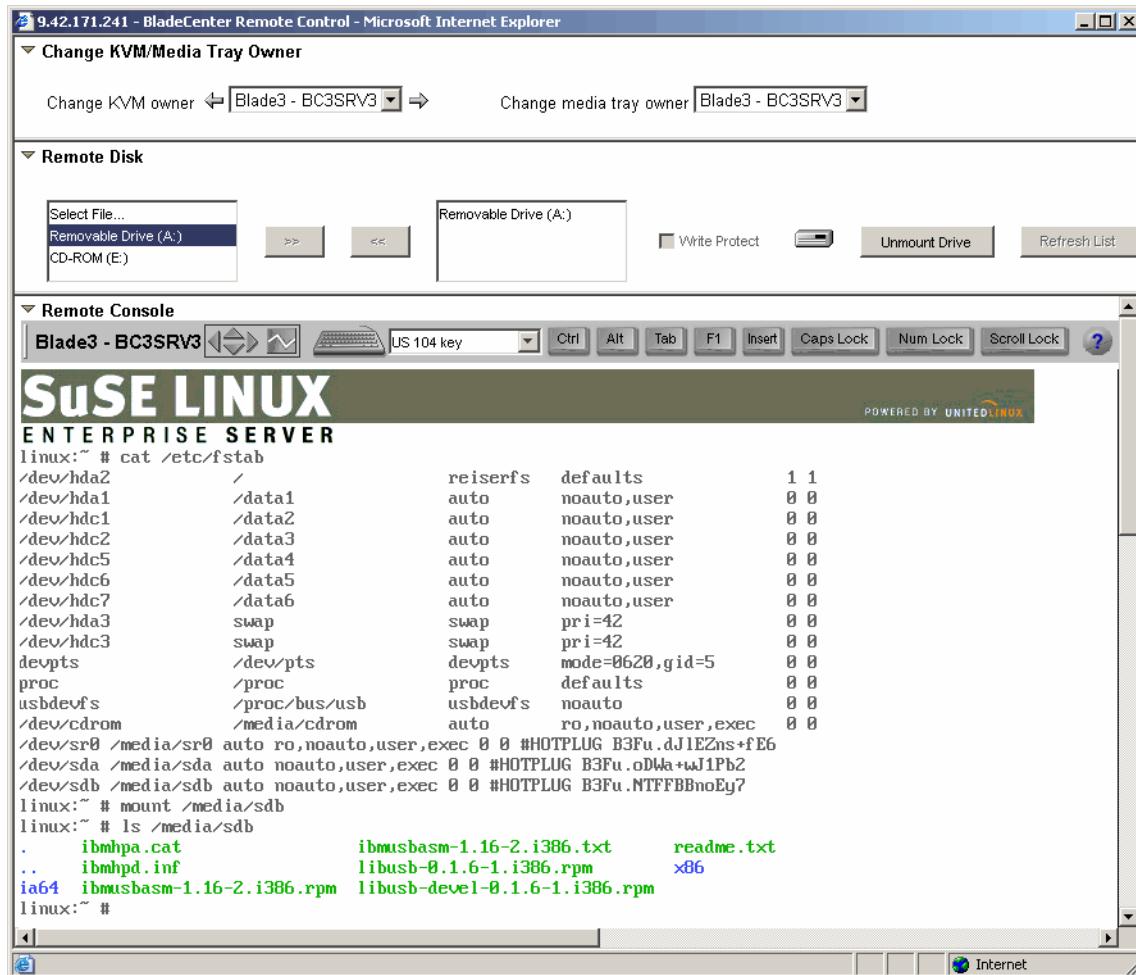


Figure 4-18 BladeCenter management module - Remote diskette in Linux

When you no longer need this drive, unmount it. Complete the steps starting with step 6 on page 107.

Red Hat Linux

When using Red Hat Linux there is no new entry in /etc/fstab for a remote diskette. The device name for the remote diskette depends on the media bay ownership and which device (remote diskette, remote file, or media bay) was used first after booting the server.

If you used a remote diskette or remote file first, then the device name will be /dev/sda. If the server had ownership of the media tray first, the device name for the remote diskette will be /dev/sdb.

As a result, you will have to try sda, sdb, sdc, etc. until you successfully connect to the remote device.

In Figure 4-19 we tried mount /dev/sda /mnt/usbfloppy first, then mount /dev/sdb /mnt/usbfloppy, which was successful.

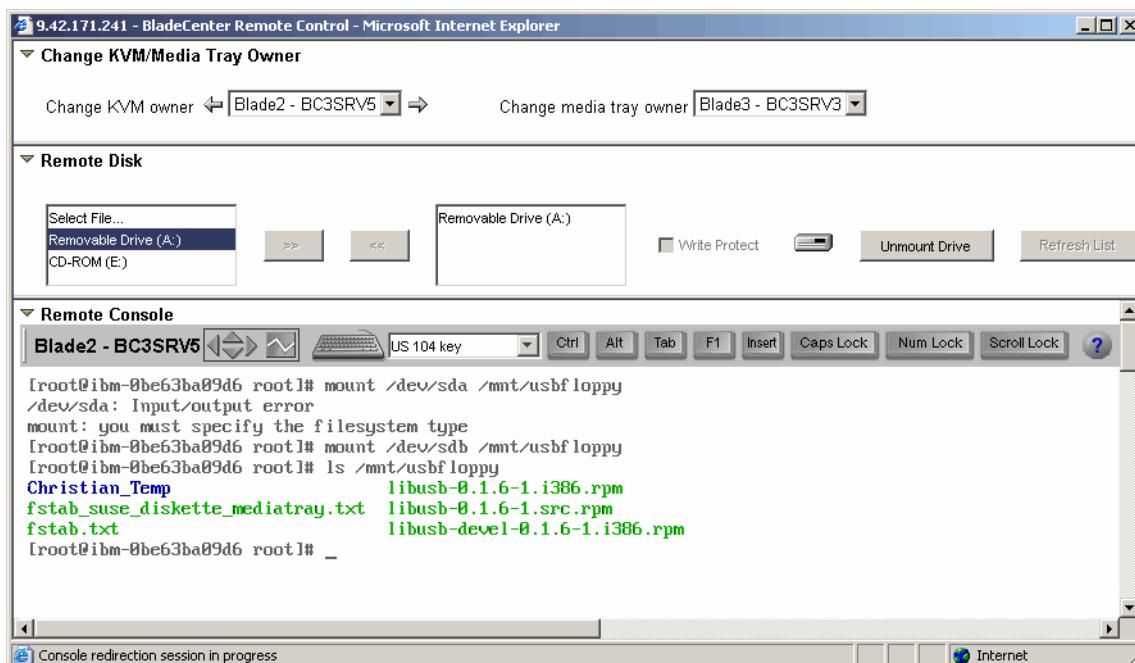


Figure 4-19 Using remote diskette with Red Hat Linux

To unmount the device, launch the remote media Web interface, and complete the steps beginning with step 6 on page 107.

4.4.4 Remote CD-ROM and DVD

Remote CD-ROM works very similar to remote disk. The only difference is that the management module will not load the content of the CD-ROM to its memory. It is possible to boot from a remote CD-ROM or use it as a drive letter within the operating system. The mount is only active while the remote media Web interface is open. If you close it, you automatically unmount the media. Remote CD-ROM works with a DVD drive and media as well.

To use a remote CD-ROM, complete the following steps:

1. Choose **CD-ROM({driveletter}:)** then click **>>**.
2. When clicking Mount Drive, the process of mounting the CD-ROM to the remote server starts. After a short time the remote CD-ROM is available to the operating system.

Windows-specific steps

In Windows the remote CD-ROM shows as a drive letter in the operating system. Here you see it as drive E:.

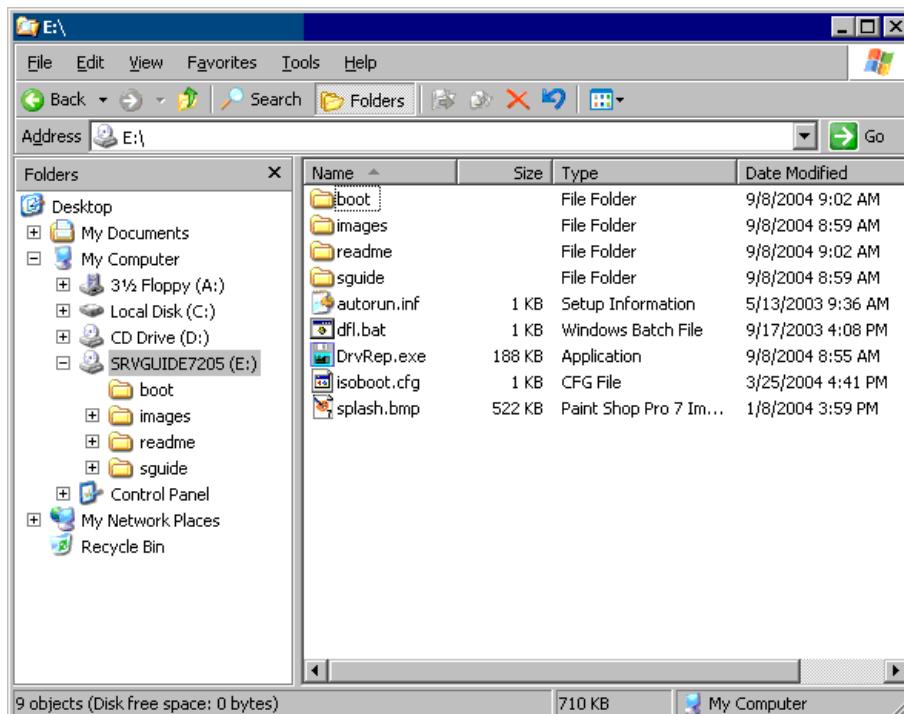


Figure 4-20 BladeCenter - Remote CD-ROM on remote Windows

To unmount, launch the remote media Web interface and follow step 6 on page 107.

Linux-specific steps

In Linux operating systems the remote media is not mounted automatically; you have to mount it. Remote CD-ROM will be shown in the file /etc/fstab for SUSE and for Red Hat.

SUSE LINUX

Check the /etc/fstab in the operating system before and after you click the Mount Drive button, to see which device is new in /etc/fstab. You will find a new "HOTPLUG" device.

In Figure 4-21 you see the device /dev/sr2, which is the remote CD-ROM in this case. Use the mount command as shown in the figure below as an example.

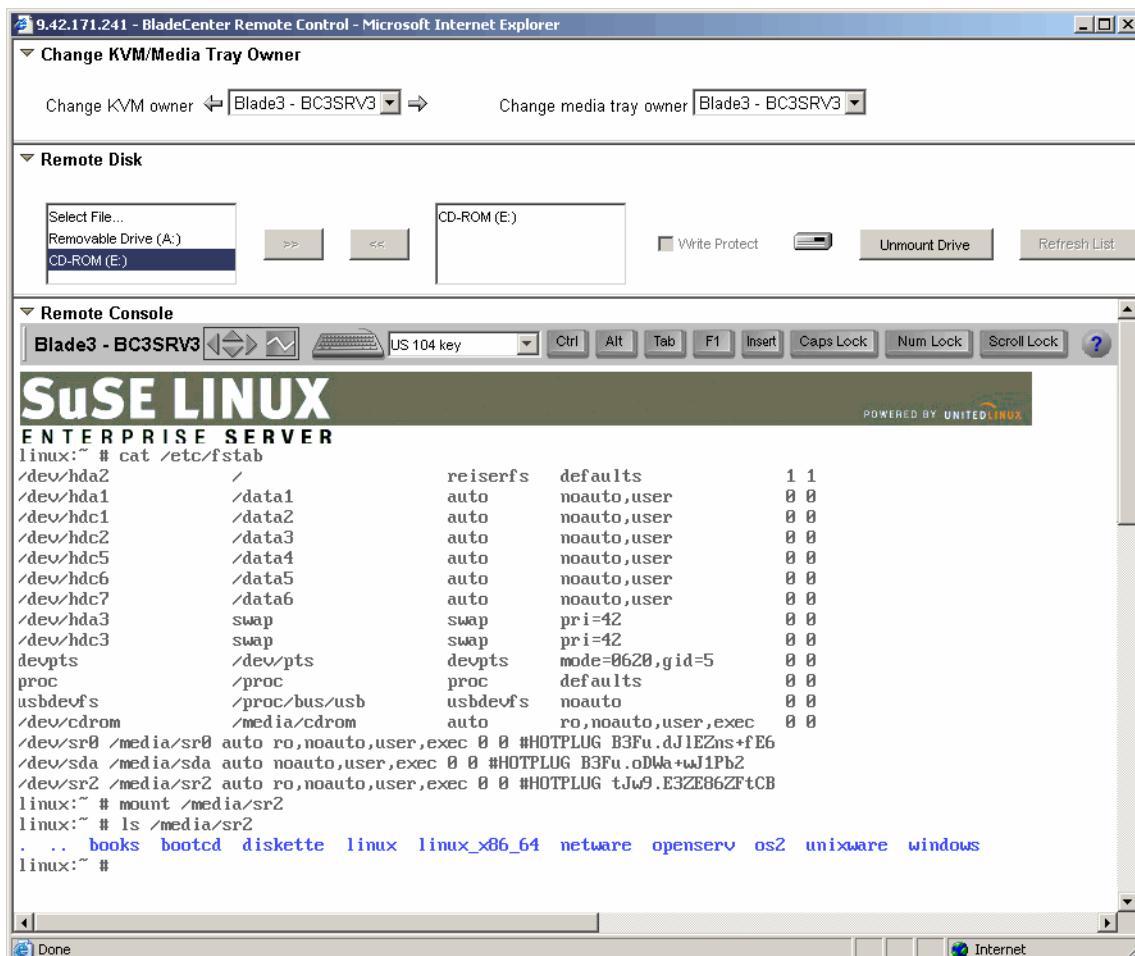


Figure 4-21 Remote CD-ROM with SUSE LINUX

After using remote diskette, unmount the remote media. To do this launch the remote media Web interface, and follow step 6 on page 107.

Red Hat

The remote CD-ROM is shown in the file /etc/fstab in Red Hat Linux, too. Check the file before and after clicking the **Mount Drive** button. The new device you will find is the remote CD-ROM. The following is an example of /etc/fstab.

LABEL=/	/	ext3	defaults	1 1
LABEL=/boot	/boot	ext3	defaults	1 2
none	/dev/pts	devpts	gid=5,mode=620	0 0
none	/proc	proc	defaults	0 0
none	/dev/shm	tmpfs	defaults	0 0
/dev/hda3	swap	swap	defaults	0 0
/dev/cdrom	/mnt/cdrom	udf,iso9660	noauto,owner,kudzu,ro	0 0
/dev/cdrom1	/mnt/cdrom1	udf,iso9660	noauto,owner,kudzu,ro	0 0
/dev/sda	/mnt/floppy	auto	noauto,owner,kudzu	0 0

Figure 4-22 Red Hat Linux - File /etc/fstab and the remote drive

The blade server became the owner of the media tray after clicking the Mount Drive button. This is the reason why the remote CD-ROM is the device /dev/cdrom and not /dev/cdrom1.

Mount the drive in your operating system:

```
mount /mnt/cdrom
```

To unmount, follow the steps beginning with step 6 on page 107.

4.4.5 Remote file

With the remote file feature you can use diskette and CD-ROM images as a drive to mount.

When you download ISO images from the Internet, you do not have to create a CD-ROM—you can use them directly as remote media.

Tip: You can create ISO images using tools such as IsoBuster (<http://www.smart-projects.net/isobuster/>) and Magic ISO maker (<http://www.magiciso.com/>). If you have a set of files that does not extend 1.44 MB, you alternatively can create a diskette disk image with one of these tools.

To mount a file do the following:

1. Select **Select File**.
2. Click >>.

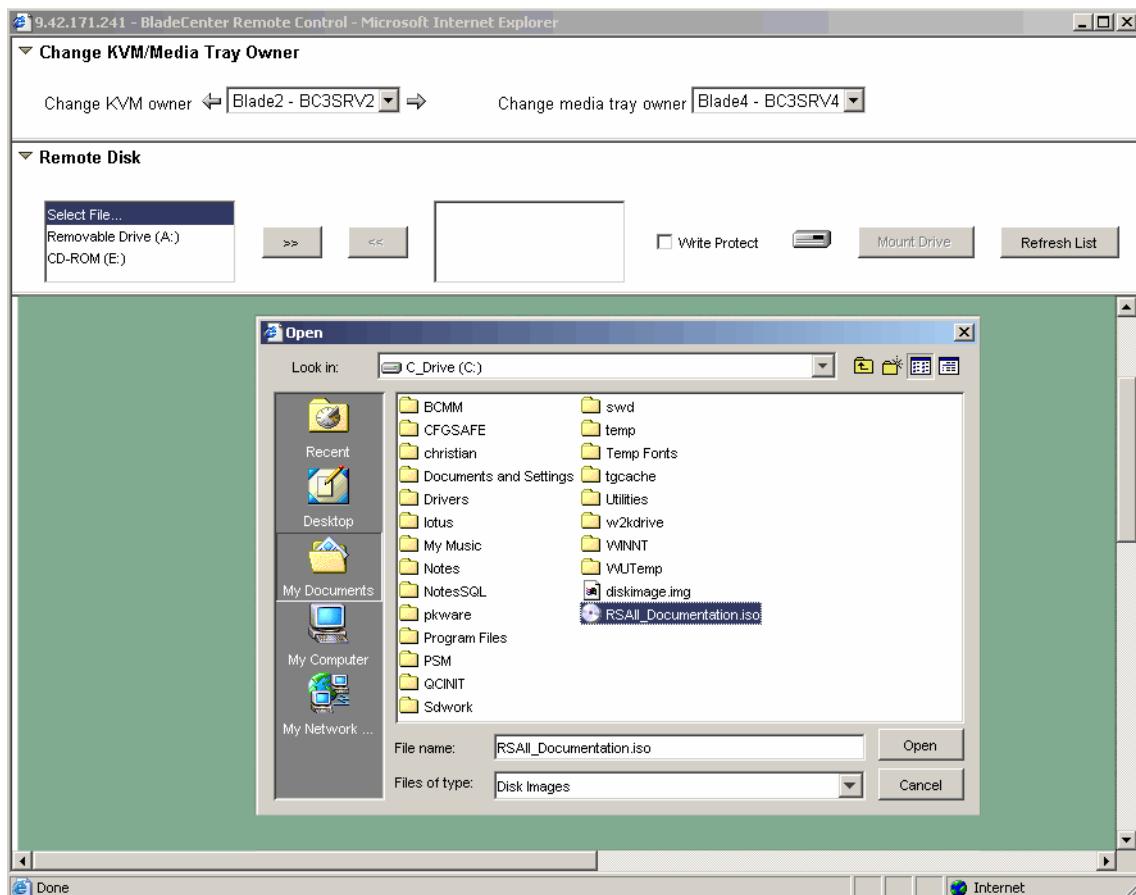


Figure 4-23 BladeCenter management module - Remote file

3. Choose the disk image file you want to use and click **Open**.
4. For diskette images (that is, not ISO files), you are prompted as shown in Figure 4-24.



Figure 4-24 BladeCenter - Upload remote file

If you click **Yes**, the file is uploaded to the RAM of the BladeCenter management module. To upload the image it must not be bigger than 1.44 MB. This may take some time depending on the network connection. A progress bar will appear.

Tip: The image will remain in the RAM and is accessible for the blade server, which is the KVM owner until you unmount it using the Unmount button. The management module is restarted or the firmware is updated. When you change the KVM owner, the new owner can use the remote disk image, too.

If you click **No**, you additionally have to click **Mount Drive** to mount the drive to the remote server. The file is not uploaded and is accessed remotely from your local PC via the network. Subsequent file access from this remote file will be at network speed. It is automatically unmounted when you close the remote console window.

5. If you have an ISO image, click the **Mount Drive** button.

Windows-specific steps

The image file is now available as a drive in the Windows operating system. Check in Windows Explorer for the new drive.

To unmount, launch the remote media Web interface, and complete the steps beginning with step 6 on page 107.

Linux-specific steps

The remote file features work similar to the remote diskette feature, except that you can use ISO image files too.

SUSE LINUX

Check the /etc/fstab file before and after you click the **Mount Drive** button to see which is the new device. In Figure 4-25 on page 118 the ISO image is device /dev/sr1.

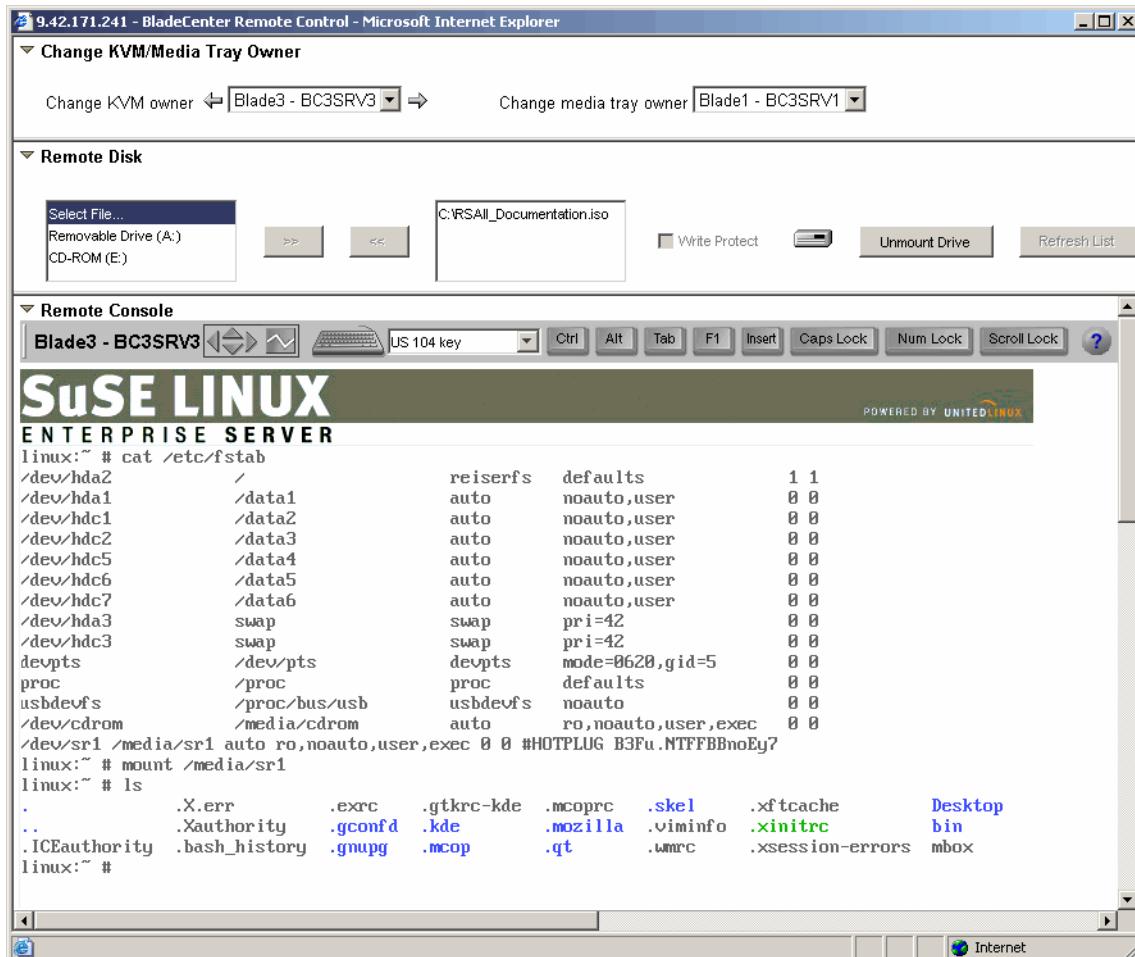


Figure 4-25 Remote file with SUSE LINUX

To unmount, follow the steps beginning with step 6 on page 107.

Red Hat

When using Red Hat Linux, the remote file is not mentioned in the file /etc/fstab. As a result, you will have to try sda, sdb, sdc, etc. until you successfully connect to the remote device.

In Figure 4-26 on page 119 the second try to mount the ISO image file was successful.

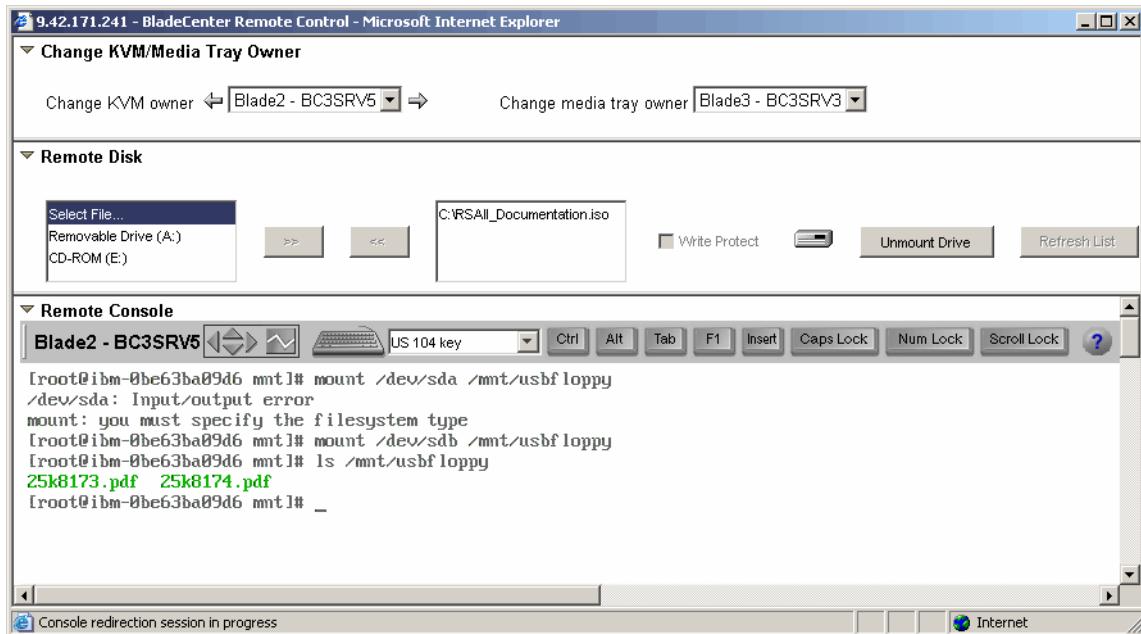


Figure 4-26 Remote file (ISO image) with Red Hat

To unmount, launch the remote media Web interface, and complete the steps beginning with step 6 on page 107.

4.5 Basic configuration of blade-specific features

In the following paragraphs we briefly describe the most common blade server-specific features. For a detailed description of the configuration refer to the following product publications, available from <http://www.pc.ibm.com/support>:

- ▶ *BladeCenter Management Module Installation Guide*
- ▶ *BladeCenter Management Module User's Guide*

4.5.1 Device drivers

The blade servers with BMC service processors (such as the HS20 8843) require IPMI drivers:

- ▶ IPMI device driver
- ▶ IPMI mapping layer (library) files
- ▶ IPMI ASR service

See 2.3.9, “Installing the BMC device drivers” on page 40, for information.

4.5.2 Blade tasks

The headings in this section are submenus of the Blade Tasks menu in the navigation frame. Click **Blade Tasks** to expand the menu then click the task you want to perform.

On Demand

This panel lets you enable any standby blade servers you have installed. Standby servers are part of the Standby Capacity on Demand offering, as described in:

http://www.ibm.com/servers/eserver/bladecenter/scod/more_info.html

On Demand Blade Activation

Click the checkboxes in the first column to select one or more On Demand blade servers that have a Standby status; then, click the 'Activate Standby Blade Servers' link below to activate the selected blade servers.

Note: You must contact IBM within 14 calendar days after you activate an On Demand blade server. See your Agreement for Standby Capacity on Demand for additional information.

Activating an On Demand blade server restarts the Blade System Management Processor on the blade server. It will take a few minutes for the status of the activated blade server to change from Standby to Active.

Select	Bay	Name	On Demand
	1	BC3SRV1	N/A
	2	BC3SRV2	N/A
	3	BC3SRV3	N/A
	4	BC3SRV4	N/A
	5	BC3SRV5	N/A
	6	BC1SRV3	N/A
	7	No blade present	
	8	No blade present	
	9	No blade present	
	10	No blade present	
	11	No blade present	
	12	No blade present	
	13	No blade present	
	14	No blade present	

[Activate Standby Blade Servers](#)

Figure 4-27 On Demand blade servers

In our example there are no on demand blades to activate.

The table on this page contains information about each blade server and shows the status (Active or Standby) of the on demand blade servers. A check box appears next to all standby servers that you check to activate.

Firmware update

Use this panel to update firmware components on a specific blade. Currently, the blade server's onboard system management processor is the only component

whose firmware can be updated on this page. You first need to download the latest firmware files from the IBM support Web site at <http://www.pc.ibm.com/support>. Then select a target blade using the Target pull-down and complete the following steps:

1. Click **Browse**. Find the firmware file in your computer's file system.
2. Click the desired file and then click **Open**. The file (including the full path) should appear in the box beside the Browse button.
3. To begin the update process, click **Update**. A progress indicator will be displayed as the file is transferred to temporary storage on the management module. Remain on this page until the transfer is complete. A confirmation page will be displayed when the file transfer is completed.
4. Verify that the type of file shown on the Confirm Firmware Update page is what you intended to update. If not, click **Cancel**.
5. To complete the update process, click **Continue**. A progress indicator will be displayed as the firmware update progresses. Remain on this page until the process is complete, at which point a status page will be displayed to indicate whether the update was successful. Additional instructions will be displayed on this page if necessary.

Configuration

On this page you can view and change some configuration parameters of blade servers.

Blade information

The blade information pane displays a table that shows the user-configured names for all the blades in the chassis. The table has one row per blade bay. The empty bays are marked as such. The blades that take up more than one bay are also indicated.

The blade names can be changed on this screen. To set the name for a blade, enter the desired name in the corresponding text box. You can enter a maximum of 15 alphanumeric characters. Click **Save** to save your changes.

Tip: The update of a blade name may take a while to take effect. If you do not see the name change reflected on the screen right away, wait a few moments and then refresh the screen.

Blade policy settings

In this section you can configure global policy settings for local control and Wake on LAN. The settings for local power control, local KVM control, local media

control, and Wake on LAN (WOL) apply to all blade bays including the empty bays.

Tip: To set policy settings for individual blade servers use the management module command line interface. Refer to *BladeCenter and BladeCenter T Management Module Command-Line Interface Reference Guide* for details.

When local power control is set to Enabled, the power buttons for all bays are enabled. When set to Disabled, the power buttons for all bays are disabled. The value of Not set indicates that no global policy has been set (some bays may have the power button enabled while others have it disabled).

Tip: You should set the local power control to disabled only during the installation process or if your BladeCenter is not installed in a secure area. If you set permanently local power control to disabled, the only way to power on or off the blade servers is to use the Web interface or the command-line interface of the management module.

Local KVM control works similar to local power control. When set to Enabled, the KVM Select buttons for all bays are enabled. When set to Disabled, the KVM Select buttons for all bays are disabled. The value of Not set indicates that no global policy has been set (some bays may have the KVM Select button enabled while others have it disabled).

In the local media tray control section you can control the access of the blade servers to the media tray (diskette, and CD-ROM/DVD-ROM, USB)

This field displays the global policy setting for local media tray switching for all blade bays. When set to Enabled, the Media Tray Select buttons for all bays are enabled. When set to Disabled, the Media Tray Select buttons for all bays are disabled. The value of Not set indicates that no global policy has been set (some bays may have the Media Tray Select button enabled while others have it disabled).

When Wake on LAN (WOL) is set to Enabled, WOL is enabled for all bays. When set to Disabled, WOL is disabled for all bays. The value of Not set indicates that no global policy has been set (some bays may have Wake on LAN® enabled, while others have it disabled). Note that the default BIOS setting for Wake on LAN is enabled for all blades.

Boot sequence

In this section you can view and change the boot sequence settings for all the blades in the chassis. The table has one row per blade bay. The empty bays are marked as such. The blades that take up more than one bay are also indicated.

In order to change the boot sequence settings for a blade, click the blade name link. This will take you to another screen where the settings can be changed and saved.

Serial over LAN (SOL)

SOL provides a text console prompt of blade servers. This is especially used for the blade server JS20, which has no video adapter. SOL will be started inside the command line interface of the BladeCenter management module.

For more information, supported hardware, and details regarding SOL refer to the publications:

- ▶ *BladeCenter and BladeCenter T Management Module Command-Line Interface Reference Guide*
- ▶ *BladeCenter and BladeCenter T Serial over LAN Setup Guide*

4.5.3 I/O Module tasks

To access the I/O module tasks, click **I/O Module Tasks** in the navigation frame to expand the menu, then click one of the submenus.

Power/restart

Here you can power on and off modules installed in the module bays 1–4. The second function is to restart a module and run standard, extended, or full diagnostics.

Attention: Before powering off or restarting a module make sure that no more data transfer over the modules occurs. If there are redundant modules make sure that the redundant module is working.

For the location of switch module bays 1–4, see Figure 4-28 on page 125.

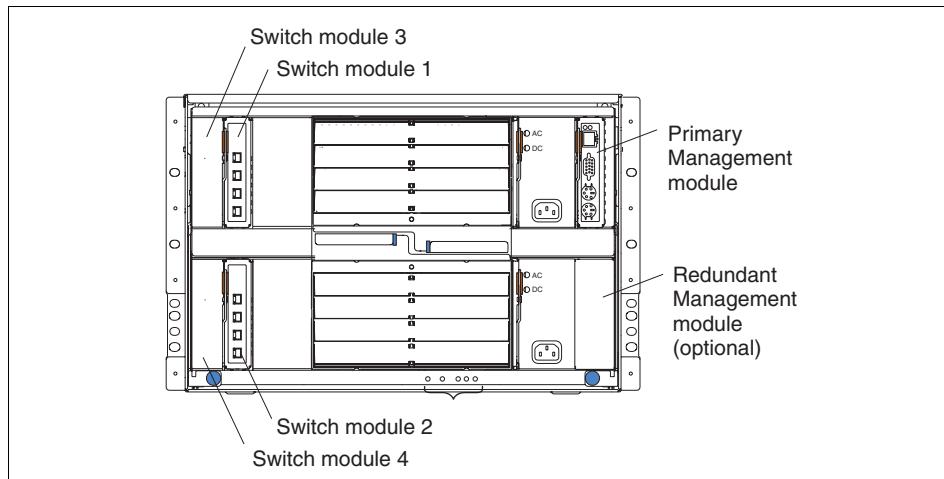


Figure 4-28 BladeCenter module bays

To power on, power off, or restart a module, add a check mark to the box beneath the corresponding module (you can check more than one box) and click the action you want to start, for example, **Restart Module(s)** and **Run Standard Diagnostics**.

Management

On this page, you can view and change basic IP configuration parameters for switch modules in the chassis. For advanced configuration of each switch module click **Advanced Management** in the appropriate module bay pane.

Advanced Management

In the advanced management you can configure advanced parameters, view the last POST result, ping the module, or start a telnet or Web browser session. To check if the module is accessible by IP, click **Ping Switch Module**. If there are problems contact your network administrator and refer to 7.3, “Provide remote access to all BladeCenter modules” on page 239.

When the switch module is accessible, you can click **Start Telnet Session** or **Start Web Session** to access it.

When you launch the Web interface, log in with the standard login. Now you can configure and manage the switch module. As a first step, update the firmware of the switch module to the most recent version.

For further information refer to the documentation that comes with the switch module.

Tip: When you have an Ethernet switch module (ESM) installed make sure you enable the external Ethernet ports of the ESM. They are initially disabled. Click **Configuration** → **Port settings** → **Configure Ports**, enable the ports, and click **Apply**.

Firmware update

Use this panel to update firmware components on a specific I/O module. You first need to download the latest firmware files from the IBM support Web site. Then select a target module using the Target pull-down and complete the procedure as prompted.

Tip: Note that only I/O modules that support flashing over the management module Web GUI are listed in the target pull-down. If the module you want to update is not available in the target pull-down, refer to “Management” on page 125 for how to access the appropriate module’s own Web interface to update the firmware.

4.6 Ports used by the management module

The management module is using several TCP/UDP ports for communication. If the communication with the management module passes firewalls it is important to know which ports you have to enable on the firewalls to communicate with the management module.

Table 4-2 lists the user-configured management module ports. Remember when you change the ports in the management module you have to change them in the firewalls too.

Table 4-2 User-configurable management module ports

Port name	Default port number	Description
http	80	Web server HTTP connection - TCP
https	443	SSL connection - TCP
telnet	23	Telnet command-line interface connection - TCP
SSH	22	Secure Shell (SSH) command-line interface - TCP
SNMP Agent	161	SNMP get/set commands - UDP
SNMP Traps	162	SNMP traps - UDP

The following ports are fixed. You cannot change them.

Table 4-3 Fixed management module ports

Fixed port number	Description
25	e-Mail alerts - TCP
53	UDP Domain Name Server (DNS) resolver - UDP
68	DHCP client connection - UDP
427	Service Location Protocol (SLP) connection - UDP
1044	Remote disk function - TCP
1045	Persistent remote disk (disk on card) - TCP
5900	Remote Console - TCP
6090	IBM Director commands - TCP
13991	IBM Director alerts - UDP

4.7 Resetting the management module back to factory defaults

The BladeCenter management module has a reset button with which you can reset the module and return it to the factory defaults. This reset button is below the management module connectors, near the MAC address.

Use a straightened paper clip or a similar item to access it. The reset button has two uses:

- ▶ Reset the network configuration: Press and hold the reset button for 3 seconds or less.
- ▶ Reset the entire management module (including user IDs and passwords) to the factory defaults. This requires a sequence of presses and releases:
 - a. Press and hold the reset button for 5 seconds.
 - b. Release the button and wait 5 seconds.
 - c. Press and hold the button for another 10 seconds.

Note that this sequence should be as precise as possible to ensure success: 5 in, 5 out, 10 in. After you do a full factory defaults reset in this way, the default user ID and password will be in effect: USERID (all caps) and PASSW0RD (a zero, not the letter O).

After the network configuration has been reset, you can access the Web interface to reconfigure it. To do this, you will need to know the management module's IP address. This can be done as follows:

- ▶ The management module defaults to using DHCP. The host name will be MMxxxxxx, where xxxxxxx is the MAC address of the management module. This number is printed below the reset button.
- ▶ If no DHCP server is found, the management module uses a default IP address of 192.168.70.125 with subnet mask 255.255.255.0. The host name will be MMxxxxxx.

Note: Because it is possible to reset the passwords using the reset button, you should ensure that your BladeCenter chassis is physically secure so that only authorized personnel can physically access the reset button.



Security and authentication

Access to the RSA II and BladeCenter management modules are initially secured through the use of a default user ID and password. Once you change this password (or disable the default and add new users), the service processor is secure from unauthorized access.

By default, the user ID and password are encrypted using a Data Encryption Standard (DES) algorithm, and private session keys are used to maintain security throughout the management session. There are additional steps you can take to further protect your systems management environment: SSL encryption and authentication using LDAP.

In this chapter, we describe the following:

- ▶ We describe how to configure the service processor to use the SSL and SSH in 5.1, “Security using SSL” on page 130.
- ▶ We describe how to implement LDAP to centralize user ID and password management for all service processors in 5.2, “Authentication using LDAP” on page 139.

These security and authentication features are available on the Remote Supervisor Adapter II (including EXA and SlimLine family members) and the BladeCenter management module. They are not available on the Baseboard Management Controller (BMC).

5.1 Security using SSL

For secure communication with the RSA II or the BladeCenter management module, especially when using a WAN connection, you can use Secure Sockets Layer (SSL) or Secure Shell Server (SSH).

5.1.1 Secure Sockets Layer (SSL)

The RSA II or BladeCenter management module can act as a SSL server for a secure Web server (HTTPS) or as a secure LDAP client (LDAPS) for a LDAP server like Windows Active Directory Service (ADS) or Linux OpenLDAP.

In order to provide an SSL connection, there must be an SSL certificate. It is possible to use a self-signed certificate or one that is signed by a third-party authority.

Using a self-signed certificate is the simplest method for using SSL, but it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection that is attempted between the client and server. It is possible that a third party could impersonate the server and intercept data that is flowing between the RSA II or management module and the Web browser. If, at the time of the initial connection between the browser and the RSA II or management module, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming that the initial connection was not compromised by an attack).

For more complete security, you can use a certificate that is signed by a certificate authority. To obtain a signed certificate, use the SSL Certificate Management page to generate a certificate-signing request. You must then send the certificate-signing request to a certificate authority and make arrangements to purchase a certificate.

Configure a secure Web server

Use the following general tasks list to configure a secure Web server for the RSA II or BladeCenter management module:

1. Open a browser window and access the RSA II Web interface.
2. Click **ASM Control** or **MM Control** → **Security**. Figure 5-1 on page 131 appears.

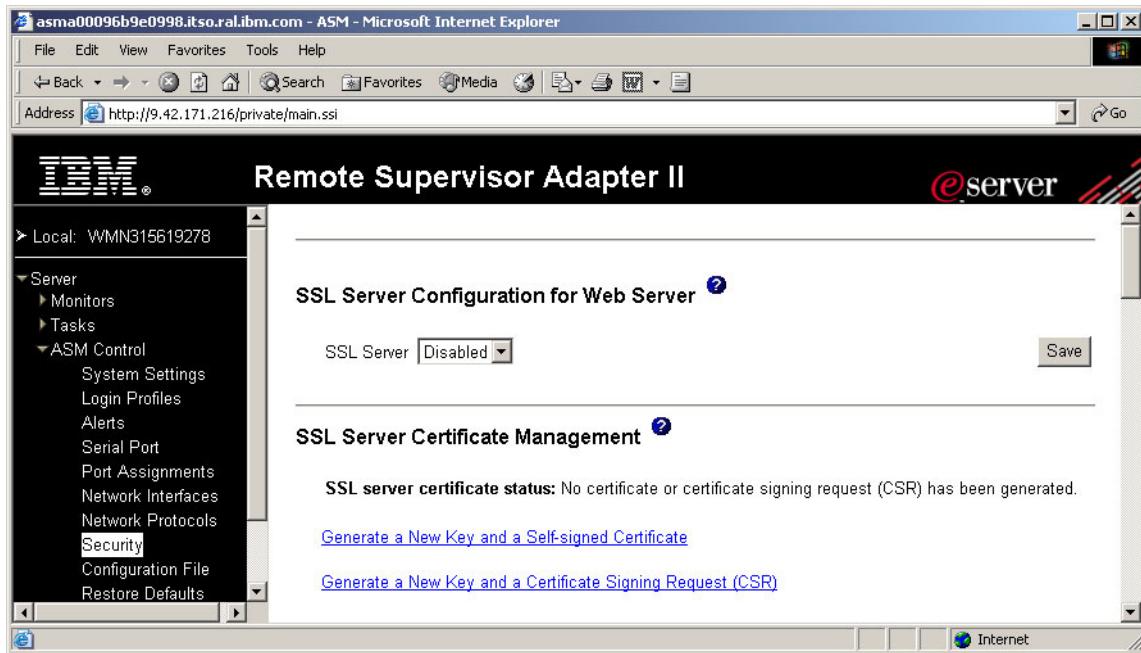


Figure 5-1 Configure a secure Web server

3. Select **Disabled** for the SSL server configuration for the Web server.
4. Click **Save**.
5. Generate or import a certificate. Click **Generate a new key and a self-signed certificate** when you use a self-signed certificate or **Generate a New Key and a Certificate Signing Request (CSR)** if you want to use a certificate of a third-party certificate authority.

Note: In the remaining steps we describe the process of a self-signed certificate. For more information on certificates signed by a third-party certificate authority refer to “Secure Web server and secure LDAP” in Chapter 3 of the *Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User’s Guide* or *BladeCenter Management Module User’s Guide*.

6. Fill in the data for the self-signed certificate.

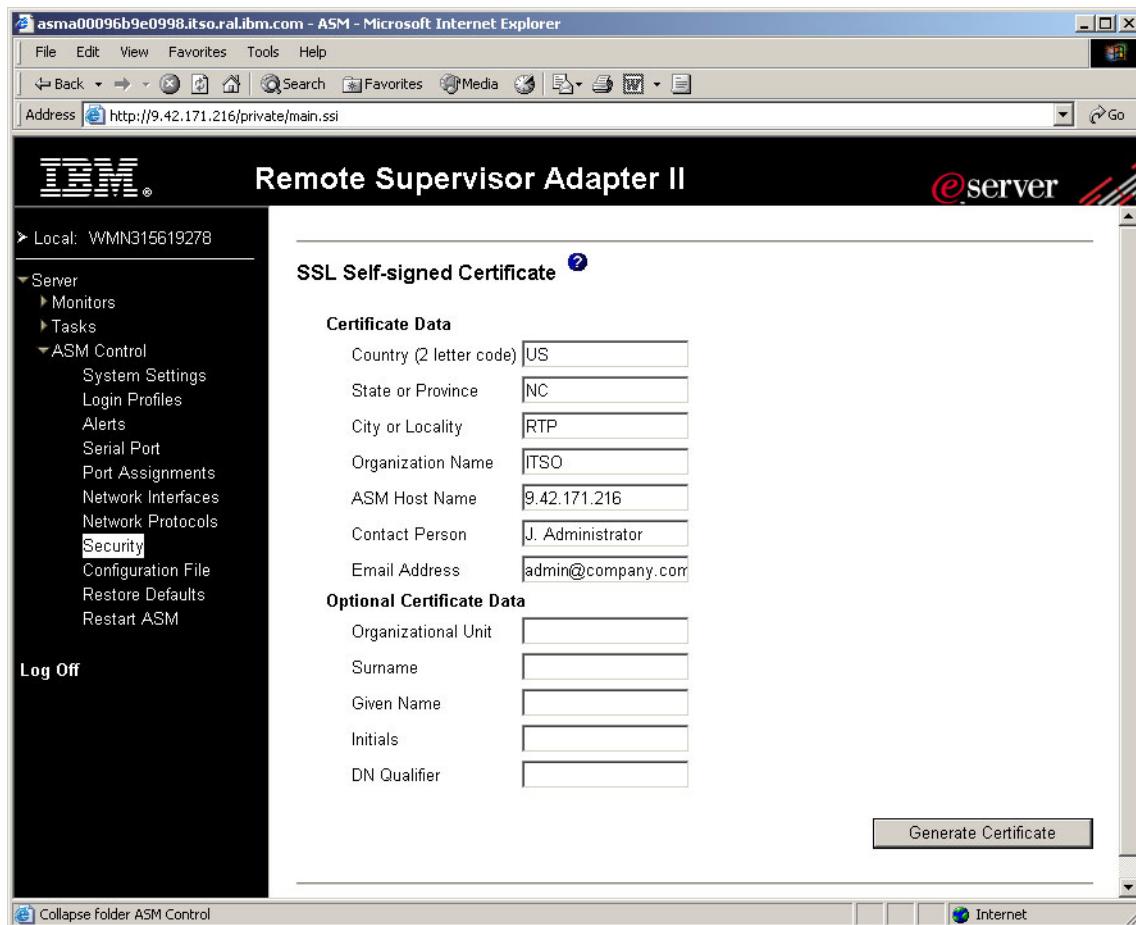


Figure 5-2 *Self-signed certificate*

Take care to ensure that the value entered into the ASM or MM host name field exactly matches the host name as it is known by the Web browser. The browser compares the host name in the resolved URL to the name that appears in the certificate.

To prevent certificate warnings from the browser, the value used in this field must match the host name used by the browser to connect to the ASM or management module.

For instance, if the URL address bar in the browser currently were to appear as <http://mm11.example.com/private/main.ssi>, the value used for the ASM or MM host name field should be mm11.example.com. If the URL were <http://192.168.70.2/private/main.ssi>, the value used should be 192.168.70.2.

7. Click **Generate Certificate** to start the generation process.
8. Wait until the process of generation finishes. Now the status of the SSL server certificate changes to:
A self-signed certificate is installed
9. Select **Enabled** for the SSL server configuration for the Web server.
10. Click **Save**.
11. To restart the RSA II click **Restart ASM**.

When you reconnect to the RSA II Web interface, it will use a secure connection. First a security alert pops up to inform you that you will use a secure connection. After clicking **OK**, another security alert pops up (Figure 5-3).



Figure 5-3 Security alert

This message indicates that you currently do not trust the certificate. To trust the certificate you have to install it on your computer. If you do not want to install the certificate on your computer, the security alert pops up every time you launch the RSA II's Web interface.

To install the certificate on your computer, do the following:

1. Click **View Certificate**.
2. On the General tab click **Install Certificate**.
3. The Certificate Import Wizard appears.
4. Click **Next**.

5. If you want to save the certificate in a specific location select **Place all certificates in the following store** and specify the location. If not, select **Automatically select the certificate store based on type of certificate**.
6. Click **Next** and then **Finish**.
7. Read the warning and click **Yes** to install the certificate.
8. The information in the certificate window was not updated. To confirm the installation, click **OK**. Now open the window again by clicking **View Certificate** and review the certificate information.

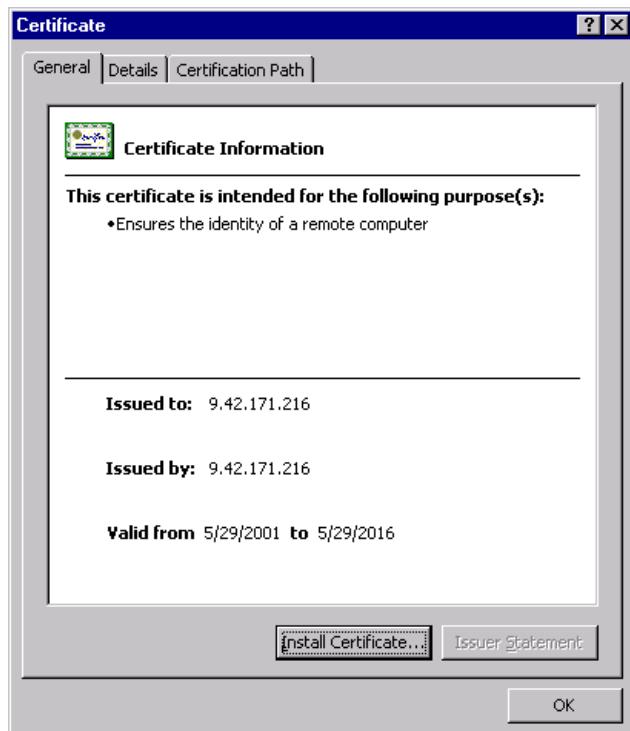


Figure 5-4 Certificate information

9. Click **OK** to close the Window.
10. To proceed click **Yes**.
11. Log on with your credentials.
12. Check the address field of the browser. Now the communication with the RSA II or management module uses HTTPS instead of HTTP protocol.

The next time you launch the Web interface there will be no more security alerts regarding certificates.

Configure a secure LDAP client

To secure an LDAP client with SSL communication, you first need an SSL client certificate. The generation process is the same as for the SSL server certificate, only the link to launch it is different. Refer to “Configure a secure Web server” on page 130 for details. For generating such a certificate, do the following:

1. Click **Generate a new key and a self-signed certificate** in the SSL client certificate management section.
2. Fill in the data for the self-signed certificate.
3. Click **Generate Certificate** to start the generation process.
4. Wait until the process of generation finishes. Now the status of the SSL client certificate changes to:
A self-signed certificate is installed

For details on configuring the LDAP client, see 5.2, “Authentication using LDAP” on page 139.

5.1.2 Secure Shell (SSH)

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial (text console) redirect features of the RSA II and BladeCenter management module.

Note: SSH is supported on the BladeCenter management module; however, the SSH feature is not available on all servers with an RSA II installed. Check the README file in the firmware update package for the RSA II for your specific server.

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial (text console) redirect features of the management module.

Secure Shell users are authenticated by exchanging a user ID and password. The password and user ID are sent after the encryption channel is established. The user ID and password pair can be one of the 12 locally stored user IDs and passwords, or they can be stored on an LDAP server. Public key authentication is not supported.

A Secure Shell server key is used to authenticate the identity of the Secure Shell server to the client. Secure Shell must be disabled before you create a new Secure Shell server private key. You must create a server key before enabling the Secure Shell server.

When you request a new server key, a Rivest, Shamir, and Adelman key and a DSA key are created to allow access to the Remote Supervisor Adapter II from either an SSH Version 1.5 or an SSH Version 2 client. For security, the Secure Shell server private key is not backed up during a configuration save and restore operation.

To access the SSH server you need a SSH client. An SSH client is standard with Linux or is available as a third-party product, such as PuTTY, as described below.

Complete the following steps to create a new Secure Shell server key:

1. Open a browser window and access the service processor Web interface.
2. Click **ASM Control** or **MM Control** → **Security**. Figure 5-5 appears.

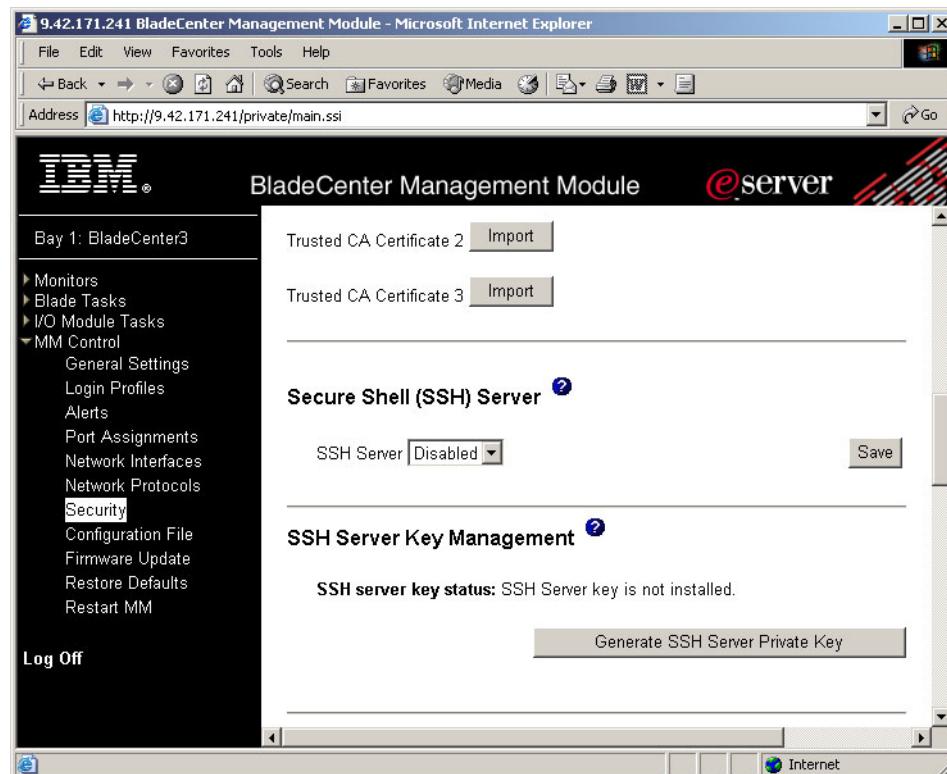


Figure 5-5 Secure Shell (SSH) Server - BladeCenter management module

3. Scroll to the Secure Shell (SSH) Server section and make sure that the Secure Shell server is disabled. If it is not disabled, select **Disabled** in the SSH Server field and then click **Save**.

4. Scroll to the SSH Server Key Management section. Click **Generate SSH Server Private Key**.
5. Click **OK** at the next window to proceed.
6. A progress window opens. Wait for completion of the operation. This can take several minutes.

From the Security page, you can enable or disable the secure shell server. The selection that you make takes effect only after the management module is restarted. The value displayed on the screen (Enabled or Disabled) is the last value selected and is the value used when the service processor is restarted.

Tip: You can enable the Secure Shell server only if a valid Secure Shell server private key is installed.

Complete the following steps to enable the Secure Shell server:

1. In the navigation frame, click **Security**.
2. Scroll to the Secure Shell (SSH) Server section.
3. Click **Enabled** in the SSH Server field, then **Save**.
4. Click **Restart ASM** or **Restart MM** in the navigation frame to restart the service processor.

Now you can use a SSH client to connect to the CLI of the management module. In our example we used the free tool PuTTY, available from:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

1. Launch PuTTY by executing the EXE file.
2. At the first time a security alert pops up. Read it carefully and click **Yes** if you want to continue.

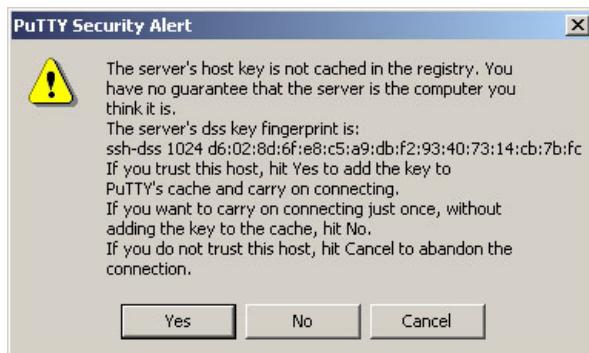


Figure 5-6 PuTTY security alert

3. Log on to the RSA II or management module.

```
login as: USERID
USERID@9.42.171.241's password:
system>
```

Now you can use the CLI through a secure connection.

If you enable SSH for a secure CLI, you should also disable the unsecure telnet interface when using the RSA II.

Restriction: At the time of writing, the option to disable the telnet protocol was not available in the management module. As a work-around, do not use telnet with the management module, and change the port of the telnet protocol.

To disable the telnet interface of RSA II, complete the following steps:

1. Open a browser window and access the RSA II Web interface.
2. Click **ASM Control → Network Protocols**.
3. Scroll to the Telnet Protocol section and select **Disabled** in the Telnet connection count field.

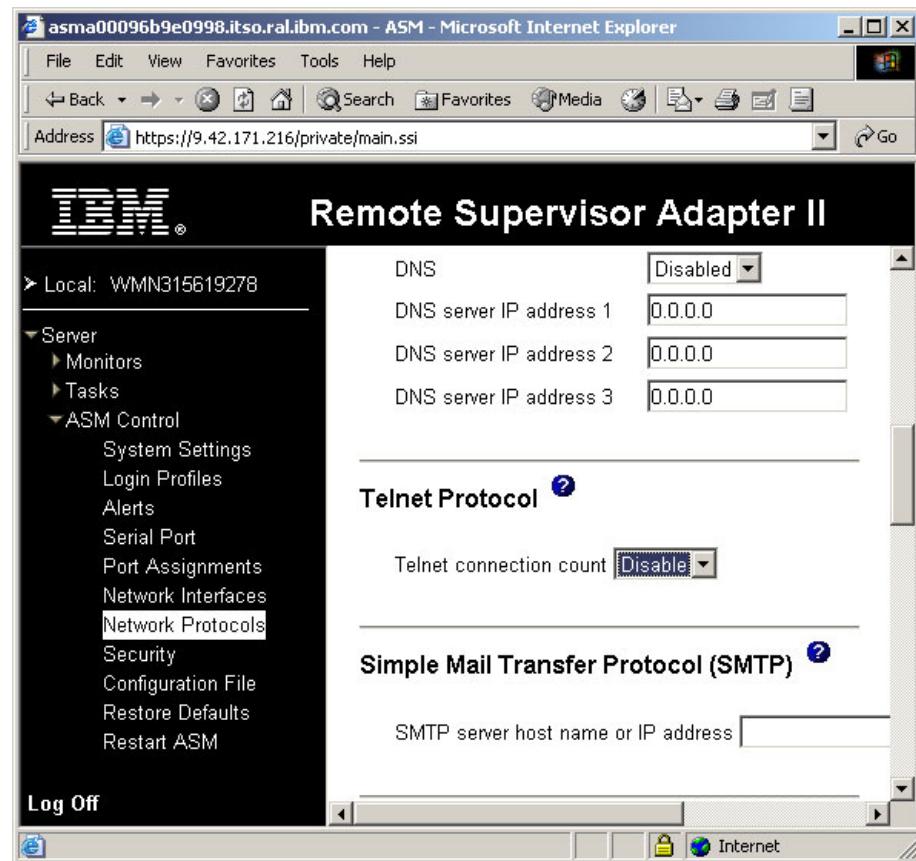


Figure 5-7 Disable telnet protocol

4. Scroll down to the bottom of the page and click **Save**.
5. Read the note and click **OK**.
6. Restart the RSA II or management module by clicking **ASM Control → Restart**.
7. Click **Restart**.

5.2 Authentication using LDAP

To optimize account administration, you can use an LDAP server for authentication with all your RSA II and management module devices instead of administrating a separate set of users on every service processor.

5.2.1 LDAP authentication attribute

For authentication with an LDAP server, the RSA II or management module must be configured as LDAP client. To set the authority levels for users, there is one attribute that is set at the LDAP server. This attribute consists of twelve bits. The bits, numbered from left to right, have the following meaning:

- ▶ Bit 0 - Deny always
If set, a user will always fail authentication. Use this function to block a particular user or users associated with a particular group.
- ▶ Bit 1 - Supervisor access
If set, a user is given administrator privileges. The user has read and write access to every function. If you set this bit, you do not have to individually set the other bits.
- ▶ Bit 2 - Read only access
If set, a user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates), and nothing can be modified (using the save, clear, or restore functions). Note that read-only and all other bits are mutually exclusive, with read-only having the lowest precedence. That is, if any other bit is set, this bit will be ignored.
- ▶ Bit 3 - Networking and security
If set, a user can modify the configuration in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages in the Web interface.
- ▶ Bit 4 - User account management
If set, a user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page in the Web interface.
- ▶ Bit 5 - Remote console access
If set, a user can access the remote server or remote blade server console.
- ▶ Bit 6 - Remote console and remote media
If set, a user can access the remote server console and the remote media functions for the remote (blade) server.
- ▶ Bit 7 - Remote power/Restart access
If set, a user can access the power on and restart functions for the remote server or blade server and I/O modules of BladeCenter. These functions are available in the Power/Restart page in the Web interface.

- ▶ Bit 8 - Basic adapter configuration
If set, a user can modify basic configuration parameters in the System Settings and Alerts pages in the Web interface.
- ▶ Bit 9 - Ability to clear event logs
If set, a user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
- ▶ Bit 10 - Advanced adapter configuration
If set, a user has no restrictions when configuring the adapter. In addition, the user is said to have administrative access to the Remote Supervisor Adapter II, meaning that the user can also perform the following advanced functions: Firmware updates, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart and reset the adapter.
- ▶ Bit 11 - Reserved for future use

Here are some examples of how this attribute might look like and what it means:

010000000000 - Supervisor Access (bit position 1 is set)
 001000000000 - Read-Only Access (bit position 2 is set)
 100000000000 - No access (bit position 0 is set)
 000011111100 - All authorities except Advanced Adapter Configuration
 000011011110 - All authorities except access to virtual media

In the following sections we use the attribute to assign the appropriate rights to the groups.

For further information refer to *Lightweight Directory Access Protocol User's Guide for IBM @server BladeCenter Management Module and IBM Remote Supervisor Adapters*, available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-55014.html>

5.2.2 Configuring the LDAP server

In our example we use Active Directory on Windows Server 2003 as our LDAP server. We create three groups and four users assigned to them. The following table shows the details.

Table 5-1 Groups, users, and rights used in our example

Domain	Group	Rights	User
ibm.com®	RSA_Supervisor	Supervisor access	Bain
			Leitenberger
	RSA_Basic	Network & Security	Administrator
	RSA_ReadOnly	Read only access	Watts

Verify that you have administrative rights in your domain (for example, member of the groups Domain Admins or Enterprise Admins, or an administrator has delegated the appropriate rights to you).

Create groups and assign users

The first step is to create groups for the administration of the service processors. In our example, we create three groups.

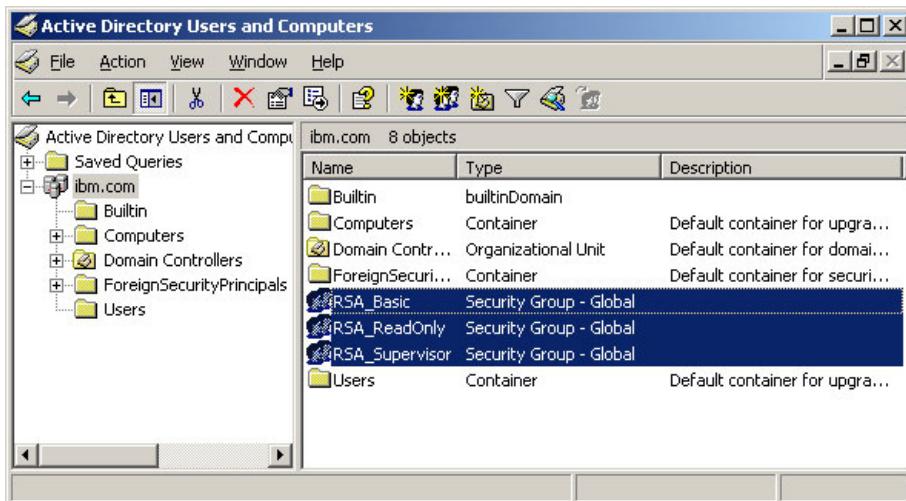


Figure 5-8 Groups in active directories

Right-click each group and click **Properties**. Click **Add** to add members to the group. Repeat this for all groups and all members.

Create new schema attribute

To create the attribute described in 5.2.1, “LDAP authentication attribute” on page 140, and assign it to the groups, you have to create an additional attribute in the Active Directory Schema and assign this to groups or users. The attribute is an additional field and has a specific value (the twelve bits).

Tip: To create a new schema attribute you need to assign an object ID (OID) to it. Your LDAP administrator can provide this value.

As an alternative, you could use an existing unused attribute that you do not plan to use in the future. If you plan to do this, you do not need to create a new attribute, and can continue with the procedure at “Assign the schema attribute to users or groups” on page 145.

The MMC snap-in for schema is not activated by default. Check the Administrative Tools in the Windows Start menu for the Active Directory Schema entry. If it is not there, complete the following steps to activate it:

1. Open a command prompt.
2. Enter the following command to register the Active Directory Schema Manager (schmmgmt.dll) on your computer:
`regsvr32 schmmgmt.dll`
3. Click **Start**, click **Run**, type `mmc /a`, and then click **OK**.
The /a parameter starts Microsoft® Management Console in author mode.
4. On the File menu, click **Add/Remove Snap-in**.
5. Click **Add**.
6. Double-click **Active Directory Schema** in the list.
7. Select local if you are working from the LDAP server, or enter the name of the LDAP server.
8. Click **Close**, and then click **OK**.
9. To save this console, on the File menu, click **Save**.
10. In Save in, point to the `systemroot\system32` directory.
11. In File name, type `schmmgmt.msc`, and then click **Save**.

For future use you can create a shortcut on your Start menu:

1. Right-click **Start**, click **Open all Users**, double-click the **Programs** folder, and then double-click the **Administrative Tools** folder.
2. On the **File** menu, point to **New**, and then click **Shortcut**.
3. In the Create Shortcut Wizard, in Type the location of the item, type `schmmgmt.msc`, and then click **Next**.
4. On the Select a Title for the Program page, in Type a name for this shortcut, type **Active Directory Schema**, and then click **Finish**.

Attention: Modifying the schema is an advanced operation best performed by experienced programmers and system administrators. For detailed information about modifying the schema, see the *Active Directory Programmer's Guide* at the Microsoft Web site.

Launch the Active Directory Schema snap-in and click **Action → Create Attribute**.

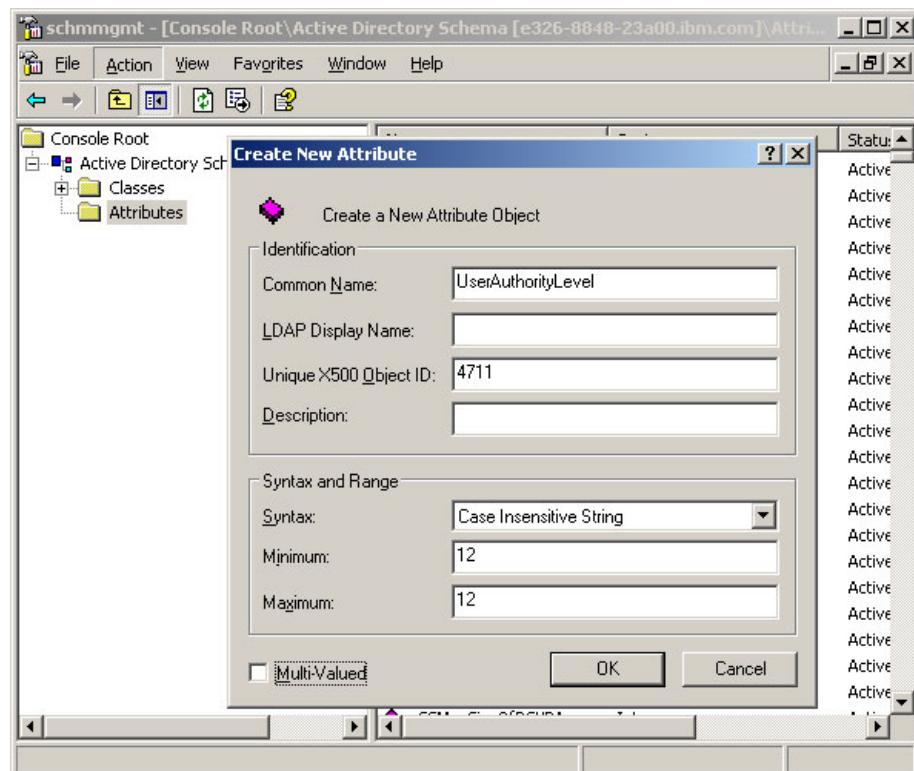


Figure 5-9 Create new attribute in Active Directory schema

Do the following entries:

1. Fill in the common name you want to use. We are using UserAuthorityLevel in our example. The name is not case sensitive.
2. Enter your X.500 object ID.

Note: Contact your LDAP system administrator to assign a new X.500 OID.

3. Set the syntax to **Case Insensitive String**.
4. Set minimum and maximum to **12**.
5. Click **OK** to save the attribute.

Assign the schema attribute to users or groups

Now assign the attribute to groups or users and enter the desired value for that attribute. This value is the twelve-bit value.

Tip: We recommend that you assign the attributes to the groups instead of the user, because it is easier to manage a few groups than a lot of users.

To assign the attribute to a user or a group do the following:

1. Click **Classes** and scroll to the entry user or groups.
2. Double-click the class **user** or **groups**.
3. The properties window pops up. Now click the **Attributes** tab.

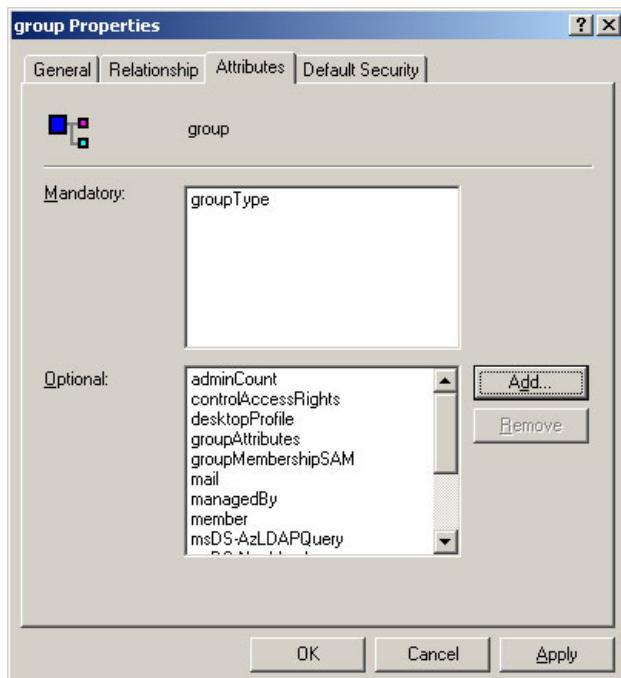


Figure 5-10 Group properties

4. Click **Add** to add an attribute to the group.

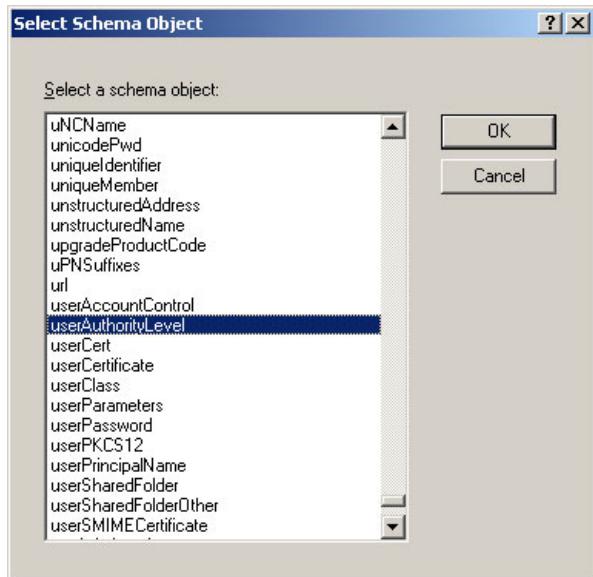


Figure 5-11 Select schema object

5. Select the attribute **UserAuthorityLevel** you created before and click **OK**.
6. Click **Apply** and **OK**.

Now you have created the new attribute and assigned it to the class group. To enter a value you have to use a special tool, because you will not find the new attribute in the normal properties window of the group.

Assign values to the new attribute

The tool to assign values to attributes that are not shown in the objects properties window is called the Active Directory Service Interfaces (ADSI) Edit tool and is part of the Windows support tools. If it is not installed, install the support tools from the Windows CD. You find the installation program in \SUPPORT\TOOLS. Run the installer and follow the instructions.

Once the tools are installed, navigate to the folder where they are installed. The default folder is \Program Files\Support Tools. Double-click the file **adsiedit.msc**.

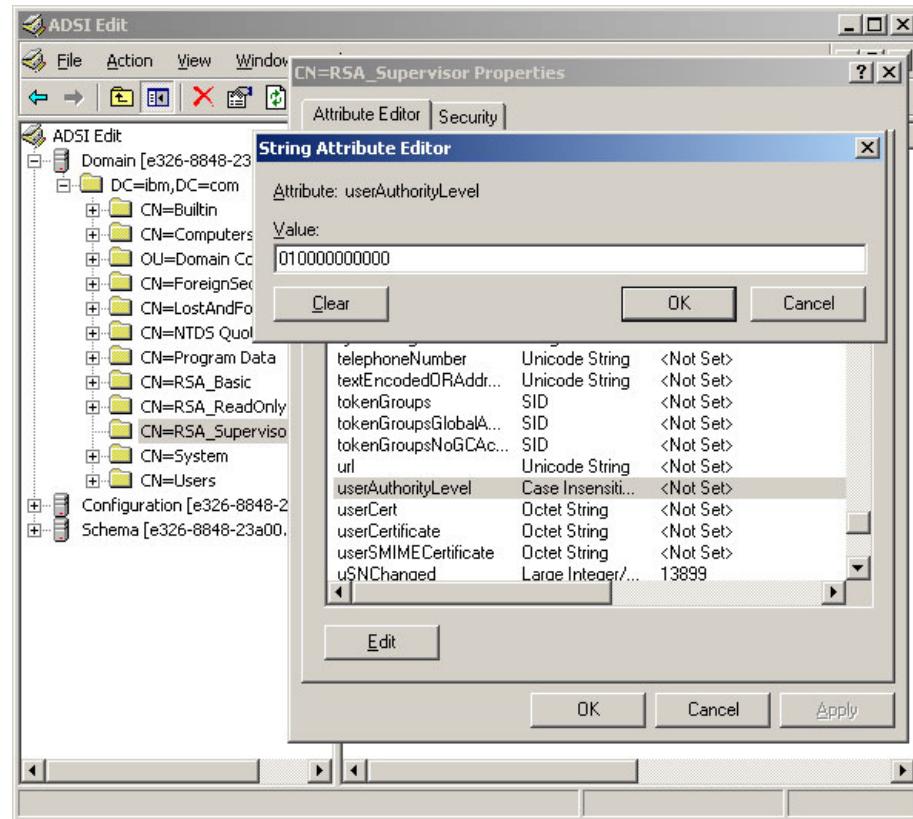


Figure 5-12 Assign value to the attribute

1. Expand the **Domain** entry in the tree view.
2. Right-click the group you want to enter a value for **userAuthorityLevel** and click **Properties**.
3. Scroll to the attribute **UserAuthorityLevel** and click **Edit**.
4. Now enter the desired value and click **OK**. Refer to 5.2.1, “LDAP authentication attribute” on page 140, for a description of the value.

Repeat the steps for all objects (groups or users) you want to enter values for the UserAuthorizationLevel.

5.2.3 Testing the LDAP server configuration

Before you configure the service processors, you should test the configuration with a LDAP browser. A LDAP browser is installed in the support tools directory, LDP.EXE.

1. In the menu pane click **Connection** → **Connect**.
2. Enter the LDAP server and port. **Click OK**.
3. Now click **Connection** → **Bind**.
4. Enter a user, password, and domain. Click **OK**. The result should look like:

```
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, 1158); // v.3
    {NtAuthIdentity: User='administrator'; Pwd= <unavailable>; domain
 = 'IBM' .}
Authenticated as dn:'administrator'.
```
5. To start the browsing click **Browse** → **Search**. The following window pops up.

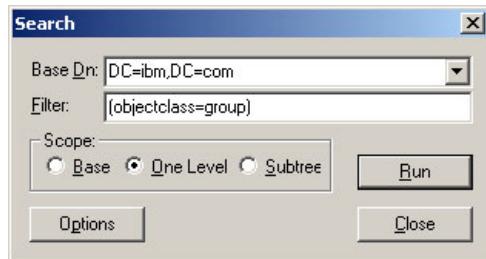


Figure 5-13 Search window

6. Select you appropriate Base Dn and change the filter to (objectclass=group).
7. Now click **Options**.
8. Change the Attributes to **member; userAuthorityLevel** and click **OK**.

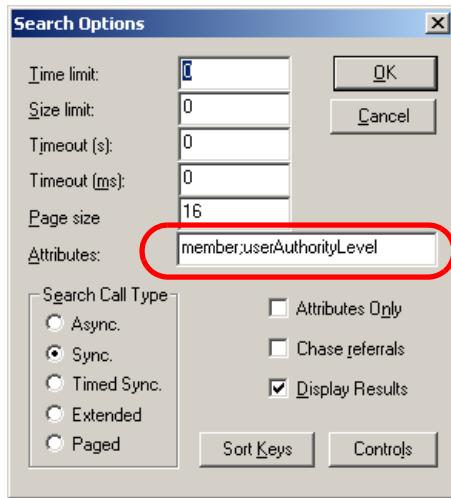


Figure 5-14 Setting the Attributes field

9. Now click **Run**.

The query result should look like Figure 5-15.

```
***Searching...
ldap_search_s(ld, "DC=ibm,DC=com", 1, "(objectclass=group)",
attrList, 0, &msg)
Result <0>: (null)
Matched DNs:
Getting 3 entries:
>> Dn: CN=RSA_Basic,DC=ibm,DC=com
 1> member: CN=Administrator,CN=Users,DC=ibm,DC=com;
 1> userAuthorityLevel: 000100000000;
>> Dn: CN=RSA_ReadOnly,DC=ibm,DC=com
 1> member: CN=Watts,CN=Users,DC=ibm,DC=com;
 1> userAuthorityLevel: 001000000000;
>> Dn: CN=RSA_Supervisor,DC=ibm,DC=com
 2> member: CN=Leitenberger,CN=Users,DC=ibm,DC=com;
CN=Bain,CN=Users,DC=ibm,DC=com;
 1> userAuthorityLevel: 010000000000;
-----
-----
```

Figure 5-15 Results of the LDAP query

In our example, we have four users in three groups with different authority levels. The LDAP browser shows the group membership of the users and the authority level of the group.

5.2.4 Configuring the LDAP client

The system management hardware acts as a Version 2.0 LDAP client. When an authentication request comes in (that is, a user logs in), the LDAP client sends the user credentials to the LDAP server for verification. If the user is authenticated, the user gets access to the RSA II or BladeCenter management module according his defined access rights.

To configure the general LDAP settings, launch the Web interface and complete the following steps:

1. Under ASM Control in the navigation pane (or MM Control when using a BladeCenter management module), click **Network Protocols**.
2. Scroll down to the Lightweight Directory Access Protocol (LDAP) Client section.
3. Select either **Use DNS to find LDAP servers** to discover them automatically through DNS or **Use pre-configured LDAP servers** to manually configure the LDAP server's addresses.
 - If you use DNS to find the LDAP server, you have to select the method to specify the domain name. The choices are:
 - Extract search domain from login id
 - Use only configured search domain below
 - Try login id first, then configured value

The screenshot shows a configuration panel for LDAP server discovery via DNS. It includes a radio button labeled 'Use DNS to Find LDAP Servers' which is selected. Below it are three input fields: 'Domain Source' with a dropdown menu set to 'Extract search domain from login id', 'Search Domain' containing the placeholder 'example.com', and 'Service Name' containing the value 'ldap'.

Figure 5-16 Parameters to specify when using DNS

With “Extract search domain from login id,” the LDAP client uses the domain name in the login ID. For example, if the login ID is admin@example.com, the domain name equals example.com. If the domain name cannot be extracted, user authentication will fail automatically.

To configure a domain name manually select **Use only configured search domain below**, and type in the domain name in the Domain search field.

The third option is “Try login id first, then configured value.” With this option, the LDAP client will first attempt to extract the domain name from the login ID. If this succeeds, this domain name will be used in the DNS SRV request. If there is no domain name present in the login ID, the LDAP client will instead use the configured Search Domain parameter as the domain name in the DNS SRV request. If nothing is configured, user authentication will fail immediately.

Tip: Make sure that you configure at least two DNS servers in the Domain Name System (DNS) section. Scroll up to find this section.

The DNS SRV request sent to the DNS server must also specify a service name. The configured value will be used for this purpose. If left blank, the default value used is LDAP. Note that the DNS SRV request must also specify a protocol name. This defaults to tcp and is not configurable.

Use Pre-Configured LDAP Servers	
LDAP Server Host Name or IP Address	Port
1. []	[]
2. []	[]
3. []	[]

Figure 5-17 Parameters to specify when using DNS

- When specifying pre-configured (hardcoded) LDAP servers (Figure 5-17), make sure that you provide at least two different server addresses to have a kind of redundancy in case of a LDAP server failure.

Type in the IP addresses or host names (ensure that name resolution, for example, DNS, is working properly when using host names) and the used LDAP port. If you have not changed the port at the LDAP server you can leave this parameter blank.

Tip: Only use the pre-configured LDAP servers option in small/medium businesses and mainly static environments, because whenever there are changes to the LDAP server addresses, you have to update every service processor.

4. Provide additional parameters for the LDAP communication. In the Root DN field, enter the distinguished name for the root entry of your domain. In our example it is dc=ibm,dc=com.

Miscellaneous Parameters	
Root DN	<input type="text" value="dc=ibm,dc=com"/>
User Search Base DN	<input type="text"/>
ASM Group Filter	<input type="text" value="RSA*"/>
Binding Method	<input type="text" value="User Principal Name"/> <input type="button" value="▼"/>
Set DN and password only if Binding Method used is Client Authentication	
Set attribute names for LDAP client search algorithm	

Figure 5-18 LDAP miscellaneous parameters

Tip: When using LDAP servers other than Windows ADS, the format of the Root DN could differ. For example, when using Novell eDirectory the parameter would be dc=ibm.com.

5. User Search Base DN field: As part of the user authentication process, it is necessary to search the LDAP server for one or more attributes associated with a particular user or group. Any search request must specify the base DN for the actual search.

The User Search Base DN field specifies the base DN that is used to search for objects whose objectClass equals user (when looking for user records) or group (when looking for group records). User and group searches are part of the authentication process. They are carried out to retrieve information about a user (login permissions and group memberships) or a group (login permissions).

It is important to note that this parameter is the search base for both users (objectClass=user) and groups (objectClass=group). If your users and groups are in different sub-trees, make sure that this parameter is set such that both sub-trees are visible. If this field is left blank, the Root DN will be used as the search base instead.

6. The Group Filter field is used for group authentication. It specifies what group or groups that this Service Processor belongs to. If left blank, group authentication is disabled. Otherwise, group authentication will be performed against the filter. The filter can be a specific group name (for example,

RSAWest), a wildcard (*) that matches everything, or a wildcard with a prefix (for example, RSA*). The default filter is RSA*.

After user authentication, group authentication will take place, whereby an attempt will be made to match the group or groups (that the user belongs to) to the group filter defined here. If there is no match, the user will not pass authentication and will be blocked. If there is a match, the login permissions for the user will be retrieved from the matched groups, unless the user already has login permissions assigned directly from the user record retrieved from the LDAP server.

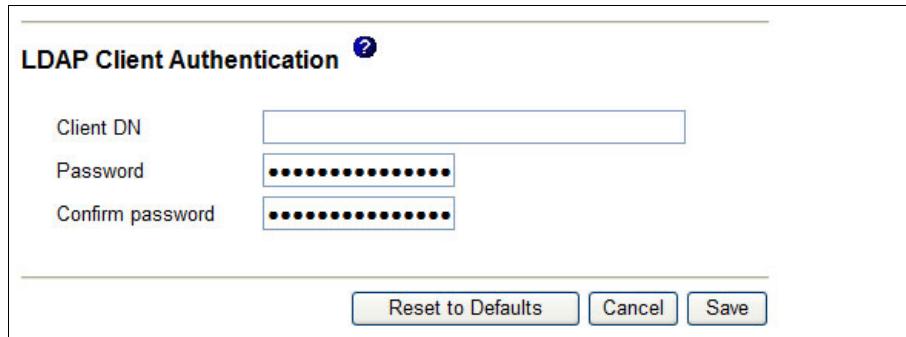
7. Binding Method field: On initial binds to the LDAP server during user authentication, there are four options to select as the binding method:
 - Anonymous authentication. Bind attempt is made without a client DN or password. If the bind is successful, a search will be requested in order to find an entry on the LDAP server for the user attempting to login. If an entry is found, a second attempt to bind will be attempted, this time with the user's DN and password. If this succeeds, the user is deemed to have passed the user authentication phase. Group authentication is then attempted if it is enabled.

Attention: Do not use anonymous authentication, because subsequent search requests will fail when a null user ID and null password are used as the parameters to the initial bind request.

- Client authentication. A bind attempt is made with a client DN and password specified by this configuration parameter. If the bind is successful, we proceed as above.
- User Principal Name (UPN). This is the default. A bind attempt is made directly with the credentials used during the login process. If this succeeds, the user is deemed to have passed the user authentication phase. For Active Directory servers, the user ID can have the form user@domain, or simply user.
- Strict UPN. This is the same as UPN above, except that the user ID must have the form someuser@domain. The string entered by the user will be parsed for the @ symbol.

Tip: Both the UPN and strict UPN methods work with Windows ADS only.

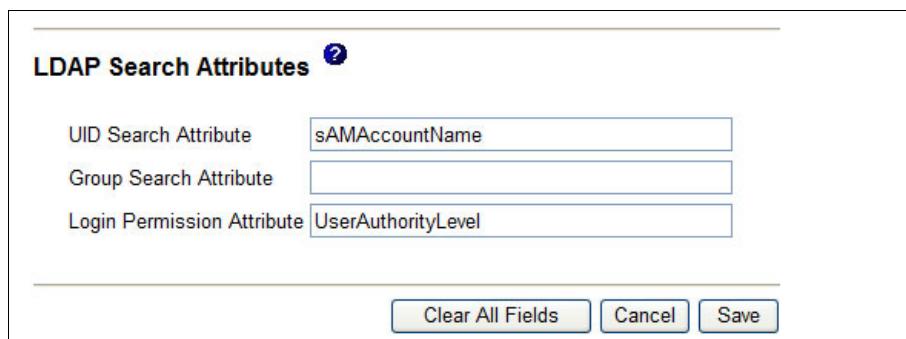
8. When client authentication is used as bind method, click **Set DN and password only if Binding Method used is Client Authentication**.
Figure 5-19 on page 154 appears. Provide a user ID and password for the initial bind request. Click **Save** after you fill in the parameters.



The screenshot shows the 'LDAP Client Authentication' configuration window. It contains three input fields: 'Client DN' (empty), 'Password' (filled with dots), and 'Confirm password' (also filled with dots). Below the fields are three buttons: 'Reset to Defaults', 'Cancel', and 'Save'.

Figure 5-19 LDAP client authentication for initial bind request

9. To set the LDAP Search attributes, click **Set attribute names for LDAP client search algorithm**. Figure 5-20 appears. Click **Save** to save any changes you make and return to the previous window.



The screenshot shows the 'LDAP Search Attributes' configuration window. It has three input fields: 'UID Search Attribute' (set to 'sAMAccountName'), 'Group Search Attribute' (empty), and 'Login Permission Attribute' (set to 'UserAuthorityLevel'). Below the fields are three buttons: 'Clear All Fields', 'Cancel', and 'Save'.

Figure 5-20 LDAP client authentication for initial bind request

- Specify the attribute name used to represent user IDs on your LDAP server. The default UID search attribute is uid. For Windows ADS enter sAMAccountName.
When the binding method selected is UPN or Strict UPN, this field defaults automatically to userPrincipalName during user authentication if the user ID entered has the form user@domain.
- To detect which user belongs to which groups specify the group search attribute. If this field is left blank, the attribute name in the filter will default to memberOf. The default works with Windows ADS and Novell eDirectory.
- For assigning the proper user rights for ASM, specify the attributes name used at the LDAP server. As per “Create new schema attribute” on page 142, we are using the attribute UserAuthorityLevel.

10. Scroll down and click **Save** to save all the changes.

Tip: A reboot is not necessary when changing the LDAP configuration.

The last step is to configure the service processor to use a LDAP server for authentication. To do this click **ASM Control** (or **MM Control** when using BladeCenter management module) → **Login Profiles** in the navigation frame. Change the values in the Global Login Settings section.

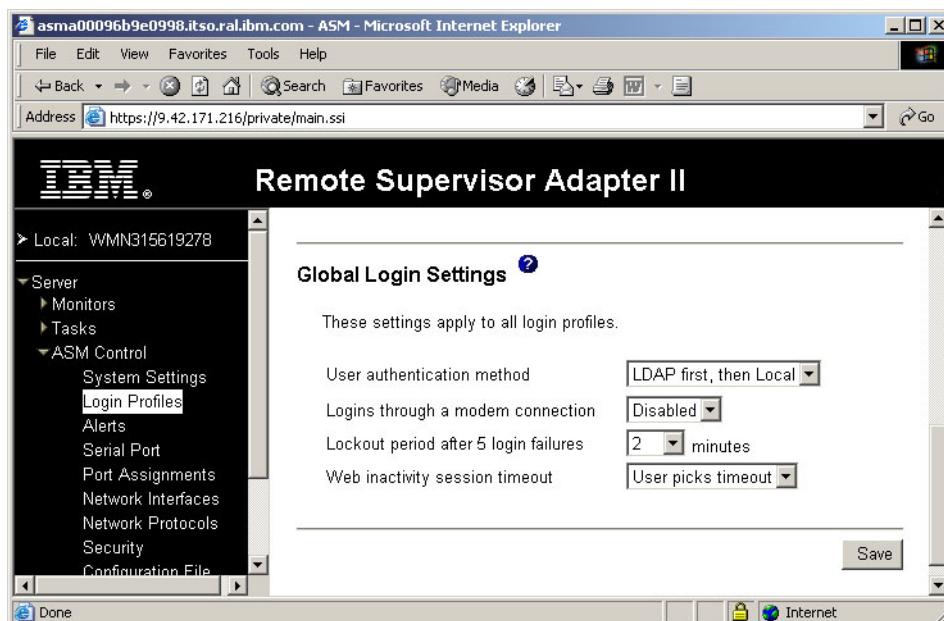


Figure 5-21 Global login settings

In the User authentication method field, there are four choices:

- ▶ Local only
- ▶ LDAP only
- ▶ Local first, then LDAP
- ▶ LDAP first, then local

We recommend that you use Local first, then LDAP or LDAP first, then local only. In case of problems regarding LDAP authentication you can still access the RSA II or BladeCenter management module through a locally defined user.

Change any other settings as you feel appropriate for your installation and click **Save** to save the changes.

Now log off and log in again with an LDAP user to test the functionality.

Tip: If you are using Windows Active Directory as your LDAP server, you can check the LDAP authentication process by reviewing the Windows Security Event Log.



System management utilities

This chapter describes the user interfaces that can be used to manage the IBM @server 325/326, BladeCenter, and xSeries families of servers. Interfaces discussed in this chapter are:

- ▶ 6.2, “Advanced Settings Utility” on page 160
- ▶ 6.3, “Management processor command-line interface” on page 175
- ▶ 6.4, “OSA SMBridge utility” on page 192
- ▶ 6.5, “Web interface” on page 219
- ▶ 6.6, “Telnet interface” on page 220
- ▶ 6.7, “IBM Director integration” on page 225

This chapter will also detail where to get the user interface from, how to install it, how to configure the user interface for system management, and detail usage of the user interface.

6.1 Comparing the tools

This chapter describes all the available user interfaces that are supported on the range of xSeries servers. However, each tool does not support every server and every service processor.

Table 6-1 lists the tools we cover in this chapter and the servers they are supported on. For more information, see the section in this chapter on each of the tools.

Table 6-1 The user interfaces supported on each xSeries server

Server	ASU	MPCLI ¹	SMBridge	SP Web	SP telnet	Director
xSeries 200	No	No	No	No	No	Supported
xSeries 205	No	No	No	Optional ²	Optional ²	Supported
xSeries 206	No	No	No	Optional ²	Optional ²	Supported
xSeries 220	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 225	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 226	No		No	Optional ²	Optional ²	Supported
xSeries 230	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 232	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 235	Supported	Supported	No	Optional ²	Optional ²	Supported
xSeries 236	No	No	Supported	Optional ²	Optional ²	Supported
xSeries 240	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 250	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 255	Supported	Supported	No	Optional ²	Optional ²	Supported
xSeries 300	No		No	No	No	Supported
xSeries 305	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 306	No	No	No	Optional ²	Optional ²	Supported
xSeries 330	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 335	Supported	Supported	No	Optional ²	Optional ²	Supported
xSeries 336	No	No	Supported	Optional ²	Optional ²	Supported
xSeries 340	No	Supported	No	Optional ²	Optional ²	Supported

Server	ASU	MPCLI¹	SMBridge	SP Web	SP telnet	Director
xSeries 342	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 343	No		No	No	No	Supported
xSeries 345	Supported	Supported	No	Optional ²	Optional ²	Supported
xSeries 346	No	No	Supported	Optional ²	Optional ²	Supported
xSeries 350	No	Supported	No	Optional ²	Optional ²	Supported
xSeries 360	No	Supported	No	Supported	Supported	Supported
xSeries 365	No		No	Supported	Supported	Supported
xSeries 366	No	No	Supported	Optional ²	Optional ²	Supported
xSeries 370	No		No	Supported	Supported	Supported
xSeries 440	Supported	Supported	No	Supported	Supported	Supported
xSeries 445	Supported	No	No	Supported	Supported	Supported
xSeries 450	No	Supported	No	Supported	Supported	Supported
xSeries 455	No	Supported	No	Supported	Supported	Supported
BladeCenter MM	No	Supported	No	Supported	Supported	Supported
Blade HS20	No	Supported	No	Supported	Supported	Supported
Blade HS40	No	Supported	No	Supported	Supported	Supported
eServer 325	No	No	No	No	No	Supported
eServer 326	No	No	No	No	No	Supported

Notes:

1. MPCLI support may only be for specific service processors on supported servers. See Table 6-3 on page 164 for specifics.
2. Support for the Web-based and telnet-based interfaces integrated into the service processor of the server requires the addition of either an RSA II SlimLine, RSA II, RSA, or ASM PCI Adapter. The ANSI terminal interface (same as telnet except uses COM port) is supported on these servers without additional hardware.

As we will be discussing in this chapter, these user interfaces let you perform a variety of management tasks. Table 6-2 on page 160 lists many of the tasks you would consider performing via the management interfaces and the tools that offer them.

Table 6-2 Comparing the tools by supported tasks

Task	ASU	MPCLI	SMBridge	SP Web	SP telnet
View server health	No	Supported	No	Supported	Supported
SP configuration	Supported	Supported	No	Supported	Supported
BIOS configuration	Yes	No	Supported ¹	Supported ¹	No
Power control	No	Supported	Supported	Supported	Supported
Graphical remote control	No	No	No	Supported ²	No
Text-based remote control	No	No	Supported	Supported	No
Batch/command-line mode	Supported	Supported	Limited ³	No	No
View event log	No	Supported	Supported	Supported	Supported
Flash SP firmware	No	Supported	No	Supported	Supported ⁵
Flash system BIOS	No	No	No	No	No
Use remotely	No ⁴	Supported	Supported	Supported	Supported

Notes:

1. Using the remote control feature and rebooting the server.
2. Older service processors such as the ASM PCI Adapter do not support this.
3. SMBridge command-line interface is limited to power control and status queries. See 6.4.7, “Connecting via the command-line interface” on page 216.
4. ASU not designed to be used remotely, but can be if used with IBM Director. See 7.7, “How to use ASU remotely” on page 253.
5. Requires a TFTP server installed on your network to host the firmware update files.

6.2 Advanced Settings Utility

The Advanced Settings Utility (ASU) enables you to modify your firmware settings from the command line on multiple operating system platforms. Using the utility, you can modify user preferences and configuration parameters in the BIOS and the service processor firmware without the need to restart the server to access BIOS Setup via the F1 key.

In addition, the Advanced Settings Utility supports scripting environments through its batch processing mode.

The utility currently supports the following firmware types:

- ▶ xSeries system BIOS code

- ▶ Remote Supervisor Adapter I firmware
- ▶ Remote Supervisor Adapter II firmware

The utility retrieves and modifies user settings from the supported firmware types using its command-line interface. The utility does not update any of the firmware code.

6.2.1 Support list for ASU

ASU currently supports the Remote Supervisor Adapter and Remote Supervisor Adapter II in the following xSeries servers:

- ▶ x235
- ▶ x255
- ▶ x335
- ▶ x345
- ▶ x440 (single-node configuration only)
- ▶ x445 (single-node configuration only)

ASU also supports these blade servers:

- ▶ BladeCenter HS20 Type 8678
- ▶ BladeCenter HS20 Type 8832

Note: Multinode configurations of the x440 and x445 are not supported.

For a current list of supported servers, see one of the ASU download pages, such as the one for Windows:

<http://www.ibm.com/pc/support/site.wss/MIGR-55019.html>

6.2.2 Supported platforms for ASU

ASU supports the following operating systems:

- ▶ Windows NT® 4.0, Windows 2000, Windows XP, and Windows Server 2003
- ▶ Red Hat Linux 7.x, 8.x, and 9
- ▶ Red Hat Enterprise Linux AS 2.1, Red Hat Enterprise Linux 3.0

Note: For Red Hat Enterprise Linux 3.0, Red Hat 9, and other Linux distributions that do not install the compatibility libstdc++ library, the following message might be displayed:

```
./asu: error while loading shared libraries:  
libstdc++-libc6.1-1.so.2: cannot open shared object file: No such  
file or directory.
```

If you see this message, install the compat-libstdc++*.rpm that is included on the distribution media.

- ▶ SUSE LINUX 7.x, 8.x, and 9
- ▶ SUSE LINUX Enterprise Server 8
- ▶ PC-DOS: 7.0 or later

The ASU is run on the server that contains the settings you want to view and change. When modifying any parameters, you will need root (Linux) or administrator (Windows) access.

To view and change RSA or RSA II settings, the RSA or RSA II device drivers are used and therefore must be installed. You can download the RSA and RSA II device drivers for your system from:

<http://www.pc.ibm.com/support>

Notes: Read over the following notes:

1. You cannot use the utility to view or configure RSA or RSAII settings from any operating system that does not have a supported device driver. For details on which device drivers are supported refer to ServerProven site:
<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>
2. You cannot use the utility to configure RSA or RSAII settings from PC-DOS because there is no RSA or RSA II device driver for PC-DOS.
3. You can view or change settings on a local server only. However, you can in conjunction with IBM Director to run it remotely. See 7.7, "How to use ASU remotely" on page 253.

6.2.3 Downloading ASU and definition files

The base ASU utility can be downloaded from the following locations

Windows	http://www.ibm.com/pc/support/site.wss/MIGR-55019.html
Linux:	http://www.ibm.com/pc/support/site.wss/MIGR-55020.html
PC-DOS:	http://www.ibm.com/pc/support/site.wss/MIGR-55021.html

Definition files are the way the ASU utility is extended to be able to configure specific servers and the Remote Supervisor Adapter. These files are available for the Remote Supervisor Adapter and supported servers from the following links:

RSA I / RSAII:	http://www.ibm.com/pc/support/site.wss/MIGR-55027.html
HS20 (8678):	http://www.ibm.com/pc/support/site.wss/MIGR-56860.html
HS20 (8832):	http://www.ibm.com/pc/support/site.wss/MIGR-56555.html
x235:	http://www.ibm.com/pc/support/site.wss/MIGR-55803.html
x255:	http://www.ibm.com/pc/support/site.wss/MIGR-56393.html
x335:	http://www.ibm.com/pc/support/site.wss/MIGR-55804.html
x345:	http://www.ibm.com/pc/support/site.wss/MIGR-55778.html
x440 (8-Way):	http://www.ibm.com/pc/support/site.wss/MIGR-56858.html
x445:	http://www.ibm.com/pc/support/site.wss/MIGR-55944.html

6.2.4 Using the ASU definition files

The ASU requires a definition file (patch) for each firmware type. The application of the definition file modifies the ASU utility so it will work with the specific hardware. You cannot use the ASU utility until a definition file for that firmware type is applied. A single definition file adds support for one of the following firmware settings:

- ▶ A single BIOS version on a server
- ▶ The RSA or RSA II on any server

An ASU definition file simply informs the ASU where the settings are located for a single BIOS version or RSA or RSA II firmware so it knows how to apply the settings. The definition file adds data to the end of the utility executable. You can either add or remove the definition file from the ASU, and you can add any number of definition files.

Figure 6-1 on page 164 shows how definition files are added to the ASU binary code. To add a definition to the ASU utility, download the appropriate definition, extract the .def file (use `unzip` for Linux), and issue the following command to add the definition:

Windows: `asu patchadd <definition file>.def`
DOS: `asu patchadd <definition file>.def`
Linux: `./asu patchadd <definition file>.def`

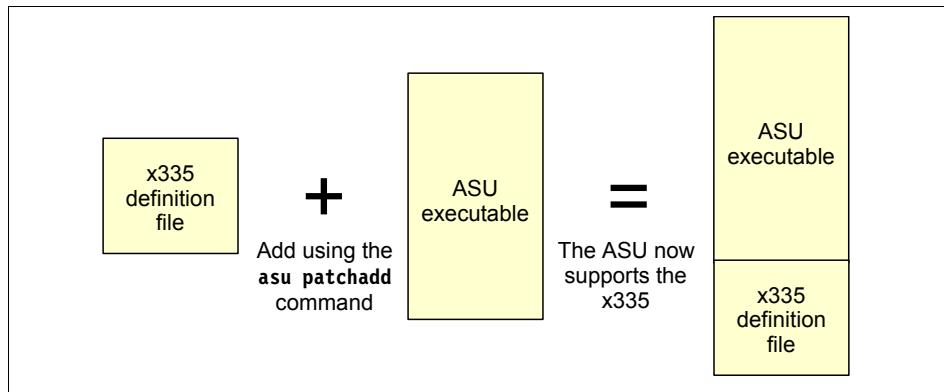


Figure 6-1 Adding x335 definitions to the ASU executable

When ASU runs, it automatically scans the patches that have been applied to it and determines if the applicable definition file exists for the setting that you want. If an applicable definition file exists, the utility applies the setting. If the definition file does not exist, ASU returns an error.

6.2.5 Using the ASU command

You must install the applicable definition files to update ASU files before using the **asu** command, and you must type the ASU commands from the directory in which the utility files are located. The syntax of the ASU command is:

- ▶ Windows: **asu [command] [setting] [value]**
- ▶ Linux: **./asu [command] [setting] [value]**

In the following list of commands, *setting* is the parameter that you want to view or change, and *value* is the value that you are placing on the parameter. If *value* contains spaces, enclose the value string with quotation marks.

ASU available commands and their syntax are listed in Table 6-3.

Tip: The **-v** option lets you specify verbose mode, which provides more detail in the output.

Table 6-3 Available ASU commands and their syntax

ASU command	Function	Syntax
(no command)	Show all the ASU commands and options.	No parameters

ASU command	Function	Syntax
batch <filename>	Execute multiple commands. See 6.2.8, “ASU batch commands” on page 174.	batch <filename> Where <filename> is the text file containing various ASU commands.
comparedefault	Compares current values to default values for one or all settings.	comparedefault [all <CMOS setting>] [-v]
dump	Show RAW CMOS settings.	dump
help	View the online help for one or all settings. For BIOS settings, the help information is the same help that you access when you press F1 during setup.	help [all <CMOS setting>]
loaddefault	Loads default values for one or all settings.	loaddefault [all <CMOS setting>] [-v]
patchadd	Add support for a particular server or device.	patchadd <.def file> [<patched program>] Where <.def file> is a CMOS definition file taken from a BIOS build, and <patched program> is the filename of the patched program to write.
patchextract	Extracts a definition file from the utility to a patch file. You can patch the extracted definition file to another version of the utility.	patchextract <patch #> <.def file> Where <patch #> is the index output by the patchlist command, and <.def file> is the file you wish to create.
patchlist	Displays the definition files that are currently applied.	No parameters
patchremove	Removes a definition file.	patchremove <patch #> [<unpatched program>] Where <patch #> is the index output by the patchlist command and <unpatched program> is the filename of the unpatched program to write.
rebootrsa	Restart the service processor. This is useful when you must restart a Remote Supervisor Adapter to bring into effect any configuration changes.	No parameters
resetrsa	Reset the RSAI/RSAII back to defaults.	No parameters

ASU command	Function	Syntax
replicate	Use the output of one or more show commands to set multiple settings at the same time.	replicate <filename> Where <filename> is a file created by piping output from the show command.
set	Change the value of a setting.	set <CMOS setting> <value> [-v] Where <value> is a string shown from showvalues .
show	Display the current value of one or all settings.	show [all <CMOS setting>] [-v]
showdefault	Display the default value for one or all settings.	showdefault [all <CMOS setting>] [-v]
showvalues	List all possible values for one or all settings. This is useful for finding the value parameter used for the set command.	showvalues [all <CMOS setting>] [-v]
version	Display the version and build date of the utility.	No parameters

6.2.6 Using ASU to view a systems setting

To show the current values of a particular system, type the following command:

```
asu show all
```

You will see the following output appear. In this example we have used the xSeries 345 with the RSAII adapter installed. This output will differ for each server configuration.

Tip: To view all these details more easily you can pipe the command to a text file, for example:

```
asu show all > showall.txt
```

This will give you a quick reference of all the available CMOS or RSA/RSA II settings. Example 6-1 shows a example of this output.

Note: This output is not sorted alphabetically.

Example 6-1 Sample output from ASU running on an x345 with an RSA II installed

```
CMOS_DisketteA=1.44 MB 3.5"
```

```
CMOS_CRTRequired=Enabled
```

```
CMOS_KbdRequired=Enabled
CMOS_UsbLegacy=Enabled
CMOS_HD_Auto1=Autoconfigure
CMOS_HD_Auto0=Autoconfigure
CMOS_PrimaryBootDevice4=Network
CMOS_PrimaryBootDevice3=Hard Disk 0
CMOS_PrimaryBootDevice2=Diskette Drive 0
CMOS_PrimaryBootDevice1=CD ROM
CMOS_AlternateBootDevice4=Hard Disk 0
CMOS_AlternateBootDevice3=CD ROM
CMOS_AlternateBootDevice2=Diskette Drive 0
CMOS_AlternateBootDevice1=Network
CMOS_NumLock=Off
CMOS_PS2Mouse=Installed
CMOS_UserPwdChange>No
CMOS_ServerMode=On
CMOS_FloppyRequired=Enabled
CMOS_PostBootFailRequired=Enabled
CMOS_MappingPref=Enabled
CMOS_PerfPref=Yes
CMOS_Remap>No
CMOS_MemoryRow0Disable=Row Is Enabled
CMOS_MemoryRow1Disable=Row Is Enabled
CMOS_MemoryRow2Disable=Row Is Enabled
CMOS_MemoryRow3Disable=Row Is Empty
CMOS_UserPrefInterleave=2 Way Interleaved
CMOS_DisketteController=Enabled
CMOS_Parallel=Disabled
CMOS_ParallelMode=Standard
CMOS_ParallelIRQ=IRQ 7
CMOS_ParallelDMA=DMA 1
CMOS_StopOnError=Disabled
CMOS_ENET1_PLANAR_ENABLE=Enabled
CMOS_SCSI_PLANAR_ENABLE=Enabled
CMOS_Slot1_ENABLE=Enabled
CMOS_Slot2_ENABLE=Enabled
CMOS_Slot3_ENABLE=Enabled
CMOS_Slot4_ENABLE=Enabled
CMOS_Slot5_ENABLE=Enabled
CMOS_SerialB=Disabled
CMOS_SPVD=Hidden
CMOS_RemoteConsoleEnable=Disabled
CMOS_RemoteConsoleComPort=COM 1
CMOS_RemoteConsoleBaud=9600
CMOS_RemoteConsoleDataBits=8
```

```
CMOS_RemoteConsoleParity=None
CMOS_RemoteConsoleStopBits=1
CMOS_RemoteConsoleEmulation=ANSI
CMOS_RemoteConsoleBootEnable=Disabled
CMOS_Serial1A=Port 3F8, IRQ 4
CMOS_ENET_PXE_ENABLE=Planar Ethernet 1
CMOS_PciUsbIrqValue=Autoconfigure
CMOS_PciSCSIAIntAValue=Autoconfigure
CMOS_PciSCSIBIntAValue=Autoconfigure
CMOS_PciVideoIntAValue=Autoconfigure
CMOS_PciEnetIntAValue=Autoconfigure
CMOS_PciEnetBIntAValue=Autoconfigure
CMOS_PciSlot1IntACValue=Autoconfigure
CMOS_PciSlot1IntBDValue=Autoconfigure
CM_VIRUS_DETECT=Disabled
CMOS_JacksonTechnology=Enabled
CMOS_INT_19H=Enabled
CMOS_PciSlot2IntAValue=Autoconfigure
CMOS_PciSlot2IntBValue=Autoconfigure
CMOS_PciSlot2IntCValue=Autoconfigure
CMOS_PciSlot2IntDValue=Autoconfigure
CMOS_PciSlot3IntACValue=Autoconfigure
CMOS_PciSlot3IntBDValue=Autoconfigure
CMOS_PciSlot4IntACValue=Autoconfigure
CMOS_PciSlot4IntBDValue=Autoconfigure
CMOS_PciSlot5IntACValue=Autoconfigure
CMOS_PciSlot5IntBDValue=Autoconfigure
CMOS_PCIMLT1=40h
CMOS_PCIBootPriority=Planar SCSI
CMOS_PrefetchQueue=Enabled
CMOS_SystemCacheType=Write Back
CMOS_SPRebootOnNMI=Enabled
CMOS_ThresholdLockout=5
CMOS_WakeOnLAN=Enabled
CMOS_IDEControllerPrimary=Enabled
CMOS_DHCPControl=Use Static IP
CMOS_OSUSBControl=Other OS
CMOS_RemoteConsoleKybdEmul=ANSI
CMOS_RemoteConsoleFlowCtrl=Disabled
CMOS_ENET_PXE_PRIORITY=High
CMOS_LoopOnBootSequence=Disabled
CMOS_PeriodicSMI=Enabled
CMOS_HD_Mode1=PIO mode 0
CMOS_HD_Mode0=PIO mode 0
RSA_Network1=Enabled
```

```
RSA_LANDataRate1=Auto
RSA_Duplex1=Auto
RSA_DHCP1=Disabled
RSA_PPAuthProt1=PAP Only
RSA_Network2=Disabled
RSA_DHCP2=Disabled
RSA_ModemBaudRate1=57600
RSA_ModemParity1=None
RSA_ModemStopBits=1
RSA_SerialRedirectionPort1=Disabled
RSA_SerialRedirectionCLIMode1=CLI disabled
RSA_SerialRedirectionNoAuthentication1=Require authentication
RSA_SerialRedirectionPort2=Enabled
RSA_SerialRedirectionCLIMode2=CLI active / EMS compatible keystroke
sequences
RSA_SerialRedirectionNoAuthentication2=Require authentication
RSA_LinkSerialPort1And2=Disabled
RSA_LoginFlags1=Read/Write, Dial back disabled
RSA_LoginFlags2=Read/Write, Dial back disabled
RSA_LoginFlags3=Read Only, Dial back disabled
RSA_LoginFlags4=Read Only, Dial back disabled
RSA_LoginFlags5=Read Only, Dial back disabled
RSA_LoginFlags6=Read Only, Dial back disabled
RSA_LoginFlags7=Read Only, Dial back disabled
RSA_LoginFlags8=Read Only, Dial back disabled
RSA_LoginFlags9=Read Only, Dial back disabled
RSA_LoginFlags10=Read Only, Dial back disabled
RSA_LoginFlags11=Read Only, Dial back disabled
RSA_LoginFlags12=Read Only, Dial back disabled
RSA_TemperatureAlert=Disabled
RSA_VoltageAlert=Disabled
RSA_TamperAlert=Disabled
RSA_MultipleFanFailureAlert=Disabled
RSA_PowerFailureAlert=Disabled
RSA_HardDriveAlert=Disabled
RSA_VRMFailureAlert=Disabled
RSA_RedundantPowerTriggeredAlert=Disabled
RSA_OneFanFailureAlert=Disabled
RSA_NonCriticalTemperatureAlert=Disabled
RSA_NonCriticalVoltageAlert=Disabled
RSA_POSTHangAlert=Disabled
RSA_OSHangAlert=Disabled
RSA_ApplicationLoggedErrorAlert=Disabled
RSA_SystemPowerOffAlert=Disabled
RSA_SystemPowerOnAlert=Disabled
```

```
RSA_SystemBootFailureAlert=Disabled  
RSA_LoaderWatchdogFailureAlert=Disabled  
RSA_PFAAlert=Disabled  
RSA_PartitionNotificationAlert=Disabled  
RSA_NetworkChangeNotificationAlert=Disabled  
RSA_AlertRecipientStatus1=Invalid  
RSA_AlertRecipientNotificationMethod1=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly1=Disabled  
RSA_AlertRecipientStatus2=Invalid  
RSA_AlertRecipientNotificationMethod2=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly2=Disabled  
RSA_AlertRecipientStatus3=Invalid  
RSA_AlertRecipientNotificationMethod3=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly3=Disabled  
RSA_AlertRecipientStatus4=Invalid  
RSA_AlertRecipientNotificationMethod4=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly4=Disabled  
RSA_AlertRecipientStatus5=Invalid  
RSA_AlertRecipientNotificationMethod5=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly5=Disabled  
RSA_AlertRecipientStatus6=Invalid  
RSA_AlertRecipientNotificationMethod6=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly6=Disabled  
RSA_AlertRecipientStatus7=Invalid  
RSA_AlertRecipientNotificationMethod7=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly7=Disabled  
RSA_AlertRecipientStatus8=Invalid  
RSA_AlertRecipientNotificationMethod8=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly8=Disabled  
RSA_AlertRecipientStatus9=Invalid  
RSA_AlertRecipientNotificationMethod9=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly9=Disabled  
RSA_AlertRecipientStatus10=Invalid  
RSA_AlertRecipientNotificationMethod10=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly10=Disabled  
RSA_AlertRecipientStatus11=Invalid  
RSA_AlertRecipientNotificationMethod11=Numeric pager  
RSA_AlertRecipientCriticalAlertsOnly11=Disabled  
RSA_AlertRecipientStatus12=Enabled  
RSA_AlertRecipientCriticalAlertsOnly12=Disabled  
RSA_POSTWatchdog=Disabled  
RSA_OSWatchdog=Disabled  
RSA_LoaderWatchdog=Disabled  
RSALogFullNotification=75% Full Enabled, 100% Full Enabled  
RSA_HostIPAddress1=9.42.171.238
```

```
RSA_GatewayIPAddress1=9.42.171.3
RSA_PPPIPAddress1=0.0.0.0
RSA_HostIPSubnet1=255.255.255.0
RSA_DHCPAssignedHostIP1=0.0.0.0
RSA_DHCPAssignedGateway1=0.0.0.0
RSA_DHCPAssignedNetMask1=0.0.0.0
RSA_DHCPAssignedDHCPServer1=0.0.0.0
RSA_DHCPAssignedPrimaryDNS1=0.0.0.0
RSA_DHCPAssignedSecondaryDNS1=0.0.0.0
RSA_DHCPAssignedTertiaryDNS1=0.0.0.0
RSA_HostIPAddress2=192.96.1.1
RSA_GatewayIPAddress2=0.0.0.0
RSA_PPPIPAddress2=255.255.255.255
RSA_HostIPSubnet2=255.255.255.255
RSAString_HostName1=ASMA00096B9E085C
RSAString_HostName2=
RSAString_LoginId1=USERID
RSAString_LoginId2=leitenberger
RSAString_LoginId3=
RSAString_LoginId4=
RSAString_LoginId5=
RSAString_LoginId6=
RSAString_LoginId7=
RSAString_LoginId8=
RSAString_LoginId9=
RSAString_LoginId10=
RSAString_LoginId11=
RSAString_LoginId12=
RSAString_Password1=
RSAString_Password2=
RSAString_Password3=
RSAString_Password4=
RSAString_Password5=
RSAString_Password6=
RSAString_Password7=
RSAString_Password8=
RSAString_Password9=
RSAString_Password10=
RSAString_Password11=
RSAString_Password12=
RSAString_AlertRecipientName1=
RSAString_AlertRecipientNumber1=
RSAString_AlertRecipientAlphanumericPIN1=
RSAString_AlertRecipientEmailAddress1=
RSAString_AlertRecipientPPPLogin1=
```

```
RSAString_AlertRecipientPPPPassword1=
RSAString_AlertRecipientName2=
RSAString_AlertRecipientNumber2=
RSAString_AlertRecipientAlphanumericPagerPIN2=
RSAString_AlertRecipientEmailAddress2=
RSAString_AlertRecipientPPPLlogin2=
RSAString_AlertRecipientPPPpassword2=
RSAString_AlertRecipientName3=
RSAString_AlertRecipientNumber3=
RSAString_AlertRecipientAlphanumericPagerPIN3=
RSAString_AlertRecipientEmailAddress3=
RSAString_AlertRecipientPPPLlogin3=
RSAString_AlertRecipientPPPpassword3=
RSAString_AlertRecipientName4=
RSAString_AlertRecipientNumber4=
RSAString_AlertRecipientAlphanumericPagerPIN4=
RSAString_AlertRecipientEmailAddress4=
RSAString_AlertRecipientPPPLlogin4=
RSAString_AlertRecipientPPPpassword4=
RSAString_AlertRecipientName5=
RSAString_AlertRecipientNumber5=
RSAString_AlertRecipientAlphanumericPagerPIN5=
RSAString_AlertRecipientEmailAddress5=
RSAString_AlertRecipientPPPLlogin5=
RSAString_AlertRecipientPPPpassword5=
RSAString_AlertRecipientName6=
RSAString_AlertRecipientNumber6=
RSAString_AlertRecipientAlphanumericPagerPIN6=
RSAString_AlertRecipientEmailAddress6=
RSAString_AlertRecipientPPPLlogin6=
RSAString_AlertRecipientPPPpassword6=
RSAString_AlertRecipientName7=
RSAString_AlertRecipientNumber7=
RSAString_AlertRecipientAlphanumericPagerPIN7=
RSAString_AlertRecipientEmailAddress7=
RSAString_AlertRecipientPPPLlogin7=
RSAString_AlertRecipientPPPpassword7=
RSAString_AlertRecipientName8=
RSAString_AlertRecipientNumber8=
RSAString_AlertRecipientAlphanumericPagerPIN8=
RSAString_AlertRecipientEmailAddress8=
RSAString_AlertRecipientPPPLlogin8=
RSAString_AlertRecipientPPPpassword8=
RSAString_AlertRecipientName9=
RSAString_AlertRecipientNumber9=
```

```
RSAString_AlertRecipientAlphanumericPagerPIN9=
RSAString_AlertRecipientEmailAddress9=
RSAString_AlertRecipientPPPLogin9=
RSAString_AlertRecipientPPPPassword9=
RSAString_AlertRecipientName10=
RSAString_AlertRecipientNumber10=
RSAString_AlertRecipientAlphanumericPagerPIN10=
RSAString_AlertRecipientEmailAddress10=
RSAString_AlertRecipientPPPLogin10=
RSAString_AlertRecipientPPPPassword10=
RSAString_AlertRecipientName11=
RSAString_AlertRecipientNumber11=
RSAString_AlertRecipientAlphanumericPagerPIN11=
RSAString_AlertRecipientEmailAddress11=
RSAString_AlertRecipientPPPLogin11=
RSAString_AlertRecipientPPPPassword11=
RSAString_AlertRecipientName12=X345DIRSERVR
RSAString_AlertRecipientNumber12=9.42.171.237
RSAString_AlertRecipientAlphanumericPagerPIN12=
RSAString_AlertRecipientEmailAddress12=
RSAString_AlertRecipientPPPLogin12=
RSAString_AlertRecipientPPPPassword12=
RSAKeystroke_EnterCLISquence='ESC' '(
RSAKeystroke_ExitCLISquence='ESC' 'Q'
```

6.2.7 Using ASU to configure RSA or RSA II settings

You can use ASU to directly configure an RSA or RSA II. Be sure to install the RSA/RSA II definition files and device driver before using the utility. To install the device driver, see 3.4.4, “Installing the device driver” on page 64.

Example: Configuring the IP address settings of the RSA II

The RSA II requires configuring to enable remote access to the adapter through the adapter’s Ethernet connectors. This is how you can perform this from the command line using ASU.

Note: If you are using a Linux operating system be sure to type `./` before `asu`.

On the server, from the directory where the ASU utility has been unpacked and patched with the appropriate definition files, we entered the following commands:

- ▶ `asu show RSA_HostIPAddress1`

Displays the value of the service processor's IP address. Output we received from this command:

```
RSA_HostIPAddress1=9.42.171.238
```

- ▶ **asu showvalues RSA_HostIPAddress1**

Displays all possible value types. Output we received is:

```
RSA_HostIPAddress1=x.x.x.x where (x is 0-255)
```

- ▶ **asu set RSA_HostIPAddress1 xxx.xxx.xxx.xxx**

Changes the value of the IP address to the one we specified.

- ▶ **set RSA_DHCP1 disabled**

Disable DHCP and use the static address.

To set other parameters see the list of them in Example 6-1 on page 166.

Other relevant parameters to set include:

```
RSA_Network1 enabled|disabled
```

```
RSA_HostIPsubnet1 xxx.xxx.xxx.xxx
```

```
RSA_GatewayIPAddress1 xxx.xxx.xxx.xxx
```

```
RSA_KLANDataRAte1 "100M Ethernet"
```

```
RSA_Duplex1 Half|Full|Auto
```

- ▶ **asu rebootrsa**

Restart the RSA once you have completed, so that the configuration changes can take effect.

- ▶ **exit**

Exit the ASU utility.

6.2.8 ASU batch commands

The ASU **batch** command lets you write scripts for utility operations. The script file syntax is independent of the operating system.

The syntax of the batch command is **asu batch commandfile**, where *commandfile* is the name of a file that contains a list of **asu** commands.

Tip: Do not include **asu** at the beginning of each line in the command file.

When using the batch command on a batch file, the output sent to stdout and stderr will be the collective output of all the commands in the batch file. The output of each command in the batch file will be preceded by the **asu** command, surrounded by square brackets, as shown in Example 6-2 on page 175.

Example 6-2 Layout of the stdout from the asu batch command

```
[command1]
output of command 1
[command 2]
output of command 2
.
[command n ]
output of command n
```

For example, our command file, showboot.txt, contains the following lines (Example 6-3).

Example 6-3 Command file showboot.txt

```
show CMOS_PrimaryBootDevice1
show CMOS_PrimaryBootDevice2
show CMOS_PrimaryBootDevice3
show CMOS_PrimaryBootDevice4
```

When we issue the following command we will see the output listed in Example 6-4.

```
asu batch showboot.txt
```

Example 6-4 Output from showboot.txt in batch mode

```
[show CMOS_PrimaryBootDevice1]
CMOS_PrimaryBootDevice1=CD ROM
[show CMOS_PrimaryBootDevice2]
CMOS_PrimaryBootDevice2=Diskette Drive 0
[show CMOS_PrimaryBootDevice3]
CMOS_PrimaryBootDevice3=Hard Disk 0
[show CMOS_PrimaryBootDevice4]
CMOS_PrimaryBootDevice4=Network
```

For example scenarios using ASU see 7.6, “Resetting the RSA II back to factory defaults” on page 248, and 7.7, “How to use ASU remotely” on page 253.

6.3 Management processor command-line interface

The IBM management processor command-line interface, or MPCLI, is a management tool for xSeries servers running Windows or Linux. The system management functions are provided from a command-line interface (CLI) that connects to the service processor in the server.

Using this CLI, you can access and set a wide range of information about the health, configuration, communication, and state of your system. These functions are immediately available after you install the CLI and make a connection to the service processor.

You can use the MPCLI on a remote server provided you know the IP address of the remote service processor and have a valid user ID and password. There are three supported methods that you can use to communicate with a service processor:

- ▶ In-band communication using a device driver
- ▶ Out-of-band communication using an IP connection
- ▶ Out-of-band communication using an RS-485 interconnect

6.3.1 Supported service processor configurations

The MPCLI is supported only on systems with at least one of the following service processors:

- ▶ Advanced System Management processor
- ▶ ASM PCI Adapter
- ▶ Integrated system management processor
- ▶ BladeCenter management module
- ▶ Remote Supervisor Adapter
- ▶ Remote Supervisor Adapter II

Restriction: The Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II-EXA are currently not supported by the MPCLI.

You must also ensure that the combination of service processor and server is supported. This information is listed in Table 6-4 on page 177.

Additionally, the table lists the different levels of support available, depending on your service processor configuration. The table has the following entries:

- ▶ Full: Supports any function available in the server relating to the system-management hardware.
- ▶ Compatible: Supports current functions of the command-line interface. There are no plans to support new functions added to the server or command-line interface.
- ▶ SP config: Service processor configuration. Supports service processor configuration only. This is because the service processor cannot access the system hardware.
- ▶ No support: The MPCLI is not support with this configuration.

- ▶ (blank cell with grey shading): This server does not support this particular service processor so the support statement is not applicable.

Table 6-4 lists the supported configurations of servers and service processors.

Note: The table does not list the support for the ASM PCI Adapter.

For information on the supported configurations for Netfinity servers and the newer xSeries servers refer to the list of supported servers:

<http://www.ibm.com/pc/support/site.wss/MIGR-54216.html>

The list of supported servers is also listed in the latest MPCLI User Guide available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>

Table 6-4 MPCLI supported configurations

xSeries server	ISMP	BMC	ASMP	RSA	RSA II	BCMM
xSeries 220				Compatible		
xSeries 225				Compatible	No support	
xSeries 230			Compatible			
xSeries 232	Compatible			Compatible		
xSeries 235	Compatible			No support	Compatible	
xSeries 236		No support				
xSeries 240			Compatible			
xSeries 250			Compatible			
xSeries 255	Compatible			Compatible	Compatible	
xSeries 305				SP config	No support	
xSeries 306					No support	
xSeries 330			Compatible	Compatible		
xSeries 335	Compatible			No support	Compatible	
xSeries 336		No support				
xSeries 340			Compatible			
xSeries 342	Compatible			Compatible		

xSeries server	ISMP	BMC	ASMP	RSA	RSA II	BCMM
xSeries 345	Compatible			Full	Compatible	
xSeries 346		No support				
xSeries 350			Compatible			
xSeries 360				Full		
xSeries 365					No support	
xSeries 366		No support				
xSeries 440				Full		
xSeries 445				Full		
xSeries 450				Compatible		
xSeries 455				Full		
BC MM						Full
HS20	No support					Full
HS40	No support					Full

6.3.2 Functions

The MPCLI has the following functions:

- ▶ Querying of vital product data (VPD) for system components:
 - BladeCenter units, including switch modules
 - Cache coherency
 - Chassis/enclosure
 - CPU and CPU EEPROM
 - Diagnostics
 - Hard disk drive backplane and system board
 - DIMMs
 - Power supply and backplane
 - Service processor device driver, firmware, and hardware revision
 - System slot
 - POST/BIOS
- ▶ Querying the component LEDs using light path diagnostics:
 - BladeCenter units
 - CD-ROM drive and hard disk drive cables
 - Centerplane, memory, and adapters

- Chip and chip set VRMs
- CPUs and CPU cache
- Diagnostics and front panel
- Expansion device, fan, scalability ports, system board, and VRM
- Memory, memory hot-plug enable, and memory subsystem
- PCI bus and PCI adapters
- Service processor adapter and slot
- ▶ Viewing and changing service processor configurations:
 - Restart
 - Network interfaces: SNMP, PPP, and IP
 - Serial port hardware and software
 - General identification
 - VPD
 - Internal clock
 - Alert dial-out settings
 - Dial-in entries
- ▶ Viewing event logs:
 - BIOS
 - Diagnostics
 - POST
 - Service processor
- ▶ Querying or setting server time-outs for your systems:
 - Operating-system loader
 - Operating-system heartbeat
 - POST
 - Power-off delay
- ▶ Viewing health and environment information for your systems:
 - System board voltages and thresholds
 - VRM voltages
 - Power-supply voltages
 - Component temperatures and thresholds
- ▶ Ability to remotely turn systems on and off:
 - Turn off immediately and with operating-system shutdown.
 - Restart immediately and with operating-system shutdown.
 - Turn on immediately, after a specified delay, and in n seconds.
- ▶ Querying the general state information for your systems:
 - System state stable or unstable
 - System power on or off
 - Number of times restarted
 - Number of hours turned on

- Universal unique ID (UUID)
- Blue indicator light on or off
- Light path LED functioning
- ▶ Create scripts that contain multiple commands for you to use and reuse.
When you run a script, each command within it is run.
- ▶ Ability to configure:
 - LDAP
 - Serial over LAN (SOL)
 - The serial port
 - The command mode interface
- ▶ Granular authorities:
 - Ability to reset HTTP.
 - Ability to verify the availability of the command mode port.
 - Ability to get and set the host operating system.
 - Ability to retrieve Management Module chassis VPD.
 - Ability to retrieve processor blade assemblies. Blade assemblies represent a single combined unit that a user would add or remove from the processor slots.

6.3.3 Limitations

The MPCLI has the following limitations under Linux:

- ▶ You cannot change the default location of the installation from the /opt/IBMmpcli/ directory.
- ▶ You cannot use the Up Arrow and Down Arrow keys to recall a command after you start the CLI.

6.3.4 Supported platforms for the MPCLI

MPCLI is supported on the following platforms:

- ▶ Red Hat 2.1 AS, WS, ES
- ▶ Red Hat 3.0 AS, WS, ES
- ▶ SUSE LINUX Enterprise Server 8.0 (SP3)
- ▶ Microsoft Windows 2000 Server (SP3 or later)
- ▶ Microsoft Windows 2000 Professional (SP3 or later)
- ▶ Microsoft Windows 2000 AS (SP3 or later)
- ▶ Microsoft Windows XP Professional (SP1 or later)
- ▶ Microsoft Windows Server 2003, Standard Edition
- ▶ Microsoft Windows Server 2003, Enterprise Edition

For the latest supported operating system platforms refer to the *MPCLI User's Guide*, available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>

6.3.5 Installing the MPCLI

This section describes how to install the MPCLI on both Windows and Linux platforms.

Download the MPCLI from:

<http://www.ibm.com/pc/support/site.wss/MIGR-54216.html>

Both the Windows and Linux versions are available from here.

Installing on a Windows operating system

You can install the command-line interface using the InstallShield wizard, or you can perform an unattended installation.

Installing using InstallShield is just like any other standard Windows installation.

To perform an unattended (silent) installation, download the install program from the above URL to a temporary directory, then issue the following command to install the MPCLI:

```
26r0684.exe /S /v/qn
```

Note that you will not receive any message that the installation was completed successfully.

Once it is installed, to start the MPCLI, click **Start** → **Programs** → **IBM** → **MPCLI**.

Installing on a Linux operating system

Before you begin the installation, note the following information:

- ▶ There is no upgrade path from V1 or V2 to V3. You must uninstall any previous installation by typing the following command at a shell prompt:
`rpm -e mpcli`
- ▶ If you are not the root user or a member of the root user group, you might not be able to install or uninstall the command-line interface.

To install the MPCLI, issue the following command from a shell prompt:

```
rpm -ivh mpcli-2.0-1.0.i386.rpm
```

Once the installation is completed, begin using the MPCLI by typing the following command:

```
/opt/IBMmpcli/bin/MPCLI.bsh
```

You will need to be either the root user or a member of the root user group. If an error is returned when you start the MPCLI, the script file may not have execute permissions. To add execute permissions, type chmod +x MPCLI.bsh at a shell prompt.

6.3.6 Using the MPCLI

Note: For remote management using MPCLI you will need to know the service processor's login credentials:

- ▶ IP address
- ▶ User ID
- ▶ Password

To start the MPCLI under Windows, click **Start** → **Programs** → **IBM** → **MPCLI**. Under Linux, enter the command:

```
/opt/IBMmpcli/bin/MPCLI.bsh
```

You will then see the MPCLI prompt ready to accept your commands:

```
mp>
```

Under Linux, you must be either the root user or a member of the root user group.

With MPCLI, you can manage and monitor system health and configuration by logging on to a service processor on a system or connected to a system, query for information about system status, or set parameters for system behavior.

Command syntax

All commands have the following basic structure:

```
command -option parameter
```

You can add multiple options to a command on one line to avoid repeating the same command, for example:

```
command -option1 parameter -option2 parameter -option3 parameter
```

The information for each option is returned in the order in which it was entered and displayed on separate lines.

Key syntax rules include the following:

- ▶ All commands and options are in lowercase and are case sensitive. Boolean parameters (true and false) and string parameters are not case-sensitive, however.
- ▶ String parameters that contain spaces should be enclosed in double quotation marks, as in “Lesley Bain”. The maximum string length is 15 characters, including spaces. String values over 15 characters long are truncated.

Tip: MPCLI V3 also supports the SMASH command-line protocol (CLP) syntax. The *MPCLI User’s Guide* describes the specific SMASH commands supported. For details about SMASH, see:

<http://www.dmtf.org/standards/smash>

Known issues

The following command-line interface issues currently exist:

- ▶ If you are logged on to a remote service processor using an RS-485 interconnect, your connection might be lost after a period of inactivity.
- ▶ When using the **setmpclock -gmtoffset** command, if you attempt to use an invalid parameter outside the range of -12 to +12, a message indicating that the command was successful might be displayed, even though the command was unsuccessful.
- ▶ If you are logged on to a Remote Supervisor Adapter and running the command-line interface, and then fail at logging on to an integrated system management processor on an RS-485 interconnect, the command-line interface might lose all functionality. You must restart the command-line interface and log on again.
- ▶ When using the **setsmmnetwork** command, if you make changes using any of the options, they remain in a pending state even if the **setsmmnetwork -enable** command is set to true, which should apply the pending changes. Instead, typing **setsmmnetwork -enable true** might return a message indicating that there was a problem sending the command.
- ▶ For x455 servers, the **logonlocal** command is not supported.
- ▶ On processor blades in an IBM BladeCenter, the management module must be restarted before a text ID changed is applied. Whenever the **setmpid** command is used on a blade server, it must be followed by a **restarttmp** command to the blade server.
- ▶ For ASM service processors, the **getvpd -postbios** and **getlightpath** commands report incorrect errors and are not supported.

Logging into a service processor

The first task before you can begin to use the MPCLI is to log into the service processor you want to manage. There are a number of ways to perform this task:

Important: Multiple logins to other service processors are allowed; however, all commands that are issued affect the most recently accessed service processor, until another service processor is accessed.

- ▶ Log on to the local service processor by entering the command:

```
logonlocal
```

- ▶ Log on out-of-band via the Ethernet network, specifying the address, user ID, and password:

```
logonip -hostname hostname -userid userid -password password
```

For example:

```
| logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
```

- ▶ Log on out-of-band via the ASM interconnect network (RS-485).

Before logging on to a service processor via the RS-485 connection, you must first connect to the gateway service processor using **logonlocal** or **logonip**.

Once you have logged on to the gateway device, issue the following command to display a list of the other service processors attached via RS-485:

```
logonrs485 -query
```

Using the results from the **query** command, you can then connect to the remote service processor by specifying the index number or the name of the remote service processor, as follows:

```
logonrs485 -index RSindex -userid userid -password password  
logonrs485 -name RSname -userid userid -password password
```

Where *RSindex* is the number of the device and *RSname* is the name of the device returned by the **-query** command.

Tip: If you are logging on to an ISM Processor, the **-userid** and **-password** parameters are not required.

- ▶ To log on to the service processor in the RXE-100, use the **logonrxe** command:
 - **logonrxe -query** - Get a list of the RXE-100 expansion units attached to the system.

- **logonrxe -index RXindex** - Log on to an IBM RXE-100 expansion unit by specifying its index from the output of the query command.

To log off from the current session and disconnect from the service processor, enter the following command:

```
logoff
```

The commands

The following commands control the behavior of the MPCLI. They affect the output and function of the application, but do not directly affect the service processor.

Table 6-5 Meta commands to control the behavior of the MPCLI

Command	Description
help	Displays the available help commands.
help-cli	Displays the application control log on and log off commands.
help-cmd	Displays all the commands available to use after logging onto a service processor.
help-cmd <i>command</i>	Displays all the commands for the specified command name.
verbose	Toggles debugging information on or off. Debugging provides additional information, such as more detail on a command success or failure. By default verbose is off.
sleep <i>milliseconds</i>	Allows the main execution thread to enter sleep mode for a specified number of milliseconds.
exit	Closes the connection to the service processor and exits the program.
connectionblocks	Toggles the grouping of commands within a logon/logoff block. When connectionsblocks is enabled, if a logon is unsuccessful, all commands will be ignored until a logoff is detected. This feature is primarily used for scripting.

A full description of the MPCLI commands can be found in the *MPCLI User's Guide*, available from the following URL:

<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>

The MPCLI commands can be split into the following groups:

- ▶ Bladecenter Unit commands

These are used to read and configure BladeCenter-supported functions.

- ▶ Network interface commands

These are used to configure network protocols and hardware such as SNMP, PPP, IP, network hardware, DHCP, and DNS.
- ▶ Serial port configuration commands

These are used to enable read and write access to both hardware and software configurations of a serial port.
- ▶ Service processor configuration commands

These enable you to read and set the service processor clock, text IDs, update the firmware, reset to the default configuration, and restart the service processor.
- ▶ Service processor event commands

These can be used to read and change dial-out and dial-in alert configuration settings; read and clear the event log; and also read, enable, or disable alert triggers for the service processor.
- ▶ System power commands

These can be used to read or set system power options such as server time-outs, remote power control, and the preboot execution environment (PXE) reboot.
- ▶ System statistical commands

These display the system statistics (which are maintained by the service processor), set the blue indicator light function, and display light path diagnostics states.
- ▶ System component commands

These provide information about system components that the service processor is monitoring, such as memory, power supplies, hard disk backplanes, and processors.
- ▶ System health and environmental commands

These provide system health and environmental information, such as voltages, temperature, and fan speeds. You can access the current values and thresholds for the system hardware that the service processor is monitoring.

Scripting with the MPCLI commands

You can use scripts instead of typing each command one at a time. For example, to make logging in to a service processor easier, you can create a logon script to avoid repeatedly typing in the host name, user ID, and password.

Scripts are text files, with one command per line. They can have any file name and extension. You can create a script using a text editor or you can create one by putting the MPCLI in record mode using the command:

```
commandfile outputfilename
```

Where *outputfilename* is the fully qualified name of the script file you want to create. To stop recording a script, issue the following command to stop writing script commands:

```
commandfile
```

Once you have created a script, you can call it from within the MPCLI using the following command:

```
inputfile inputfilename
```

Where *inputfilename* is the fully qualified name of the script file you wish to run.

In addition, you can control where the output from the scripted commands is to appear:

- ▶ **outputfile *outputfilename*** - Redirects the output of subsequent commands to the specified file rather than the command window. No further messages appear in the MPCLI window, because all results, even failures, are captured in the output file.
- ▶ **resetoutput** - Returns command output back to the command window from the output file specified in the outputfile command.

MPCLI sample scripts

You can use these scripts by modifying them to suit your needs, or refer to them when you are creating your own scripts. In the following sample scripts, the parameters are examples only; the parameters that you choose to use will be specific to your environment.

Note: You must be logged on to a service processor to operate these commands.

See the *MPCLI User's Guide* for information about these commands.

Get and set network hardware configuration

Figure 6-2 shows the get and set network hardware configuration.

```
outputfile ./enetcfgresults.txt
getmpid
getmpclock
setnethw -interface 1 -enabled false
setdhcp -enabled false
setnethw -interface 1 -linetype "ENET" -enabled true
setip -interface 1 -hostname X
setip -interface 1 -ipaddress 9.67.37.00
setip -interface 1 -subnet 255.255.255.128
setnethw -interface 1 -datarate "AUTO"
setnethw -interface 1 -duplex "AUTO"
setnethw -interface 1 -adminmac "00 00 00 00 00 00"
setnethw -interface 1 -gateway 9.67.37.1
setnethw -interface 1 -enabled true
resetoutput
restartmp
```

Figure 6-2 Script to get and set network hardware configuration

Log onto and get service processor information

Figure 6-3 shows the script to log on to and get SP information.

```
outputfile ./getaccess.txt
logonip -hostname SPbatman -userid gisellem -password s0ngb1rd
getmpid -text
getmpclock -timeanddate
getdialinentry -index 12
logoff
exit
```

Figure 6-3 Script to log on and get SP information

Get service processor information and log

Figure 6-4 on page 189 shows the script to get and log SP information.

```
outputfile ./mplog.txt
getmpid
getmpclock
getmplog -first
getmplog -all
resetoutput
```

Figure 6-4 Script to get and log SP information

Get and set various policies and set start options

Figure 6-5 shows a script to get and set policies and start options in a BladeCenter chassis.

```
getpbpolicy -localpower 2
setpbpolicy -localpower 2,false
getpbpolicy -localpower 2
setpbpolicy -localpowerall true
getpbpolicy -localpower 2
getpbpolicy -localkvm 2
setpbpolicy -localkvm 2,false
getpbpolicy -localkvm 2
setpbpolicy -localkvmall true
getpbpolicy -localkvm 2
getpbpolicy -localusb 2
setpbpolicy -localusb 2,false
getpbpolicy -localusb 2
setpbpolicy -localusball true
getpbpolicy -localusb 2
bootoptions -get 2
bootoptions -set 2,"pxe,cdrom,floppy"
bootoptions -get 2
getkvm
setkvm -owner 2
getkvm
setkvm -park
getkvm
```

Figure 6-5 Script to get and set policies and start options in a BladeCenter chassis

Log on to and flash service processor

Figure 6-6 on page 190 shows a script to log on and flash the service processor over an Ethernet.

```
outputfile ./rsaflash.txt
logonip -hostname 192.168.1.100 -userid gisellem -password s0ngb1rd
getmpid -text
getvpd -mpboot
getvpd -mprom
fwupdate -mn d:\firmware\x220\batman\CNETMNUS.PKT
logoff
sleep 15000
logonip -hostname 192.168.1.100 -userid gisellem -password s0ngb1rd
fwupdate -br d:\firmware\x220\batman\CNETBRUS.PKT
logoff
sleep 15000
logonip -hostname 192.168.1.100 -userid gisellem -password s0ngb1rd
fwupdate -vnc d:\firmware\x220\batman\CNETRGUS.PKT
logoff
exit
```

Figure 6-6 Script to log on and flash the service processor over Ethernet

Log on and create a user ID

Figure 6-7 shows a script to log on and set dial-in configuration.

```
outputfile ./setaccess.txt
logonip -hostname svcprocella -userid gisellem -password s0ngb1rd
getmpid -text
getmpclock -timeanddate
setdialinentry -index 12 -id gisellem -password s0ngb1rd -readonly
false
logoff
exit
```

Figure 6-7 Script to log on and set dial-in configuration

Get and set switch module configuration

Figure 6-8 on page 191 shows a script to get and set switch module configuration.

```
getsmnetwork -currentconfig 1
getsmnetwork -currentmethod 1
getsmnetwork -pendingconfig 1
getsmnetwork -pendingmethod 1
switchmodule -getpoweron 1
switchmodule -getmemdiagson 1
switchmodule -getcfgotherports 1
switchmodule -getextportson 1
switchmodule -ping 1
switchmodule -getpostresults 1
setsmnetwork -ipaddress 1, 192.168.1.125
setsmnetwork -gateway 1, 192.168.1.126
setsmnetwork -subnet 1,255.255.255.0
setsmnetwork -method 1, "static"
setsmnetwork -pending 1,false
setsmnetwork -pending 1,true
switchmodule -setpoweron 1,true
switchmodule -setmemdiagson 1,true
switchmodule -setcfgotherports 1,true
switchmodule -setextportson 1,true
switchmodule -ping 1
switchmodule -getpostresults 1
```

Figure 6-8 Script to get and set switch module configuration

Creating a nested script

MPCLI is capable of nested scripts, which means that you can call a script inside another script. The advantage of this is that you can put one script in multiple larger scripts to make it easier to maintain your script library overall. For example, if you regularly change passwords of the user IDs used to access your service processors, then it may make sense to keep this information in files separate from your library of scripts. For example, a script to log on to the service processor in server FILE1 might be like that shown in Figure 6-9.

```
logonip -hostname file1sp -userid USERID -password PASSWORD
```

Figure 6-9 Script file logon-file1.txt

You would create separate logon scripts for each of your systems. Then, for each of your management scripts, you can then simply call this script. For example, to flash multiple service processors you could modify the script in Figure 6-6 on page 190 as shown in the figure (modified lines highlighted).

```
outputfile ./rsaflash.txt

getmpid -text
getvpd -mpboot
getvpd -mprom
fwupdate -mn d:\firmware\x220\batman\CNETMNUS.PKT
logoff
sleep 15000

fwupdate -br d:\firmware\x220\batman\CNETBRUS.PKT
logoff
sleep 15000

fwupdate -vnc d:\firmware\x220\batman\CNETRGUS.PKT
logoff
exit
```

Figure 6-10 Script to log on and flash the service processor over Ethernet

When you later change your password, you only have to update the logon scripts.

6.4 OSA SMBridge utility

The OSA System Management Bridge (SMBridge) is a utility that lets you perform certain remote management functions on a server that has a BMC service processor. It allows the administration of servers using IPMI1.5 protocol and the Serial Over LAN (SOL) protocol via either the server's Ethernet or serial interfaces. The primary function of SMBridge is to provide remote control of the text-mode console via Ethernet.

The xSeries servers supported are those with the BMC controller, as listed in Table 1-1 on page 2.

There are two ways to use the SMBridge utility: As a telnet server and as a direct command-line interface to the BMC. These are shown in Figure 6-11 on page 194.

- ▶ Telnet server connection

Used as a telnet server, SMBridge is started as a background service or daemon on a system on your network (typically not the server with the BMC).

You connect to the telnet server, then from there, connect to the BMC via the server Ethernet port.

SMBridge uses the Serial Over LAN protocol to let the administrator remotely control text-mode tasks such as POST messages, BIOS setup, and text-mode tasks with operating systems. Tasks you can perform are:

- Establish a text-mode console session with the remote server.
- Power on, power off (immediate and graceful), or reboot a server.
- Turn on/off the blinking system identifier.
- Display the current power status.
- Display the event log.

Any standard telnet client application, such as HyperTerminal on Microsoft Windows or telnet on Linux, can be used to access the server's features.

The SOL protocol coupled with the remote system's BIOS console redirection allows administrators to view and change the BIOS settings over LAN. Linux serial console and Microsoft's Emergency Messaging Service (EMS)/Special Administration Console (SAC) interfaces can also be accessed over LAN using SOL.

This is discussed further in 6.4.3, “Connecting via the telnet server” on page 199.

► **Command-line interface**

Used in this way, SMBridge lets an administrator perform the following tasks on a remote BMC service processor to:

- Power on, power off (immediate and graceful), or reboot a server.
- Turn on/off the blinking system identifier.
- Display the current power status.
- Display or clear the event log.

The CLI lets you do all but the remote console feature offered by the telnet server.

This is discussed further in 6.4.7, “Connecting via the command-line interface” on page 216.

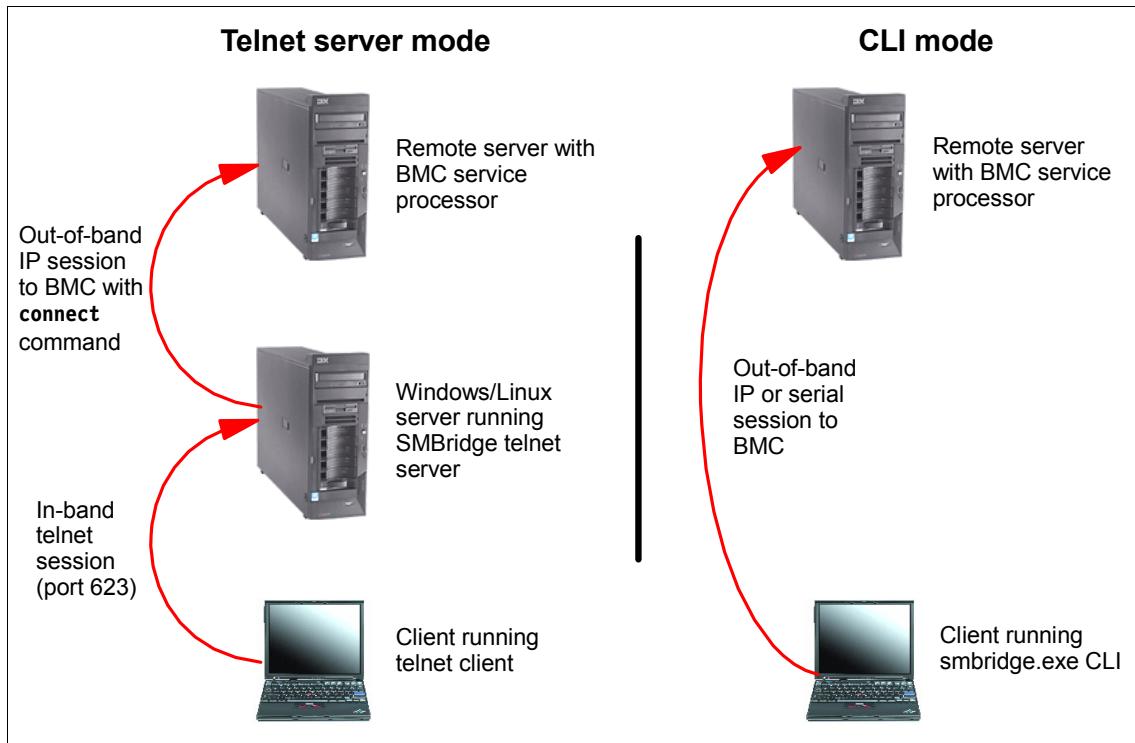


Figure 6-11 The two modes of the SMBridge utility

SMBridge can be downloaded from:

<http://www.ibm.com/pc/support/site.wss/MIGR-57729.html>

The current version supports the following operating systems:

- ▶ Red Hat Linux 7.2
- ▶ Red Hat Linux 8.0
- ▶ Red Hat Linux 9.0
- ▶ Red Hat Enterprise Linux 3.0
- ▶ Microsoft Windows XP
- ▶ Microsoft Windows 2000 Professional
- ▶ Microsoft Windows 2000 Server
- ▶ Microsoft Windows Server 2003

The *OSA System Management Bridge User's Guide* is available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-57816.html>

6.4.1 Configuring BIOS

Before SMBridge can be used to manage a remote server via SOL, the BMC and BIOS of the remote server must have the following settings configured.

Note: This procedure disables PXE boot on Gigabit port 1 on the server. If you plan to use PXE, you will need to connect Gigabit port 2 to your network and ensure that your remote install procedure is configured to use that port.

1. Enter BIOS Setup by pressing F1 when prompted during boot.
2. If you have not done so already, configure the static IP address, subnet mask, and gateway of the BMC as described in 2.3.5, “Configuring the BMC in BIOS” on page 34.
3. From the main menu, select **Devices and I/O Ports**. Set the following:
 - Set field Serial Port A to Auto-configure.
 - Set field Serial Port B to Auto-configure.
4. Select **Remote Console Redirection**. Set the following:
 - Remote Console Active to Active
 - Remote Console Text Emulation to VT100/VT220
 - Remote Console Keyboard Emulation to VT100/VT220
 - Remote Console Active After Boot to Enabled
 - Remote Console Flow Control to Hardware

The result is shown in Figure 6-12.

```
*****
*          Remote Console Redirection      *
*****
*  Remote Console Active      [ Enabled ]  *
*  Remote Console COM Port   [ COM 1 ]    *
*  Remote Console Baud Rate  [ 19200 ]   *
*  Remote Console Data Bits  [ 8 ]        *
*  Remote Console Parity    [ None ]     *
*  Remote Console Stop Bits [ 1 ]        *
*  Remote Console Text Emulation [ VT100/VT220 ] *
*  Remote Console Keyboard Emulation [ VT100/VT220 ] *
*  Remote Console Active After Boot [ Enabled ]  *
*  Remote Console Flow Control [ Hardware ] *
*****
```

Figure 6-12 Remote Console Redirection settings to enable SOL

5. Press Esc twice to return to the main menu, then select **Start Options**. Set the following:
 - Planar Ethernet 1 PXE to Disabled
 - Planar Ethernet 2 PXE to Enabled
 - Planar Ethernet PXE/DHCP to Planar Ethernet 2
 - Run PXE only on Selected Planar NIC to Enabled
- Note that you will most likely only have some of these options on your server. For example, on the x236, we only set Planar Ethernet PXE/DHCP to Planar Ethernet 2.
6. Press Esc to return to the main menu, then select **Advanced Options**, then **Baseboard Management Controller (BMC) Settings**. Set the following:
 - System-BMC Serial Port Sharing to Enabled
 - BMC Serial Port Access Mode to Dedicated
7. Save the BIOS settings and reboot the server.

6.4.2 Installation

This section describes how to install the SMBridge utility on both Windows and Linux platforms. The latest version of the utility is available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-57729.html>

Microsoft Windows

The procedure both installs the CLI, and it installs and enables the telnet server.

Tip: This installation is normally run on the server you plan to have act as the telnet server, as shown in Figure 6-11 on page 194. If you plan to use the CLI, you do not actually need to install the tool, since the only files you need to run the CLI are smbridge.exe and smbridge.cfg.

Consequently, if you plan to use the CLI on other systems, you can either:

- ▶ Copy the files smbridge.exe and smbridge.cfg from the telnet server.
- ▶ Install SMBridge then disable the service.

1. Run Setup, agree to the license, and specify an installation directory.
2. You will now be prompted to enter an IP address and TCP/IP port number, as shown in Figure 6-13 on page 197.

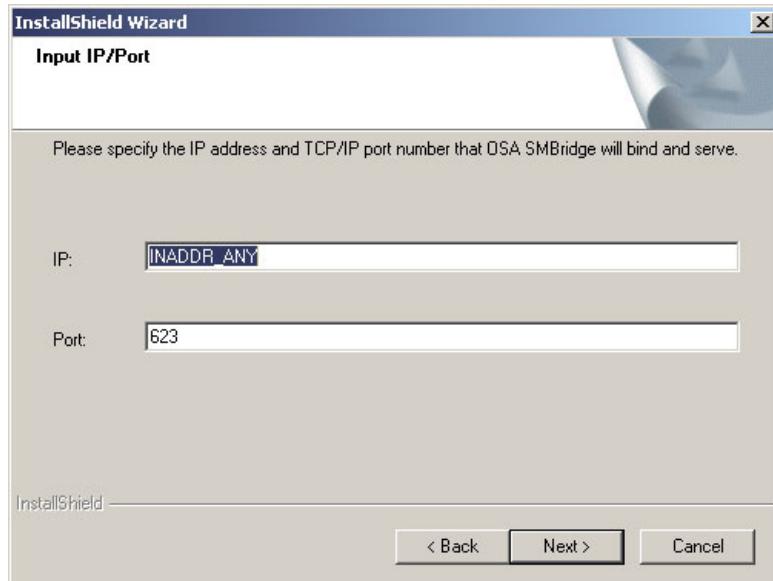


Figure 6-13 IP address and port number window

These values are as follows:

- IP specifies the server IP address that SMBridge will bind to.

Since a server may have multiple valid IP addresses, SMBridge allows you to restrict access to it via a single IP address. Specify INADDR_ANY as the IP address if any of the multiple IP addresses can be bound to SMBridge. Specify 127.0.0.1 or localhost as the IP address if SMBridge should only accept local connections. Specify a specific IP address if only this IP address should be bound to SMBridge.

- Port specifies the server port number that SMBridge will listen on.

Note: These two values will be recorded in the smbridge.cfg file for automatic startup of SMBridge as a service daemon.

3. Next, you are asked to specify timeout values for telnet sessions (in minutes) and the power-off command (in seconds) (Figure 6-14 on page 198).

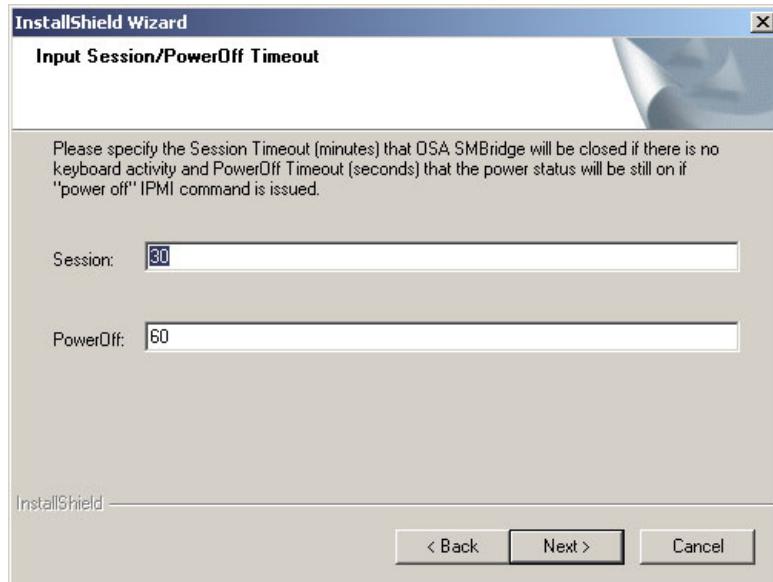


Figure 6-14 Session and power off timeout settings window

These values are as follows:

- Session specifies the number of minutes without any keyboard activity before an established telnet session is ended.
 - PowerOff specifies the number of seconds to wait for an IPMI power off command (graceful or forced) to complete. If time has exceeded the timeout value and the power status is still on, an error code will be returned to indicate that the power off command may have failed.
4. Click **Next** to confirm your choices, then begin the installation. Once the installation is complete, click **Finish** to end the installer.

The OSA SMBridge service is started automatically and is configured to start every time the server starts. You can change this via **Control Panel** → **Administrative Tools** → **Services**.

Installation on a Linux platform

To install SMBridge on Linux, follow these steps:

1. Log in as root.

2. If the SMBridge RPM file is on CD, then insert the CD into the drive and enter the following commands to mount the drive and change to the root directory of the CD:

```
mount /mnt/cdrom  
cd /mnt/cdrom
```

3. Run the installation with the following command (substitute the filename of the rpm file you have if it is different):

```
rpm -i osasmbridge-1.0.3-1.i386.rpm
```

When the installation process has finished successfully, files are copied to the following directories:

- ▶ /etc/init.d/smbridge
- ▶ /etc/smbridge.cfg
- ▶ /usr/bin/smbridge
- ▶ /var/log/smbridge
- ▶ /var/log/smbridge/LICENSE

Additionally, the symbolic link /usr/sbin/smbridge is created.

The text file /etc/smbridge.cfg contains a number of SMBridge runtime parameters that you should review and modify if necessary.

To start the daemon, navigate to directory /etc/int.d and use the following command to start or stop the OSA SMBridge daemon service:

```
smbridge start  
smbridge stop
```

You can also start the daemon using the command:

```
smbridge -d -c config-file
```

Where *config-file* is the name of the file containing the telnet server configuration. By default it is /etc/smbridge.cfg. See Appendix C of the *SMBridge User's Guide* for more details about this file.

6.4.3 Connecting via the telnet server

As shown in Figure 6-11 on page 194, you can use SMBridge as a telnet interface (or a “bridge”) to the BMC. You connect to a telnet server (where you installed SMBridge), and from there you connect to the BMC using a Serial Over LAN (SOL) connection.

Using a SOL connection, you can perform over a LAN connection all tasks that you would normally only be able to do connecting directly to the server's serial port:

- ▶ Change the BIOS settings.
- ▶ Linux serial console.
- ▶ Emergency Messaging Service (EMS) from Microsoft.
- ▶ Special Administration Console (SAC) from Microsoft.

Information on Microsoft EMS is available from:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_topnode.asp

The SAC commands you can perform are described here:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp

With BIOS console redirection to serial port enabled on the remote server, applications that use the BIOS to read and write to the system console will have their I/O redirected to the serial port. With SOL, the BMC firmware then reads the data written to the serial port and transmits it to the SMBridge as LAN packets. SMBridge then forwards the data to the telnet client as TCP/IP packets.

One SMBridge session supports one SOL session with one BMC at a time.

Telnet clients

To access the SMBridge telnet server, connect using port 623 (or the port you selected during installation if you changed it from this default). For example:

`telnet smbridge-server 623`

Note: By default, the SMBridge telnet server listens on port 623.

Telnet clients that support VT100 terminal emulation can be used to access the BMC via SMBridge, including to following.

- ▶ The **telnet** command-line utility in Windows

Additional information:

- Our testing showed that on a Windows XP system, pressing F1 on the keyboard correctly sent F1 to the remote server (for example, to enter BIOS Setup). If your telnet client does not work this way (such as the **telnet** command in Windows Server 2000), you can simulate the F1 and F2 keys in two ways. To simulate F1, either of:
 - Esc, then Numeric+1 (that is the 1 key on the numeric keypad)

- Esc, then Shift+O, then Shift+p

To simulate F2, either of:

- Esc, then Numeric+2 (that is the 2 key on the numeric keypad)
- Esc, then Shift+O, then Shift+q

Tip: We recommend that you use this telnet client when running Windows. It is a standard implementation of telnet and also supports colors.

► HyperTerminal in Windows

Additional information:

- HyperTerminal supplied with Windows Server 2003, Enterprise Edition may not work correctly. You should upgrade to the Private version.
 - HyperTerminal supplied with Windows 2000 Server displays random characters and loses some text. We recommend that you do not use this client.
 - When creating a new connection, select **TCP/IP (WinSock)** in the Connect using drop-down menu. Enter the IP address of the telnet server and specify port 623 (or the port you specified when you installed SMBridge).
 - Turn off automatic line wrapping by clearing the check box “Wrap lines that exceed terminal width” in **File → Properties → Setting → ASCII → Setup**.
 - Configure the connection to emulate a VT100 terminal in the Properties window.
- The **telnet** command as part of csh or ksh in Linux.

The F1 and F2 keys may not work correctly, especially outside of an X-Windows environment. You may be able to reconfigure X-Windows to generate VT100 keystrokes. With KDE, for example, use Settings to reconfigure the keyboard.

Connecting

In this section, we describe the process by referring to servers in our lab. We have installed the SMBridge telnet server on the system at address 9.42.171.121, and the remote server has a BMC configured to use address 9.24.171.237. Our BMC uses the default USERID/PASSW0RD authentication.

To connect to the BMC do the following (using our example addresses):

1. Issue the following to connect to the telnet server on port 623:

```
telnet 9.42.171.121 623
```

2. You will be prompted as shown below.

```
Username:
```

3. Enter an administrator user ID and password that is valid for the telnet server (for example, Administrator or root).

Note: If the SMBridge telnet server is running on the local system you will not see this prompt, as SMBridge uses the authority of the current user logged on.

4. You will then see the following welcome message.

```
Username:Administrator  
Password:  
  
Administrator login successful.  
  
OSA System Management Bridge (SMBridge), Version 1.0.3.1  
Copyright (c) 2004 - OSA Technologies, an Avocent Company. All  
Rights Reserved.  
  
SMBridge>
```

5. Connect to the BMC on the server you wish to manage using the **connect** command.

```
SMBridge>connect -ip 9.42.171.237 -u USERID -p PASSWORD  
SMBridge>
```

The user ID and password here are ones that have previously been configured as users able to log into the BMC.

If the command was successful, you will be returned to the SMBridge command prompt.

6. You can now issue commands against the remote BMC as described below.
7. To exit, enter the **exit** command.

Available commands

The commands are a superset of those of the command-line interface and are listed in Table 6-6. To get detailed help about a command, issue the **help** command. For example:

```
help power
```

Tip: Most of the commands available to the telnet interface are the same as those used in the CLI. The additional telnet commands are **console**, **sol**, and **reboot**.

Table 6-6 SMBridge telnet subcommands

Subcommand	Description and syntax
console	<p>Start a Serial Over LAN (SOL) session with the BMC, displaying the text that has been redirected from the console to the serial port. There are no parameters.</p> <p>When you enter the console command, you will see:</p> <p>Activating remote console now. Remote console is now active and ready for user input.</p> <p>To return to the telnet session press the tilde key followed by the period key, as in:</p> <p>~.</p>
sol	<p>Used to enable or disable Serial Over LAN and to configure serial parameters to match the Console Redirection parameters of the remote server's BIOS. The options are:</p> <p>sol enable sol disable sol config [-baud <i>baud_rate</i>] [-priv <i>privilege_level</i>] [-retry count <i>retry_count</i>] [-retry interval <i>retry_interval</i>]</p>
reboot	<p>Performs the equivalent of a power off (graceful shutdown), power on, then starts the remote console. The options are:</p> <p>reboot reboot -force</p> <p>Note that the x236, x336, and x346 do not support the graceful shutdown option. The -force parameter is required on these servers.</p>

Subcommand	Description and syntax
sysinfo	<p>Displays general system information related to the server and BMC. The options are:</p> <pre>sysinfo fru sysinfo id</pre> <p>id is the default if no parameter is specified.</p>
identify	<p>Controls the blue identification LED on the front panel of the server. The options are:</p> <pre>identify on [-t <seconds>] identify off</pre> <p>on is the default if no parameter is specified.</p>
power	<p>Controls the power options of the server. The options are:</p> <pre>power status power on power cycle power reset power off [-force]</pre> <p>status is the default if no parameter is specified.</p> <p>Note that the x236, x336, and x346 do not support the graceful shutdown option. The -force parameter is required on the server.</p>
sel	<p>Performs operations with the System Event Log (SEL). The options are:</p> <pre>sel status sel get sel get -last <n> sel get -begin <index1> -end <index2> sel get -begin <index1> -max <count> sel clear sel set -time <YYYY/MM/DD hh:mm:ss></pre> <p>status is the default if no parameter is specified.</p>
help	<p>Displays general help about all commands or help about a specific command.</p>

6.4.4 Configuring Windows Server 2003 to support SOL

When you connect to the BMC using the SMBridge telnet server, you can remotely control the text console. With SOL this also includes operating systems such as Windows Server 2003 and Linux.

Windows Server 2003 has two components that work with SMBridge and the BMC to provide out-of-band access to the operating system:

- ▶ Microsoft Emergency Messaging Service (EMS)
- ▶ Microsoft Special Administration Console (SAC)

Information on Microsoft EMS is available from:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_topnode.asp

The SAC commands you can perform are summarized in Table 6-7.

Table 6-7 Windows Server 2003 Special Administration Console (SAC) commands

Command	Description
ch	Lists all channels.
cmd	Creates a command-prompt channel. You will be asked to log on.
crashdump	Manually generates a Stop error message and forces a memory dump file to be created.
d	Dumps the current kernel log.
f	Toggles the information output by the t-list command, which shows processes only, or shows processes and threads.
i	Lists the TCP/IP details of all network interfaces, and lets you configure the IP address, subnet mask, and gateway of a given network interface. To change the parameters, specify them as: network# IPaddress subnet gateway
id	Displays identification information about the server.
k <i>pid</i>	Ends the given process. <i>pid</i> is the process identification number you specify.
L <i>pid</i>	Lowers the priority of a process (and any associated child processes) to the lowest possible level.

Command	Description
lock	Restricts access to Emergency Management Services command-prompt channels. You must provide valid logon credentials to unlock a channel.
<i>m pid mb-allow</i>	Limits the memory usage of a process (and any associated child processes) to a specified number of megabytes. <i>mb</i> is the number of megabytes you specify.
p	Causes t-list command output to pause after displaying one full screen of information.
r <i>pid</i>	Raises the priority of a process and any associated child processes by one level.
restart	Restarts the server.
s	Displays or sets the system time. To set the time, use the format: mm/dd/yyyy hh:mm
shutdown	Shuts down and powers off the server. Terminates the console session and returns you to the SMBridge prompt.
t	Lists the processes and threads that are currently running.
? or help	Lists the available commands.

To exit SOL and return to the SMBridge prompt, press the tilde key and the period key (that is, ~.).

For more information, see:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp

To enable EMS on a Windows Server 2003, do the following.

1. Log in to Windows as an administrator.
2. Launch a command prompt and enter the command **bootcfg**.

```
C:\>bootcfg

Boot Loader Settings
-----
timeout:30
default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Boot Entries
-----
Boot entry ID: 1
OS Friendly Name: Windows Server 2003, Enterprise
Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options: /fastdetect
```

Figure 6-15 Output from the bootcfg command

3. Examine the output. If there is more than one boot entry then you will need to determine the default entry by looking at the default line under Boot Loader Settings and determining whether Boot Entry has a matching Path value. In our case, there is only one boot entry, 1.
4. Issue the following command, substituting your boot entry number in the /id parameter if it is not 1 as in our example.

```
bootcfg /ems on /port com1 /baud 19200 /id 1
```

```
C:\>bootcfg /ems on /port com1 /baud 19200 /id 1
SUCCESS: Changed the redirection port in boot loader section.
SUCCESS: Changed the redirection baudrate in boot loader section.
SUCCESS: Changed the OS entry switches for line "1" in the
BOOT.INI file.
```

Figure 6-16 Changing the boot configuration

5. Reissue the **bootcfg** command to see the result. The changes in our example are highlighted.

```
C:\>bootcfg /ems on /port com1 /baud 19200 /id 1
SUCCESS: Changed the redirection port in boot loader section.
SUCCESS: Changed the redirection baudrate in boot loader section.
SUCCESS: Changed the OS entry switches for line "1" in the BOOT.INI
file.

C:\>bootcfg

Boot Loader Settings
-----
timeout:      30
default:      multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
redirect:     COM1
redirectbaudrate:19200

Boot Entries
-----
Boot entry ID:    1
OS Friendly Name: Windows Server 2003, Enterprise
Path:           multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options: /fastdetect /redirect
```

Figure 6-17 The bootcfg command after enabling EMS

6. Reboot the server to have the changes take affect.

Note: To turn EMS off again, issue the following command:

```
bootcfg /ems off /id 1
```

Where 1 is the boot entry you have modified in the above steps. Reboot to bring the changes online.

Once you have rebooted and engaged the SMBridge console (see the **console** command in Table 6-6 on page 203), you will see the EMS console.

```
<?xml version="1.0"?>
<machine-info>
Computer is booting, SAC started and initialized.
<processor-architecture>x86</processor-architecture>
<os-version>5.2</os-version>
<os-build-number>3790</os-build-number>

SAC>
```

Figure 6-18 Microsoft Emergency Messaging Service console

You can now issue the various SAC commands described in Table 6-7 on page 205. For example, to start a command prompt, the commands are as follows (Figure 6-19 on page 210).

Tip: After you start the SMBridge console, if you only get a blank screen, press Enter a few times to get the SAC> prompt.

```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Cmd0002
SAC>ch
Channel List

(Use "ch -?" for information on using channels)

# Status Channel Name
0 (AV) SAC
1 (AV) Cmd0002
SAC>ch -si 1
Name: Cmd0002
Description: Command Prompt
Type: <Esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.

Please enter login credentials.
Username:
Domain:
Password:

Attempting to authenticate...

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003

C:\WINDOWS\system32>
```

Figure 6-19 SAC commands to launch a command prompt channel

To close the command prompt channel, enter `exit`. To leave the channel open and return to the SAC prompt, press `Esc+Tab+0` (the number zero key) (three keys in sequence). To leave the remote console and return to SMBridge press `tilde+period` (that is, `~.`)

6.4.5 Configuring Red Hat Linux to support SOL

You must configure Red Hat Linux to expose the Linux initialization (booting) process. This enables users to log in to the Linux console through an SOL session and directs output to the serial console. The following instructions are for Red Hat Enterprise Linux ES 2.1 or 3.0 to enable SOL:

1. Log in as root.
2. Modify the /etc/inittab file by adding the following line to the end of the # Run gettys in standard runlevels section to enable users to log in at the SOL console:

```
7:2345:respawn:/sbin/agetty -h -L ttyS1 19200 vt102
```

3. Modify the /etc/securetty file by adding the following line to enable users to log in as root at the SOL console:

```
ttyS1
```

For LILO users (GRUB users jump to step 1 on page 213):

1. Modify the /etc/lilo.conf file:
 - a. Add -Monitor to the first default line.
 - b. Comment out the map line.
 - c. Comment out the message line.
 - d. In the first Image section, append -Monitor to the label line, and append the following line:
`append="console=ttyS1,19200n8 console=tty1"`
 - e. Add the following lines between the two Image sections

```
# This will allow you to Interact with the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
label=linux-Interact
initrd=/boot/initrd-2.4.9-e.12smp.img
read-only
root=/dev/hda6
append="console=tty1 console=ttyS1,19200n8"
```

The result is shown in Figure 6-20 on page 212. Changes are highlighted.

```

prompt
timeout=50
default=linux-Monitor
boot=/dev/hda
#map=/boot/map
install=/boot/boot.b
#message=/boot/message
linear

# This will allow you to only Monitor the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
label=linux-Monitor
initrd=/boot/initrd-2.4.9-e.12smp.img
read-only
root=/dev/hda6
append="console=ttyS1,19200n8 console=tty1"

# This will allow you to Interact with the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
label=linux-Interact
initrd=/boot/initrd-2.4.9-e.12smp.img
read-only
root=/dev/hda6
append="console=tty1 console=ttyS1,19200n8"

image=/boot/vmlinuz-2.4.9-e.12
label=linux-up
initrd=/boot/initrd-2.4.9-e.12.img
read-only
root=/dev/hda6

```

Figure 6-20 Changes to the lilo.conf file

2. Enter lilo to store and activate the new LILO configuration.
3. Restart Linux.

When the operating system starts to boot, you will now see a LILO prompt instead of the usual GUI interface. Pressing the Tab key while at this prompt will display the boot options. To load the operating system in interactive mode, you would enter:

linux-Interact

For GRUB users:

1. Modify the /boot/grub/grub.conf file as follows:
 - a. Comment out the splashimage line.
 - b. Add the following comment before the first title line.

```
# This will allow you to only Monitor the OS boot via SOL
```
 - c. Append SOL Monitor to the first title line.
 - d. Append the following text to the end of the kernel line of the first title section:

```
console=ttyS1,19200 console=tty1
```
 - e. Add the following lines between the two title sections:

```
# This will allow you to Interact with the OS boot via SOL
title Red Hat Linux (2.4.9-e.12smp) SOL Interactive
root (hd0,0)
kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=tty1
    console=ttyS1,19200
initrd /initrd-2.4.9-e.12smp.img
```

The result is shown in Figure 6-21 on page 214. Changes are highlighted.

2. Restart Linux.

```

#grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda6
#          initrd /initrd-version.img
#
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
# This will allow you to only Monitor the OS boot via SOL
title Red Hat Enterprise Linux ES (2.4.9-e.12smp) SOL Monitor
    root (hd0,0)
    kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=ttyS1,19200 console=tty1
    initrd /initrd-2.4.9-e.12smp.img

# This will allow you to Interact with the OS boot via SOL
title Red Hat Linux (2.4.9-e.12smp) SOL Interactive
    root (hd0,0)
    kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=tty1 console=ttyS1,19200
    initrd /initrd-2.4.9-e.12smp.img

title Red Hat Enterprise Linux ES-up (2.4.9-e.12)
    root (hd0,0)
    kernel /vmlinuz-2.4.9-e.12 ro root=/dev/hda6
    initrd /initrd-2.4.9-e.12.img

```

Figure 6-21 Changes to the grub.conf file

6.4.6 Configuring SUSE LINUX to support SOL

You must configure SUSE LINUX to expose the Linux initialization (booting) process. This enables users to log in to the Linux console through an SOL session and directs output to the serial console. The following instructions are for SUSE LINUX Enterprise Server 8.0 to enable SOL:

1. Log in as root.
2. Modify the /etc/inittab file by adding the following line to the end of the #getty-programs for the normal runlevels section to enable users to log in at the SOL console:

```
7:2345:respawn:/sbin/agetty -h -L ttyS1 19200 vt102
```

3. Modify the /etc/securetty file by adding the following line after the tty6 line to enable users to log in as root at the SOL console:

```
ttyS1
```

4. Modify the /boot/grub/menu.lst file as follows:

- a. Comment out the gfxmenu line.

- b. Add the following comment line before the first title line:

```
# This will allow you to only Monitor the OS boot via SOL
```

- c. Append SOL Monitor to the first title line.

- d. Append the following text to the kernel line of the first title section:

```
console=ttyS1,19200 console=tty1
```

- e. Add the following lines between the first two title sections:

```
# This will allow you to Interact with the OS boot via SOL
```

```
title linux SOL Interactive
```

```
kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791
```

```
    console=tty1 console=ttyS1,19200
```

```
initrd (hd0,1)/boot/initrd
```

The result is shown in Figure 6-22 on page 216. Changes are highlighted.

5. Restart Linux.

```

#gfxmenu (hd0,1)/boot/message
color white/blue black/light-gray
default 0
timeout 8

# This will allow you to only Monitor the OS boot via SOL
title linux SOL Monitor
# Note: The following "kernel" line is all one line, not two separate lines
# The text has wrapped in this example
    kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791
console=ttyS1,19200 console=tty1
    initrd (hd0,1)/boot/initrd

# This will allow you to Interact with the OS boot via SOL
title linux SOL Interactive
# Note: The following "kernel" line is all one line, not two separate lines
# The text has wrapped in this example
    kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791 console=tty1
console=ttyS1,19200
    initrd (hd0,1)/boot/initrd

title floppy
    root
    chainloader +1
title failsafe
    kernel (hd0,1)/boot/vmlinuz.shipped root=/dev/hda2 ide=nodma apm=off vga=normal
nosmp disableapic maxcpus=0 3
    initrd (hd0,1)/boot/initrd.shipped

```

Figure 6-22 Changes to the menu.lst file

6.4.7 Connecting via the command-line interface

OSA SMBridge also supplies and command-line tool, smbridge.exe, which lets you perform a subset of the functions that you can perform using the telnet server. Specifically, tasks missing are the ability to remotely control the text console of the server via SOL. The CLI does, however, let you connect to the server via a serial connection.

In CLI mode, SMBridge supports out-of-band access through the LAN or serial port to one server at a time. However, multiple IPMI sessions can run

simultaneously on the same remote server. LAN connections are via Ethernet and serial connections are typically via a null modem.

To run SMBridge in CLI mode, simply open a command prompt/shell prompt at the directory where SMBridge is installed and issue the **smbbridge** command.

- ▶ With Windows, SMBridge is installed by default in c:\Program Files\OSA.
- ▶ With Linux, it is installed by default in /usr/sbin.

The syntax is as follows for Ethernet or Serial connectivity.

For Ethernet connections:

```
smbbridge -ip address -u user -p password subcommand
```

Where

- ▶ **-ip address** is the IP address or host name of the remote server.
- ▶ **-u user -p password** is a valid service processor user ID and password (default USERID/PASSW0RD).

For Serial connections:

```
smbbridge -com serialport [-baud baudrate] [-flow flowcontrol] -u user  
-p password subcommand
```

Where:

- ▶ **-com serialport** specifies the serial port on remote server. In Windows systems, it can be 1 for COM1, 2 for COM2, etc. In Linux systems, it can be ttyS0, ttyS1, etc.
- ▶ **-baud baudrate** specifies the baud rate you wish to communicate at, such as 9600 and 19200. It should match the one set in BIOS of the remote server (in the Remote Console Redirection window). If not specified, it defaults to 19200.
- ▶ **-flow flowcontrol** specifies the flow control. If not specified, it defaults to CTS (hardware flow control). The options are:
 - CTS = hardware flow control
 - XON = software flow control
 - NONE = no flow control

The valid subcommands and the syntax of those commands is listed in Table 6-8 on page 218. For more information about the syntax, issue the **-help** command. For example:

```
smbbridge -help power
```

Table 6-8 SMBridge CLI subcommands

Subcommand	Description and syntax
sysinfo	Displays general system information related to the server and BMC. The options are: sysinfo fru sysinfo id id is the default if no parameter is specified.
identify	Controls the blue identification LED on the front panel of the server. The options are: identify on [-t <seconds>] identify off on is the default if no parameter is specified.
power	Controls the power options of the server. The options are: power status power on power cycle power reset power off [-force] status is the default if no parameter is specified. Note: The x236, x336, and x346 do not support the graceful shutdown option. The -force parameter is required on these servers.
sel	Performs operations with the System Event Log (SEL). The options are: sel status sel get set get -last <n> sel get -begin <index1> -end <index2> sel get -begin <index1> -max <count> sel clear sel set -time <YYYY/MM/DD hh:mm:ss> status is the default if no parameter is specified.

6.5 Web interface

The Remote Supervisor Adapter II and BladeCenter management module have a built-in Web server that allows users to access these service processors using a Web browser.

The following browsers are supported to use with the RSA II and the BladeCenter management module:

- ▶ Microsoft Internet Explorer 5.5 (with the latest service pack installed) or later
- ▶ Netscape Navigator 4.72 or later (Version 6.x is not supported)
- ▶ Mozilla 1.3 or later (remote control features for RSA II are not supported)

The browser must be Java enabled, support JavaScript 1.2 or later, and have Java 1.4.1 plug-in installed.

Tip: For best results when using the Web browser, ensure that your monitor's resolution is at least 800x600 and at least 256 colors.

A Java runtime is required. If your computer has no Internet connection, you can download the Java software using another computer, from:

<http://www.java.com/en/download/manual.jsp>

If you have an Internet connection, you can force the browser to download the Java software. In the following example we use Windows and Internet Explorer.

1. Launch the browser and connect to a RSA II or BladeCenter management module.
2. Log in (the default user ID/password are USERID/PASSW0RD).
3. Click **Tasks → Remote Control** in the navigation frame.
4. Click **Start Remote Control in Single User Mode**.

A new browser window opens and a security warning pops up. If it does not and you get error messages from your browser, check that your browser is Java enabled and Java script is supported.

5. Follow the remainder of the instructions on screen to complete the installation.

6.5.1 Structure of the Web interfaces

All Web pages served by the service processors have a similar structure. Refer to the numbers in Figure 6-23 on page 220:

1. The top shows which type of service processor you are connected to.

2. The left side is the navigation frame with hierachal menus.
3. The remainder of the window is the information related to the active menu.

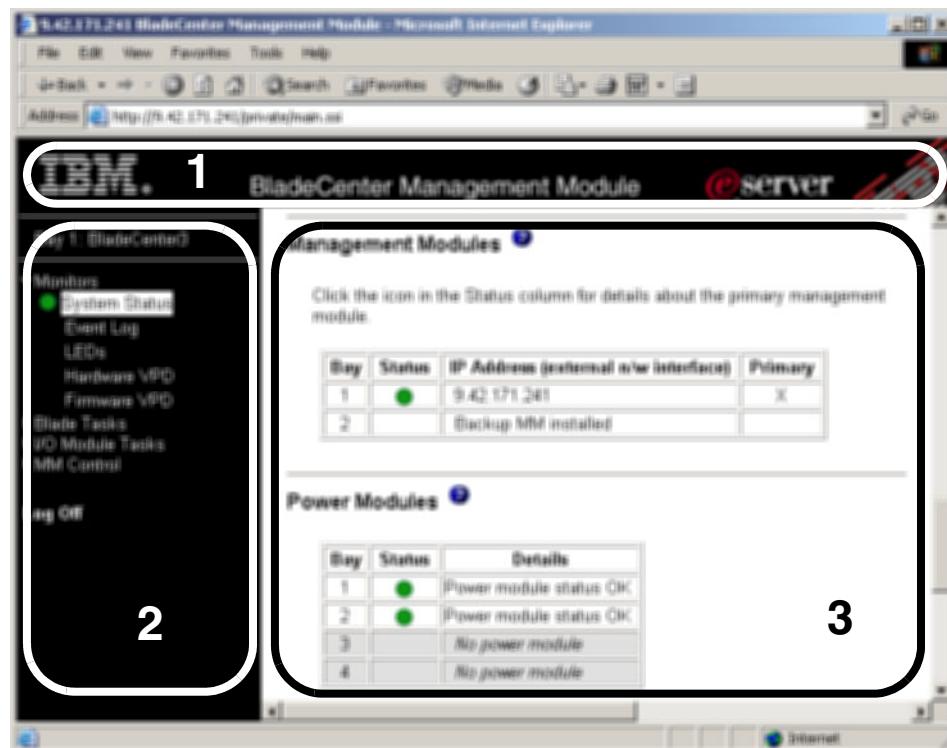


Figure 6-23 Web interface structure

6.6 Telnet interface

In addition to the Web interface described in 6.5, “Web interface” on page 219, some of the xSeries service processors also have a built-in interface that is accessible through the following connections, depending on the service processor:

- ▶ Telnet via Ethernet
- ▶ SSH via Ethernet
- ▶ ANSI terminal via serial

Note: Even though the interface works via telnet, ssh, and via an ANSI terminal session, we collectively refer to them as telnet for the sake of simplicity.

The service processors that support these interfaces are:

- ▶ BladeCenter management module
- ▶ Remote Supervisor Adapter II
- ▶ Remote Supervisor Adapter II SlimLine
- ▶ Remote Supervisor Adapter II-EXA
- ▶ Remote Supervisor Adapter
- ▶ ASM PCI Adapter (telnet and ANSI only)
- ▶ ASM Processor (telnet only via the ASM interconnect network)

The xSeries BMC service processor supports telnet but only via SMBridge, as discussed in 6.4, “OSA SMBridge utility” on page 192. The eServer BMC does not support a telnet session.

This interface provides a subset of the management functions that are provided by the Web interface. Like the other interfaces, you will need to authenticate before you can issue any commands.

For the RSA II, RSA II SlimLine, and BladeCenter management module service processors, the Telnet interface is command-line based. Each command has the following format:

command [arguments] [-options]

Notes:

- ▶ The command syntax is case sensitive.
- ▶ The command name is always lowercase.
- ▶ Options always start with a hyphen.
- ▶ One command per line.

Issuing the command **help** displays all available commands. Example 6-5 lists the commands available with the RSA II.

Example 6-5 RSA II commands (from the help command)

```
? -- Display command list
clearcfg -- Resets the ASM to its default settings
clearlog -- Clear ASM event log
    clock -- Display/set date, time, GMT offset, and dst setting
    console -- Exit CLI, attach to serial console
    dhcpinfo -- View DHCP server assigned settings
    exit -- Exit CLI (log off)
    fans -- Displays the fan speed for all system fans
    help -- Display command list
    history -- Display history of last 8 commands
    ifconfig -- Ethernet and PPP configuration
    portcfg -- Serial port configuration.
```

```
power -- Control server power
readlog -- Displays the ASM event log, five entries at a time
reset -- Reset server
resetasm -- Reset ASM
slp -- View/edit SLP parameters
srcfg -- Serial redirection configuration
syshealth -- System Health
tcpcmdmode -- View/edit TCP command mode config.
    temps -- Display system temperatures
    timeouts -- Server timeouts configuration
    users -- User profile configuration
update -- Update firmware
volts -- Displays all the voltages and voltage thresholds
vpd -- Display VPD
```

Example 6-6 lists the commands available using a BladeCenter management module.

Example 6-6 BladeCenter management module commands (from the help command)

```
?- Display commands
alertentries- View/edit remote alert recipients
    boot- Boot target
    clear- Clear the config
    clearlog- Clear the event log
    console- Start SOL session to a blade
    dhcpinfo- View DHCP server assigned settings
displaylog- Display log entries
    dns- View/edit DNS config
    env- Set persistent command target
    exit- Log off
    fuelg- Power management
    health- View system health status
    help- Display command list
    history- Display command history
    identify- Control target location LED
    ifconfig- View/edit network interface config
        info- Display identity and config of target
        list- Display installed targets
    power- Control target power
    reset- Reset target
shutdown- Shutdown target
    slp- View/edit SLP parameters
    smtp- View/edit SMTP config
    snmp- View/edit SNMP config
```

```
sol- View SOL status and view/edit SOL config
tcpcmdmode- View/edit TCP command mode config
telnetcfg- View/edit telnet config
update- Update firmware from TFTP server
users- View/edit user login profiles
```

Issuing a command with an -h parameter provides syntax help for that command. Example 6-7 shows the output from the **ifconfig -h** command.

Example 6-7 Displaying the syntax help for the ifconfig command (RSA II)

```
x345rsa2> ifconfig -h
usage:
ifconfig eth0 [-options]  - ethernet interface configuration
ifconfig ppp  [-options]  - ppp interface configuration
eth0 options:
-state <enabled|disabled> - interface status
-c <dhcp|static|dthens>  - configuration method
-i <ip_addr>             - IP address
-g <ip_addr>             - gateway
-s <ip_addr>             - subnet mask
-n <hostname>            - host name
-r <10|100|auto>         - data rate
-d <full|half|auto>      - duplex mode
-m <num>                 - MTU
-l <mac_addr>            - LAA
Note: The -b option in the ifconfig display is for the burned-in
      MAC address and is read-only

ppp options:
-state <enabled|disabled> - interface status
-i <ip_addr>             - IP address
-ri <ip_addr>            - remote IP address
-s <ip_addr>             - subnet mask
-a <pap|chap|cthenp>     - authentication method
```

As an example of usage, Example 6-8 is used to display the current Ethernet configuration, then change the host name, then restart the service processor.

Example 6-8 Changing the host name of the Ethernet interface

```
x345rsa2> ifconfig eth0
-state enabled
-c dthens
-i 9.42.171.7
```

```
-g 9.42.171.3
-s 255.255.255.0
-n ASMA00096B5E1209
-r auto
-d auto
-m 1500
-b 00:09:6B:5E:12:09
-l 00:08:04:06:4B:4F
x345rsa2> ifconfig eth0 -n x345rsa2
These configuration changes will become active after the next reset of
the ASM.
x345rsa2> resetsp
Submitting reset request
x345rsa2>
Connection to host lost.
```

The telnet interface has the following limitations:

- ▶ The command syntax is case sensitive.
- ▶ At most, two telnet and two ssh sessions (at most) are allowed at any one time.
- ▶ One command is allowed per line. There is a 160-character limit, including spaces.
- ▶ There is no continuation character for long commands. The only editing function is the Backspace key to erase the character that you just typed.
- ▶ The up arrow and down arrow keys can be used to browse through the last eight commands. The **history** command displays a list of the last eight commands, and you can use an exclamation point (!) to reissue a command. For example, to reissue the fourth command displayed by history, enter !4.

Unlike the RSA II and BladeCenter management module, the Telnet interface for the Remote Supervisor Adapter is menu driven, as shown in Figure 6-24 on page 225. The Telnet interface for the ASM PCI Adapter is also menu driven, albeit more rudimentary.

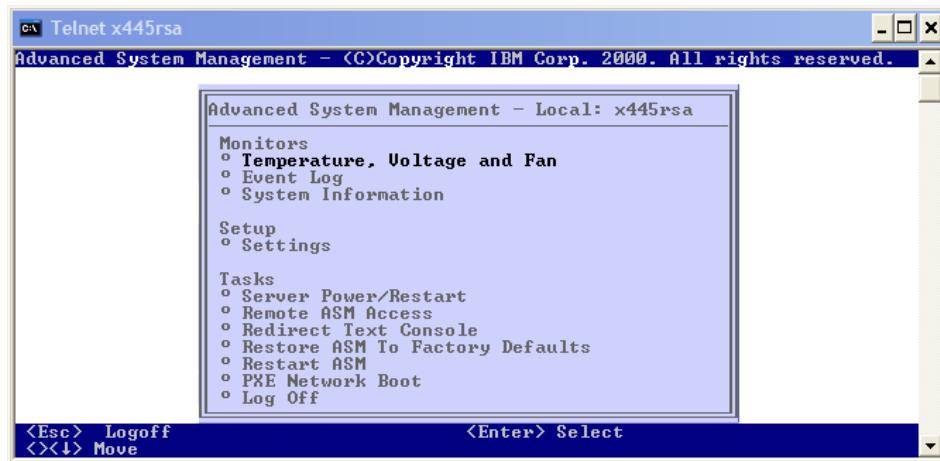


Figure 6-24 Telnet interface for the Remote Supervisor Adapter (xSeries 445)

6.7 IBM Director integration

For complete systems management of xSeries and BladeCenter systems, the recommended tool is IBM Director. With IBM Director, you have complete access to the systems management hardware in addition to other management tasks such as event management, inventory, and deployment.

IBM Director is available for IBM customers from:

<http://www.ibm.com/pc/support/site.wss/MIGR-57057.html>

The IBM Director console is divided in three panes, as shown in Figure 6-25 on page 226. On the left-hand side you can see the groups, in the middle the group members (for example, servers), and on the right are the available tasks.

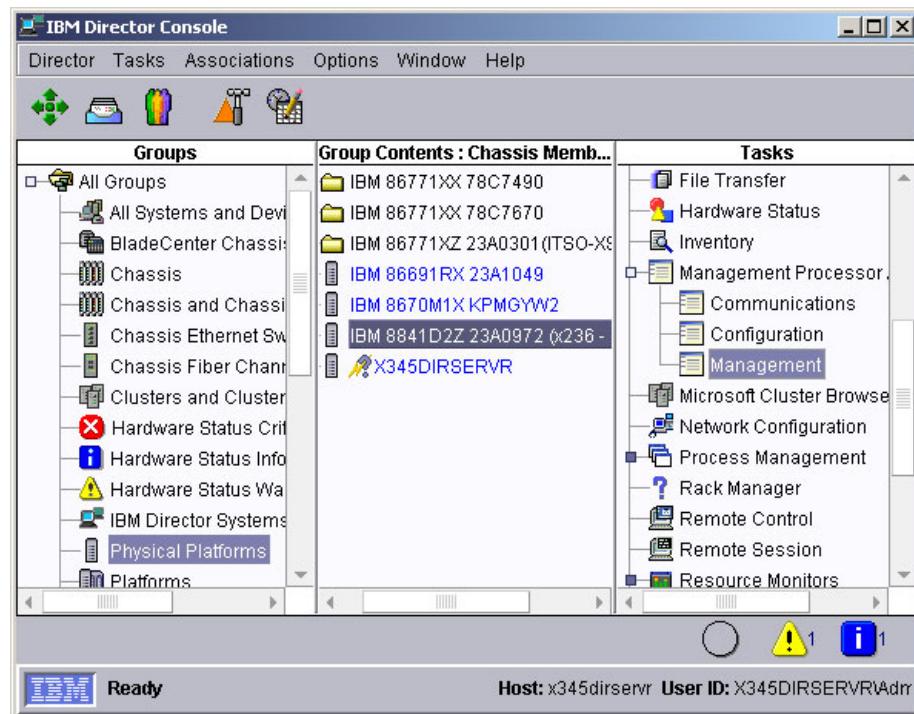


Figure 6-25 IBM Director console

The component used specifically to manage service processors within IBM Director is the Management Processor Assistant. See 6.7.1, “Management Processor Assistant” on page 227.

To access the service processors in xSeries servers using IBM Director, the IBM Director Agent and the appropriate service processor driver must first be installed on the target server, and the operating system has to be up and running.

Tip: This way of communication between the IBM Director components (console, agent, and server) via inter-process communication (IPC) is called *in-band* communication. All other communication, for example, with the Web interface over Ethernet to the hardware, is called *out-of-band*. You will find these expressions in IBM Director-related documentation.

To access the BladeCenter management module you do not have to install any agents or drivers, because the management module has a dedicated Ethernet connection, unlike the systems management processors.

For more information and details regarding IBM Director, refer to:

- ▶ The IBM Redbook *Implementing Systems Management Solutions using IBM Director*, SG24-6188
- ▶ The product publication *IBM Director Systems Management Guide*, available on the IBM Director CD in the docs directory

6.7.1 Management Processor Assistant

The Management Processor Assistant (MPA) is the interface of IBM Director to configure and manage service processors. It works with IBM servers that contain one or more of the following service processors:

- ▶ Advanced Systems Management Processor (ASMP)
- ▶ Advanced Systems Management PCI Adapter (ASMA)
- ▶ Integrated Systems Management Processor (ISMP)
- ▶ Intelligent Platform Management Interface (IPMI) Baseboard Management Controller (BMC)
- ▶ Remote Supervisor Adapter (RSA)
- ▶ Remote Supervisor Adapter II (RSA II)

Tip: Using the MPA requires the IBM Director agent to be installed on the target server. If you are using blade servers as targets, use the BladeCenter Assistant instead of the MPA. See 6.7.2, “BladeCenter Assistant” on page 228.

To launch the MPA, do the following:

1. Click the small bullet in front of the task Management Processor Assistant to expand its menu.
2. Click **Management** or **Configuration** with the left mouse button and drag and drop it onto the server whose systems management component you want to manage.

The Management Processor Assistant window, Figure 6-26 on page 228, appears. In the left pane select the task you want to do: Management, Configuration, or Communication from the pull-down menu.

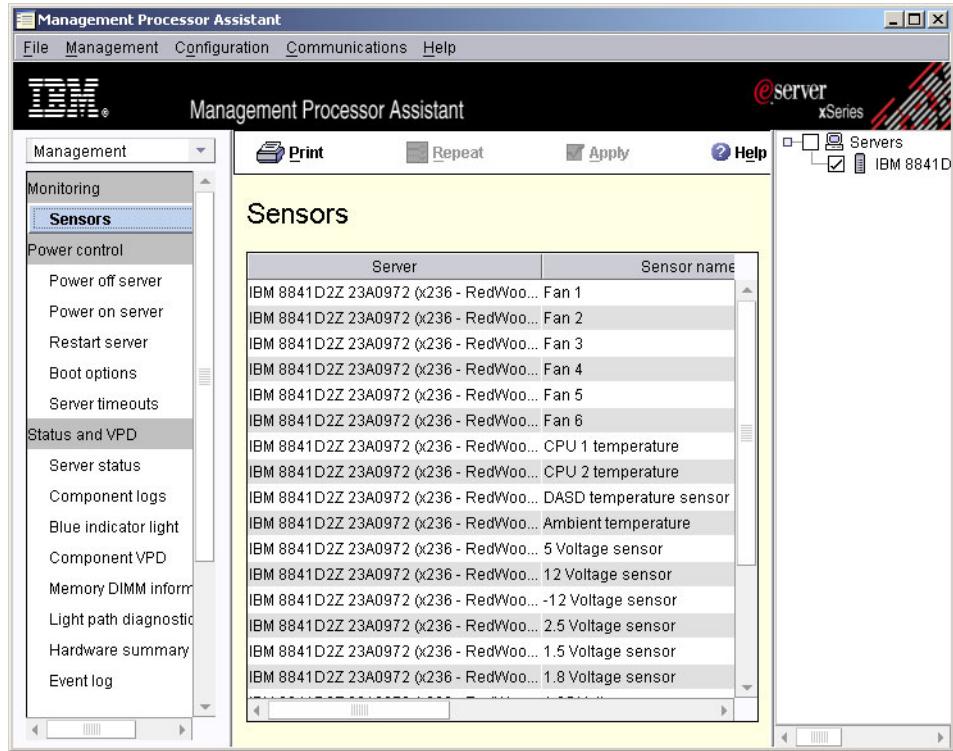


Figure 6-26 Management Processor Assistant of IBM Director

As you can see, the MPA is very similar to the Web interface of the RSA II.

6.7.2 BladeCenter Assistant

The BladeCenter Assistant of IBM Director works similar to the MPA. It has some additional BladeCenter-specific tasks. To launch it, do the following:

1. Click the small bullet in front of the task BladeCenter Assistant to expand its menu.
2. Click **BladeCenter Management** or **BladeCenter Configuration**.
3. Click **BladeCenter Management** or **BladeCenter Configuration** and drag and drop it onto the BladeCenter you want to manage.

The Management Processor Assistant for BladeCenter window appears. In the left pane select the task you want to do from the pull-down menu: Management or Configuration.

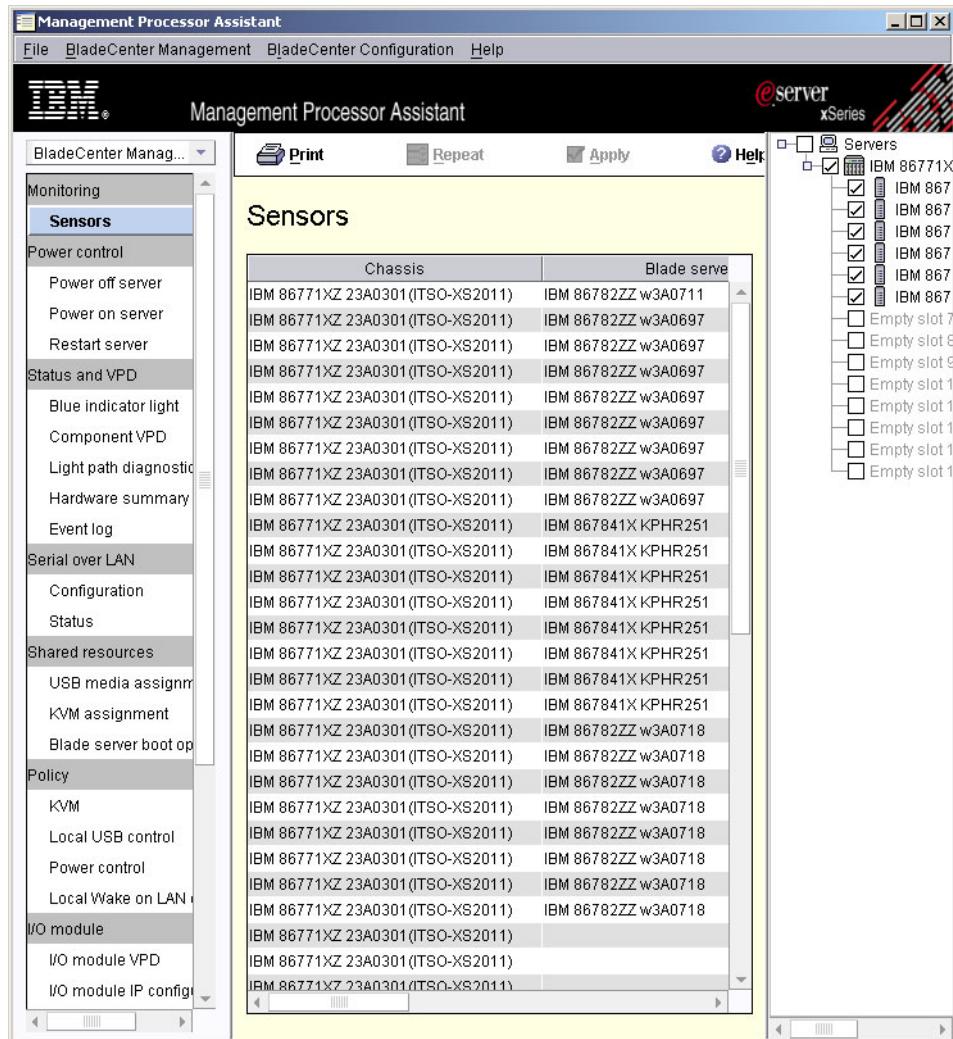


Figure 6-27 BladeCenter Assistant of IBM Director

6.7.3 Alerting

IBM Director can act as an alert destination for xSeries service processors and the management module. To make the systems management hardware send alerts to the IBM Director server, configure the hardware as follows.

To configure alert forwarding to IBM Director:

- ## 1. Launch the Web interface.

2. Log in.
3. Click **ASM Control (MM Control** if using BladeCenter management module) → **Alerts** in the navigation frame.
4. Click one of the ~not used ~ entries.

Remote Alert Recipient 12

Receives critical alerts only

Status	Enabled
Name	X345DIRSERVR
Notification method	IBM Director (comprehensive)
Number	9.42.171.237
PIN	[redacted]
E-mail address (userid@hostname)	[redacted]

Reset to Defaults | Cancel | Save

Figure 6-28 Configure alerting

5. Enter values as follows.

Check **Receives critical alerts only** if you want to receive critical alerts only. To view the list of critical alerts, click the **Alerts** link on the navigation frame and scroll down to the Monitored Alerts section. Critical alerts are listed there.

To allow alerts to be sent to this recipient, click the pull-down button and select **Enabled**.

Enter the name of the person or system who is to receive the alerts.

Select **IBM Director over LAN** or **IBM Director (comprehensive)** from the Notification method pull-down. When you chose the comprehensive entry, IBM Director will discover the systems management hardware automatically. If you select the other entry you have to force IBM Director to discover it.

In the field number enter the IP address or host name of the IBM Director server. If you enter the host name, ensure that name resolution works.

6. Click **Save** when you have finished.

When the IBM Director receives an alert it is automatically added to the event log.

Tip: If a RSA II is part of an ASM network it can work as a gateway of the connected systems management processors. To do so click **Make this ASM the Gateway** in the Alert Forwarding section. There can be only one gateway per ASM network.

To test the functionality click **Generate Test Alert** in the Remote alert recipients section. Check the event log of IBM Director for the test entry.

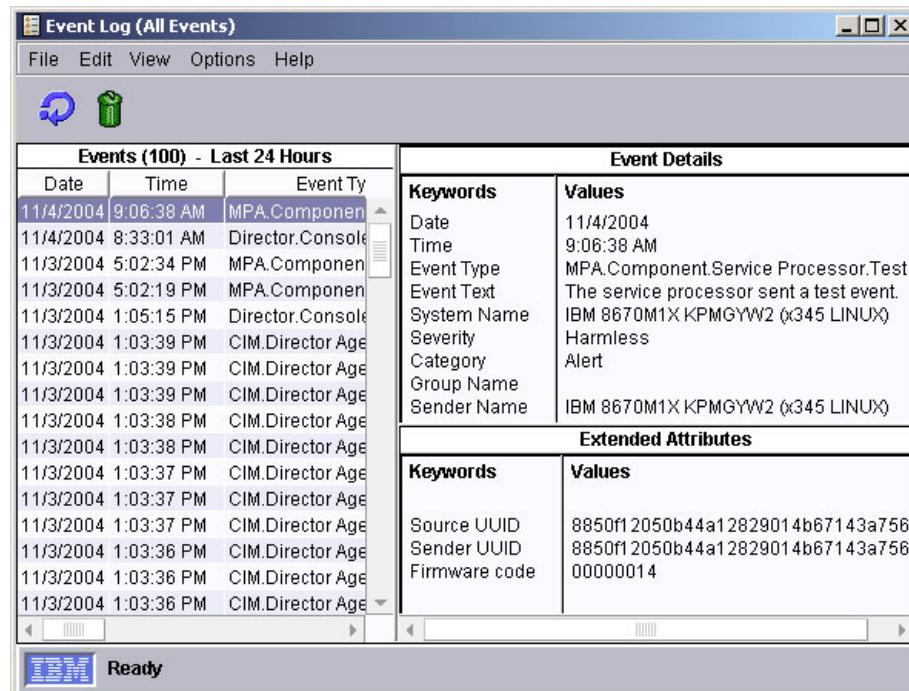


Figure 6-29 IBM Director event log entry for test alert

Now that the events are being sent to IBM Director, the next step is to configure IBM Director to process these events using an Event Action Plan. Refer to *Implementing Systems Management Solutions using IBM Director*, SG24-6188, for details on this activity.



Scenarios and best practices

This chapter describes examples of how to put the service processors and the management interfaces to work. Topics in this chapter are:

- ▶ 7.1, “Securing communication and authentication” on page 234
- ▶ 7.2, “Backing up and restoring the configuration” on page 236
- ▶ 7.3, “Provide remote access to all BladeCenter modules” on page 239
- ▶ 7.4, “Multi-subnet environment” on page 243
- ▶ 7.5, “Mass configuration of user IDs and passwords” on page 245
- ▶ 7.6, “Resetting the RSA II back to factory defaults” on page 248
- ▶ 7.7, “How to use ASU remotely” on page 253
- ▶ 7.8, “Remote BIOS and firmware updates” on page 256
- ▶ 7.9, “UpdateXpress firmware update scripts for BladeCenter” on page 274

7.1 Securing communication and authentication

There are steps you can take to secure communication and authentication with your systems management hardware. In this section, we summarize the best practices in this area. For details, review Chapter 5, “Security and authentication” on page 129.

Note: The steps we provide here do not secure your environment completely. The intention is to secure as best as possible using the abilities the systems management hardware has.

Data like user IDs, passwords, and configuration files should be secured by encryption, and the access should be restricted.

7.1.1 General considerations

When choosing passwords, do not use expressions that are easy to guess like password, ibm, rsa, or your company name. Keep the passwords in a secure place and make sure that access to the passwords is restricted. Implement a password policy for your company.

Here are some other general issues to consider:

- ▶ Where possible and practical, place the systems management hardware in a separate subnet. Only users in that LAN (typically the administrators group) should have access to it. No normal user should be able to get to the Web interface of a systems management hardware by accident.
- ▶ For each service processor, change the password of default user USERID. Better still, create a new supervisor user with a different ID and password, and delete the default user USERID on every service processor. The MPCLI can be used to perform this in batch; see 6.3, “Management processor command-line interface” on page 175.
- ▶ When an LDAP server is available, configure LDAP for user authentication on all service processors that support it (RSA II, BladeCenter management module). Activate SSL for the LDAP communication (refer to “Configure a secure LDAP client” on page 135, and 5.2, “Authentication using LDAP” on page 139). Have at least one supervisor user defined locally on every service processor just in case you have LDAP problems.
- ▶ Use the different authorization levels for different users. Do not allow all users to work with the same supervisor user ID.

- ▶ For BladeCenter chassis, install a redundant management module to provide access even if the primary management module fails. Refer to 4.3, “Redundant management modules” on page 97.
 - ▶ Do not enable the external management ports of the BladeCenter Ethernet switch modules (ESMs). This will ensure that you separate the management traffic from the production LAN traffic. Instead, use the connection of the management module to the internal Ethernet interfaces of the ESMs.
 - ▶ If you have a server with BMC and RSA II SlimLine installed, make sure to disable the unsecured direct communication to the BMC by setting its IP address to 0.0.0.0. See 3.2.3, “Remote Supervisor Adapter II SlimLine” on page 53, for details.
 - ▶ If you are using IBM Director, make sure that encrypted communication between the server and the agent is enabled. See Chapter 5 of the IBM Redbook *Implementing Systems Management Solutions using IBM Director*, SG24-6188.
 - ▶ Make sure that at least critical firmware updates are installed. Check the IBM support Web site at <http://www.pc.ibm.com/support> for available updates.
- You can also use IBM UpdateXpress Server to make updates available from a server on your network. UpdateXpress Server is a Web-based program that you can use to manage multiple versions of IBM device drivers and firmware updates from a central repository within your network. It is available from:
- <http://www.ibm.com/pc/support/site.wss/MIGR-57426.html>
- ▶ After making any changes, back up the configuration of your service processors. Refer to 7.2, “Backing up and restoring the configuration” on page 236, for details.

7.1.2 Web interface

To secure the Web interface of RSA II or BladeCenter management module use SSL. For details on configuring SSL, see 5.1.1, “Secure Sockets Layer (SSL)” on page 130.

Additionally, you can change the port of the HTTPS protocol for additional security. This can be done as follows:

1. Click **ASM Control** (or **MM Control** when using management module) → **Port Assignments** in the navigation frame.
2. Change the port number of HTTPS.
3. Click **Save**.
4. To activate the change click **Restart ASM** (or **Restart MM**).

With a new port number, you would then access the Web interface with the following URL (for example, if the port you select is 4711):

<https://9.42.171.241:4711>

7.1.3 Command-line interfaces

All command-line interfaces (CLIs) are not secure by default. The exception to this is Secure Shell (SSH).

Telnet and Secure Shell (SSH)

Disable the telnet service of RSA II and activate SSH instead. For activating and using SSH refer to 5.1.2, “Secure Shell (SSH)” on page 135.

When using a server with RSA II installed, check first if it supports SSH connection, then disable the telnet service. Some older servers do not support SSH. If your server does not support SSH use the Web interface instead.

Tip: To check if SSH is available for your combination of server and RSA II, launch the Web interface, click **ASM Control → Security**, and check if there is a Secure Shell (SSH) Server section.

When you are using a BladeCenter management module, you cannot disable the telnet protocol. Activate the SSH protocol, change the port of telnet, but use SSH instead of telnet. For instructions on how to change the port of a protocol like telnet refer to 7.1.2, “Web interface” on page 235.

MPCLI

At the time of publication, the current version of the MPCLI does not offer a way to encrypt communications.

ASU

The advanced settings utility (ASU) works only locally at the server. No network connection is used for the communication between ASU and the server. There is no need to secure this communication, assuming that the server itself is secured.

7.2 Backing up and restoring the configuration

Once you have finished configuring the RSA II or BladeCenter management module, we recommend that you back up the configuration in case you have a need to restore it.

7.2.1 Backup procedure

To save the configuration to a file, launch the Web interface:

1. Click **ASM Control** (or **MM Control** when using management module) → **Configuration File** in the navigation frame.
2. Click **Backup** to save your configuration.

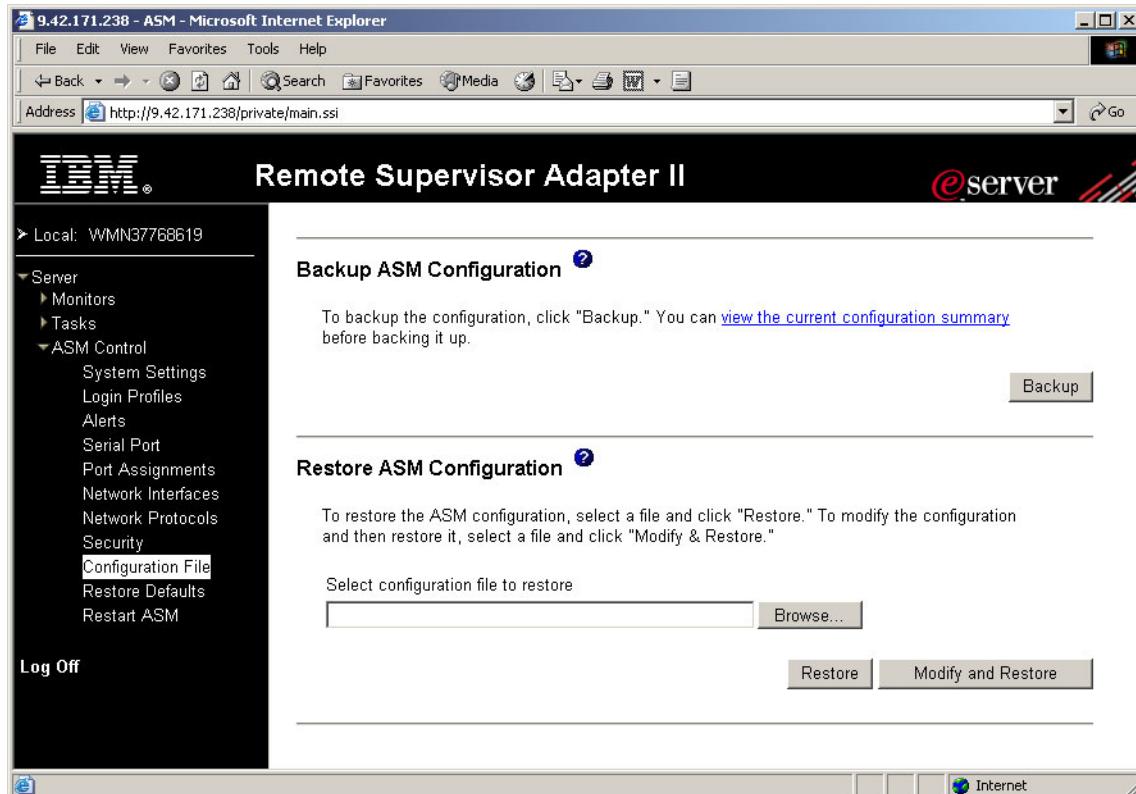


Figure 7-1 Backup configuration

3. The file download window pops up. Choose the folder and file name for the file and click **Save**.

Tip: If you use one directory to save the configurations files of more than one systems management hardware, be sure to name the backup files appropriately. Choose a file name that corresponds to the server or BladeCenter where the service processor is installed. If you have to restore a configuration, the correct file will then be easier to find.

7.2.2 Restore procedure

If you want to restore a configuration, use the same panel as shown in Figure 7-1 on page 237.

1. Click **ASM Control** (or **MM Control** when using management module) → **Configuration File** in the navigation frame. Figure 7-1 on page 237 appears.
2. In the Restore ASM Configuration section, click **Browse** and select the configuration file you want to restore.
3. Click **Restore** if you want to restore the original settings or **Modify and Restore** if you want to view or modify the settings before restore.
4. If you click **Modify and Restore**, you will see Figure 7-2, where you can enter any changes. Click **Restore Configuration** to proceed.

The screenshot shows a software interface titled 'Restore ASM Configuration'. At the top right are buttons for 'Toggle View', 'Cancel', and 'Restore Configuration'. Below this is a section titled 'ASM Information' containing fields for Name (WMN37768619), ID number (37768619), Contact (No Contact Configured), Location (No Location Configured), and Host OS (Other). A note below says '~~~~~ Section(s) Hidden ~~~~~'. The next section is 'Ethernet' with fields for Interface (Enabled), DHCP (Disabled - Use static IP configuration), and Hostname (ASMA00096B9E085C). The final section is 'Static IP Configuration' with fields for IP address (9.42.171.238), Subnet mask (255.255.255.0), Gateway address (9.42.171.3), Data rate (Auto), Duplex (Auto), MTU (1500), and Locally admin. address (00:00:00:00:00:00).

Figure 7-2 Restore configuration file

5. After restoring, you have to restart the RSA II or management module. Click **Restart ASM** (or **Restart MM** if using management module).

Tip: You can restore a saved file from one RSA II to another RSA II or from one management module to another too, when they have similar configurations. Make sure you modify the information and IP configuration parameters in the configuration file before restoring it.

7.3 Provide remote access to all BladeCenter modules

To access and manage the switch modules in a BladeCenter, the management module (external and internal interface) and the switch modules must reside in the same IP subnet.

Note: If there is a redundant management module installed, the IP configuration will be retrieved from the active module. Do not configure the IP settings of the redundant module; in the event management functions failover to the redundant module, it will take on the IP configuration of the failed primary module.

The management module has an external and an internal Ethernet interface, as shown in Figure 7-3 on page 240.

- ▶ External Ethernet: DHCP configured or static (default is 192.168.70.125)
- ▶ Internal: Static (default is 192.168.70.126)

From the management module, you can also connect to the Web interfaces of any of the Ethernet switch modules (ESMs) in bays 1, 2, 3, and 4. These ESMs have the following default addresses:

- ▶ 192.168.70.127 (bay 1)
- ▶ 192.168.70.128 (bay 2)
- ▶ 192.168.70.129 (bay 3)
- ▶ 192.168.70.130 (bay 4)

By default, the ESMs are not accessible from the external production ports of the switch modules. We recommend that you keep it this way, thereby maintaining a single entry point into chassis management, via the management module. If you do enable them, you will need to configure addresses that are valid on your production network.

The internal interface of the management module is connected to the management interfaces of the ESMs in bays 1–4. The addresses of the connections to the switch modules are shown in Figure 7-3 on page 240.

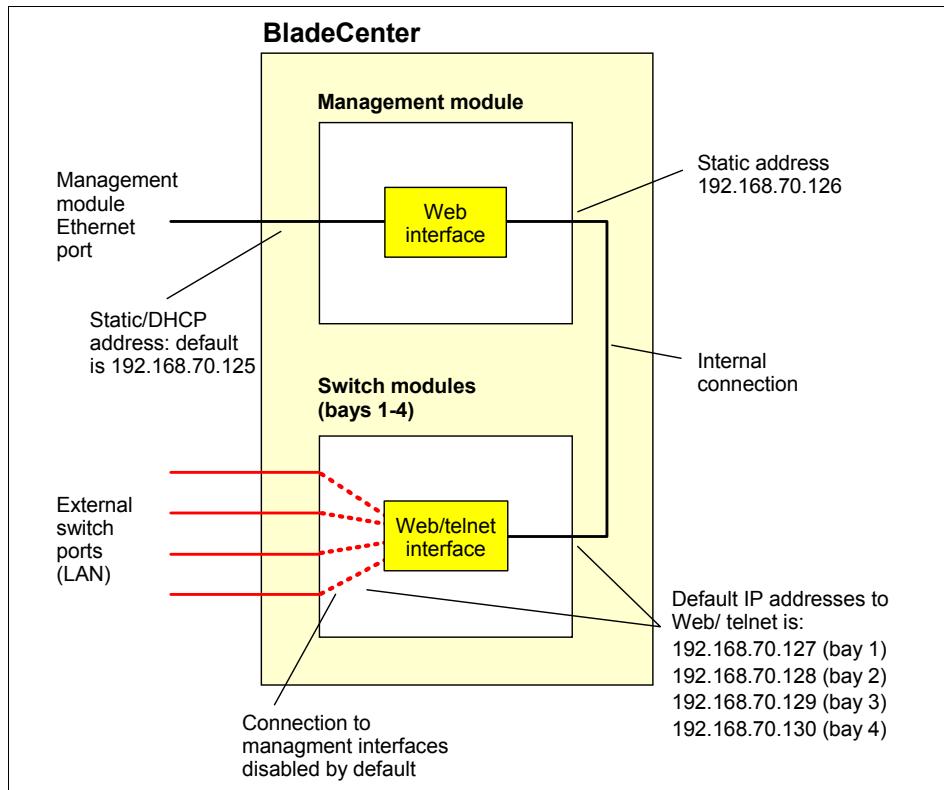


Figure 7-3 BladeCenter internal Ethernet

The ESMs have an additional external interface you can configure for management. This external interface is disabled by default. To have a single point of administration for a BladeCenter you should not enable this interface, especially when the management module is connected to a management LAN and the ESM external interface is connected to the production LAN.

Tip: To separate the management tasks from the production LAN you should build a dedicated Ethernet segment for management purposes. This could be a VLAN or a physically separate LAN. A dedicated management LAN eases control of the access to the systems management hardware for users and computers.

Additionally, the production LAN will not be influenced when using remote media, for example, for installation purposes. Use a dedicated PCI network adapter to connect your servers to the management LAN if you use additional software for systems management.

Details on how to configure the external Ethernet interfaces of the management module can be found in 4.2.2, “Network settings” on page 92.

The next step is to configure the internal IP addresses of the management module and all other switch modules. All internal interfaces have default IP addresses. To change them, launch the Web interface of the management module and complete the following steps:

1. Click **MM Control** → **Network Interfaces**.
2. Scroll down to the Internal Network Interface (eth1).
3. Make sure that the interface is enabled.
4. Enter the IP configuration parameters.
5. Click **Save**.

Now configure the internal IP interface for all installed modules:

1. Click **I/O Module Tasks** → **Management**.
2. Enter the IP configuration parameters.
3. Click **Save**.
4. Repeat steps 2 to 3 for all installed modules.

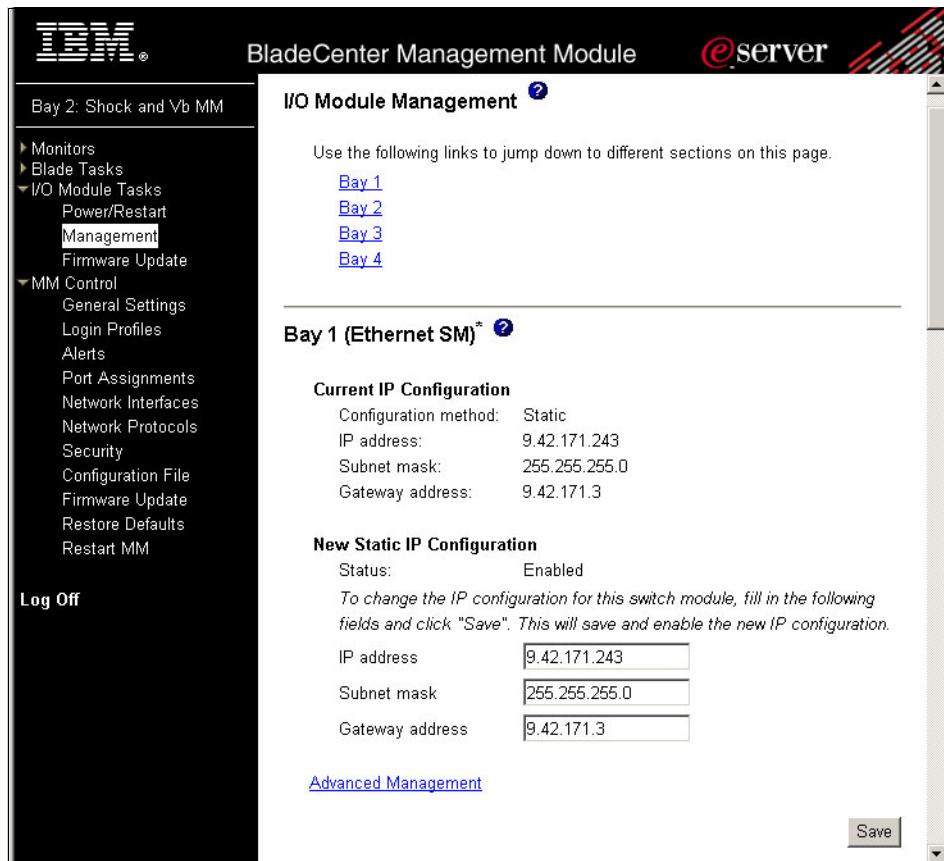


Figure 7-4 Configure IP settings of I/O modules

To test the configuration, do the following for all switch modules:

1. Click **Advanced Management**.
2. Click **Send Ping Requests**.
3. Click **Ping Switch Module**. It should look like the figure below.

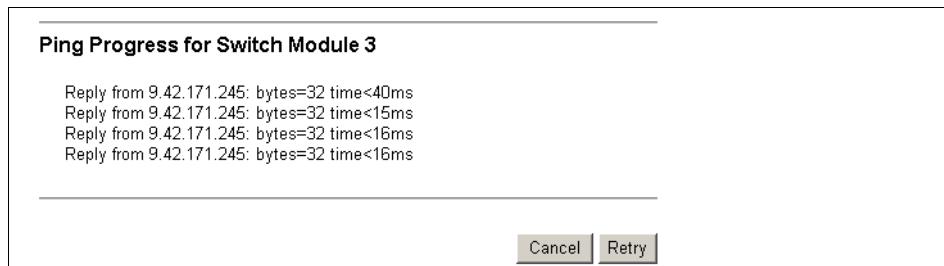


Figure 7-5 Ping request

Make sure that all switch modules answer the ping request. Now you can access each module's Web interface via the management module or directly by launching a browser with the module's IP address.

To manage the switch modules, refer to the documentation that came with the module.

7.4 Multi-subnet environment

In this scenario, your network is divided into three separate subnets: Production, test, and management. You have to implement a hardware-based systems management solution.

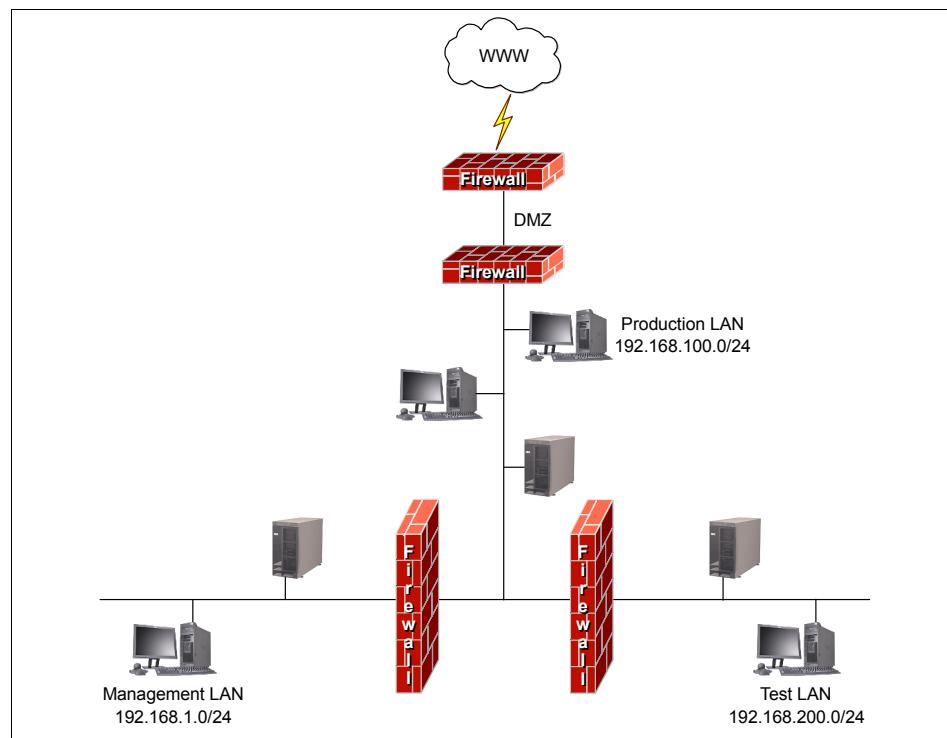


Figure 7-6 Example for a network with three subnets

7.4.1 General considerations

Connect the Ethernet ports of the RSA II adapter and BladeCenter management modules to the management LAN.

For servers with integrated BMCs (such as the x236, x336, or x346) and no RSA II SlimLine installed, it is important to realize that the BMC shares one of the system Ethernet ports with the operating system, so it will be connected to the production network. There are two possibilities.

Tip: Refer to the documentation that came with your server for which of the two Ethernet ports the BMC uses. Usually the Ethernet port that the BMC uses is the one nearer to the power supply.

- ▶ Use only one Ethernet port for the operating system and make the other one dedicated for use by the BMC:
 - a. Configure the BMC with IP settings of the management LAN and connect the Ethernet cable to it.
 - b. Disable the Ethernet port used for BMC in the operating system.
- ▶ Use both Ethernet ports for the operating system and share one of them with the BMC.
 - a. Configure the BMC with IP settings of the production network.
 - b. Make sure that the BMC can reach the management LAN and vice versa.

Note: We recommend that you use the second option to have redundant Ethernet connections for the operating system. If you do not have the requirement of redundant Ethernet ports, use the first option.

7.4.2 Access to other subnets

To connect to the management network, for example, from the administrator's desktop on the production network, the connecting devices (routers and firewalls) must be configured properly.

Test the routing of TCP/IP with the **ping** command. Make sure that ping (ICMP) packets are allowed through your firewall. You may need to open ports. Check the tables in 3.6, "Ports used by Remote Supervisor Adapter II" on page 85, and 4.6, "Ports used by the management module" on page 126, for the appropriate port numbers.

Tip: The MPCLI uses the same port as for IBM Director commands: TCP port 6090.

Make sure that only the ports that are really needed and will be used are opened. Open these ports only for the group of users that need to have access to the service processors.

7.4.3 DHCP in different subnets

If a DHCP server is installed, it will only provide IP addresses for DHCP clients in the same subnet, because it works with broadcasts that are normally not forwarded by a router. If your routers are RFC 1542 compliant (meaning they can route DHCP Discover packets to other subnets), it will work and you do not have to consider the options below. If not, you have two options to enable DHCP in the other two subnets:

- ▶ Install one DHCP server in each of the other two subnets.
- ▶ Install DHCP relay agents in the other two subnets. You can install a DHCP relay agent on servers running Windows or Linux, for example.

When preboot execution environment (PXE) in conjunction with deployment services like the IBM Remote Deployment Manager (RDM) is used, make sure that the DHCP server provides the BOOTP protocol as well.

7.5 Mass configuration of user IDs and passwords

In this scenario we look at ways to do a mass configuration of user IDs and passwords for the RSA II and the BladeCenter management module. This scenario is very useful when you have a large number of servers to configure, or if your company policy specifies a password change at regular intervals.

The utility we use in this scenario is the MPCLI, which we discuss in 6.3, “Management processor command-line interface” on page 175.

Creating the script file

First, create the script file chnguidpwd.script, as shown in Example 7-1. This script changes (or creates) user ID ADMIN3 on server 9.42.171.216.

Tip: As an alternative to creating the script using a text editor, you could also use the interactive mode of generating the script using the **commandfile** command. See “Scripting with the MPCLI commands” on page 186.

Example 7-1 Script c:\IBM\chnguidpwd.script

```
logonip -hostname 9.42.171.216 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
```

logoff

Duplicate these commands for each of the servers in your environment. Be sure to specify logoff after each RSA/BCMM is changed. For example, we have four systems to maintain, so our script is as follows.

Example 7-2 Modified script to run against all four systems

```
logoff
logonip -hostname 192.168.70.120 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
logonip -hostname 192.168.70.121 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
logonip -hostname 192.168.70.122 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
logonip -hostname 192.168.70.123 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
```

Tip: You can also include comments in the script files by starting each comment line with a # character. For example:

```
#Ensure you are not logged into another Service Processor.
logoff
```

To execute the script, issue the following command at the mp> prompt:

```
inputfile c:\IBM\chnguidpwrd.script
```

The output of each command in the script file will be displayed on screen. For our example, the output is as follows.

Example 7-3 Output from our script

```
mp> inputfile c:\ibm\chngspuid.script
FAILURE: You are not logged in.
SUCCESS: logonip -hostname 9.42.171.238 -userid USERID -password PASSWORD
SUCCESS: setdialinentry -index 2 -id ADMIN2 -password ADMIN2 -dialback false
-readonly false
SUCCESS: setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false
-readonly false
SUCCESS: setdialinentry -id ADMIN3
true
```

```
SUCCESS: setdialinentry -password ADMIN3
true
SUCCESS: setdialinentry -dialback false
true
SUCCESS: setdialinentry -readonly false
true
SUCCESS: logoff
SUCCESS: logonip -hostname 9.42.171.216 -userid USERID -password PASSWORD
SUCCESS: setdialinentry -index 2 -id ADMIN2 -password ADMIN2 -dialback false
-readonly false
SUCCESS: setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false
-readonly false
SUCCESS: setdialinentry -id ADMIN3
true
SUCCESS: setdialinentry -password ADMIN3
true
SUCCESS: setdialinentry -dialback false
true
SUCCESS: setdialinentry -readonly false
true
SUCCESS: logoff
mp>
```

Note: Even though in the above output it states FAILURE, this is not actually a failure. MPCLI will give this output when you are not logged on and you try to log off.

If you want to check whether the command executed correctly, you could check this via the Web interface for the specific server. See Figure 7-7 on page 248 for an example of the Web interface updated with the above changes.

Login Profiles	
To configure a login profile, click a link in the "Login ID" column.	
Access	Login ID
Read/Write	1. USERID
Read/Write	2. ADMIN2
Read/Write	3. ADMIN3
~ not used ~	4. ~ not used ~
~ not used ~	5. ~ not used ~
~ not used ~	6. ~ not used ~
~ not used ~	7. ~ not used ~

Figure 7-7 Viewing change in RSA II login profiles after script file completes

7.6 Resetting the RSA II back to factory defaults

This section describes how to return the RSA or RSA II back to the factory default settings.

Notes: Changes made include the following:

- ▶ Reset the user ID and password back to the default setting USERID and PASSW0RD (with a zero and not the letter o).
- ▶ For the RSA II, change the IP address back to the default setting of DHCP, then static, with a static IP address 192.168.70.125 and subnet mask 255.255.255.0.
- ▶ For the RSA, change the IP address back to the default setting of DHCP with no static backup.
- ▶ Reset the host name back to ASMA +, the MAC address of the service processor (for example, ASMA00096b0a8469).

An easy way to reconfigure these service processors after resetting them is connecting via an ASM interconnect network connection.

There are four ways to perform this task.

- ▶ ASU: See below.
- ▶ IBM Director: See “Using IBM Director” on page 250.
- ▶ MPCLI: See “Using MPCLI” on page 252.
- ▶ Web interface (select **Restore Defaults** from the navigation menu).

The ASU and IBM Director methods do not require that you know a valid user ID and password on the service processor. The MPCLI, however, does require that you know this information.

7.6.1 Using ASU

You would need to use ASU to reset the RSA or RSA II back to factory defaults if the administrator has forgotten the IP address, user ID, and/or password, or the service processor (or left the company), and your company has not implemented IBM Director.

To reset the adapter to factory defaults using ASU, do the following:

1. Install ASU locally on the server (see 6.2, “Advanced Settings Utility” on page 160).
2. Add the RSAI/RSAII definition file to ASU (see 6.2.4, “Using the ASU definition files” on page 163).
3. Enter the following command to reset the service processor:
 - For Windows: `asu resetrsa`
 - For Linux: `./asu resetrsa`
4. The service processor will be reset to the factory defaults and then be restarted.
5. You may also wish to configure some of the basic settings using ASU:
 - Disable DHCP.
 - Set a static IP address, subnet mask, and gateway.
 - Replace the default user ID with a new one (for example, `u=lesley`, `p=ba1n`).

Use the SET commands as shown in Example 7-4 (for Linux use `./asu` instead of `asu`). See Example 6-1 on page 166 for a complete list of SET commands.

Example 7-4 ASU commands to configure basic RSA settings

```
asu set RSA_DHCP1 Disabled
asu set RSA_Network1 Enabled
asu set RSA_HostIPAddress1 xxx.xxx.xxx.xxx
asu set RSA_HostIPSunet1 xxx.xxx.xxx.xxx
asu set RSA_GatewayIPAddress1 xxx.xxx.xxx.xxx
asu set RSAString_loginId1 "lesley"
asu set RSAString_Password1 "ba1n"
```

Tip: See 6.2.8, “ASU batch commands” on page 174, for information on how to issue these commands in batch.

7.6.2 Using IBM Director

IBM Director also has the capability to reset the RSA and RSA II settings back to the factory defaults. You will need:

- ▶ IBM Director Agent installed on the server where you have the service processor you are wishing to reset (we will call this the target server)
- ▶ The appropriate service processor drivers installed for your server
- ▶ IBM Director Server installed on a server in your network

To reset the adapter to factory defaults using IBM Director, do the following:

1. Using the IBM Director management console, ensure that the target server has been discovered by IBM Director.
2. Expand the **Management Processor Assistant** task in the Tasks pane.
3. Select **Configuration** subtask and drag and drop it on to the target server. Figure 7-8 on page 251 opens. If you are not able to connect to the service processor you will see a pop-up message. Verify that the service processor driver is installed correctly.

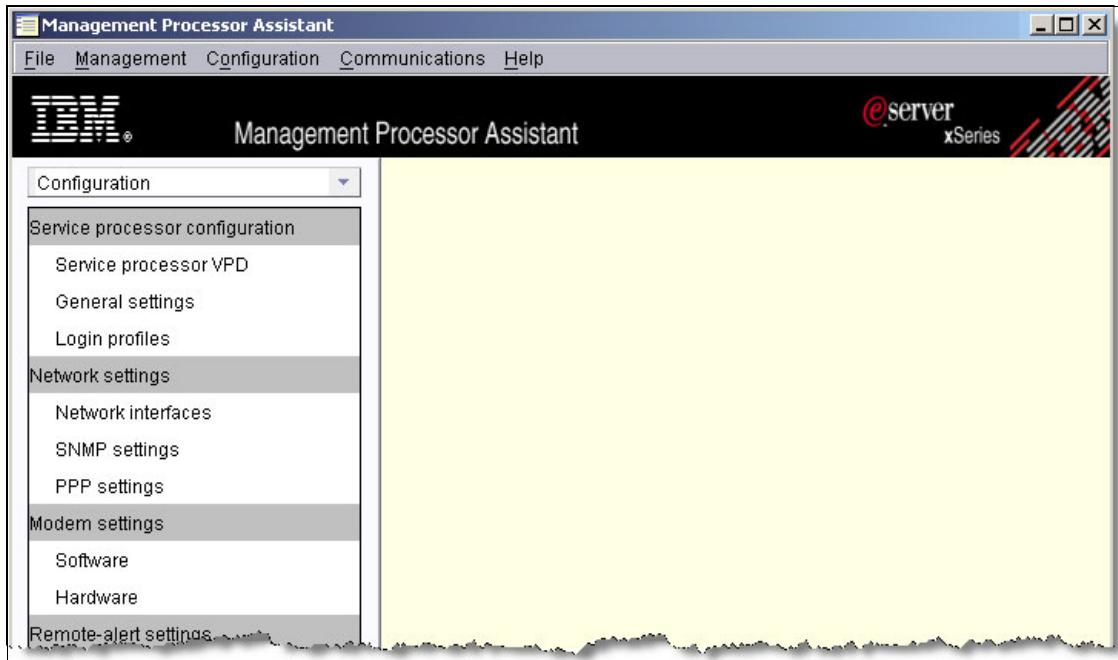


Figure 7-8 IBM Director MPA configuration view

4. To restore the service processor factory defaults, click **General settings**. Figure 7-9 appears.

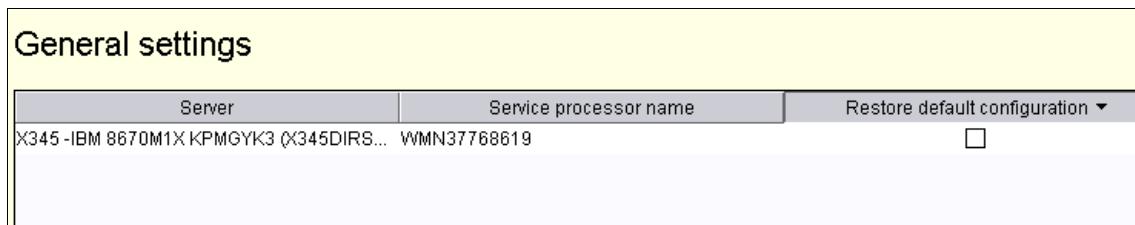


Figure 7-9 General settings window within the MPA configuration window

5. Check the check box under the heading Reset default configuration (scroll to the right if necessary; see Figure 7-9).
6. Click **Apply** in the menu above to save your changes to the service processor.
7. All the factory defaults should now be set again, ready to be reconfigured either via this interface or another of your choice.

Note: There are no security risks with either of the above tasks to reset the RSA or RSAII adapter. ASU is secure because this is a local tool and will only be installed by the company system administrator. IBM Director is fully secure, as there is a requirement to have a user ID and password to log on to the IBM Director management console.

7.6.3 Using MPCLI

If you know the IP address, user ID, and password of the service processor, you can reset the configuration back to the factory defaults using the MPCLI utility. The MPCLI is useful when the server does not have an operating system installed that you can log into.

To reset the adapter to factory defaults using MPCLI, do the following:

1. Install the MPCLI on another workstation. See 6.3.5, “Installing the MPCLI” on page 181, for details.
2. Start the MPCLI:
 - Windows: **Start → Programs → IBM → MPCLI → MPCLI**
 - Linux: **/opt/IBMmpcli/bin/MPCLI.bsh**
3. At the MPCLI command prompt type in the following command (substituting your own values for service processor IP address, user ID, and password):
logonip -hostname xxx.xxx.xxx.xxx -userid userid -password password
4. Enter the following command to reset the service processor:
resetmp

Note: Default network configurations are as follows:

- ▶ RSA II: Use DHCP if it can reach a DHCP server, or failing that, to set the static address 192.168.70.125, subnet 255.255.255.0.
- ▶ RSA: Use DHCP. If no DHCP server can be found, no IP address is assigned.

5. You may also wish to configure some of the basic settings using the MPCLI:
 - Disable DHCP.
 - Set a static IP address, subnet mask, and gateway.
 - Replace the default user ID with a new one (for example, u=lesley, p=ba1n).

You can use scripting for this task. Refer to “Scripting with the MPCLI commands” on page 186. The commands used for this task are as shown in

Example 7-5 (substitute the DHCP-assigned address for the service processor in the **logonip** command, if applicable).

Example 7-5 MPCLI commands to set basic defaults

```
logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
setnethw -interface 1 -enabled true
setdhcp -enabled false
setip -interface 1 -method static
setip -interface 1 -ipaddress xxx.xxx.xxx.xxx
setip -interface 1 -gateway xxx.xxx.xxx.xxx
setip -interface 1 -subnet xxx.xxx.xxx.xxx
setdialinentry -index 1 -id userid -password password -dialback false -readonly false
```

Note: There are three method types applicable for the RSA II (the RSA only supports the first two):

- ▶ static - Uses the static IP address
- ▶ dhcp - Gets an assigned IP address from a DHCP server
- ▶ dhcpstatic - Uses static IP address if DHCP server is not available

7.7 How to use ASU remotely

As described in 6.2, “Advanced Settings Utility” on page 160, ASU is a utility designed to be installed and run locally on the server. However, with the use of IBM Director’s File Transfer and Remote Console tasks, you can install and use the ASU tool remotely.

This scenario could help when, in a lights out remote environment, you need to make changes to the server’s CMOS or RSA/RSA II adapter settings without restarting the server.

We make the following assumptions for this scenario:

- ▶ You already have an IBM Director management server installed in your environment.
- ▶ You have already installed IBM Director Agent on the server you want to use the ASU utility with.
- ▶ You have IBM Director console installed at your remote location, for example, on your laptop, and you are able to connect to the IBM Director server.
- ▶ You are able to discover the IBM Director Agent from the IBM Director management server.

- ▶ You have downloaded the required ASU code to your laptop or remote location. For details on what code is required, refer to 6.2.3, “Downloading ASU and definition files” on page 162.

Refer to the *IBM Director Installation Guide* for details on installation of the agent and server portions of IBM Director.

Using ASU remotely can be done as follows:

1. Open and connect to the IBM Director server from your remote console.
2. Once connected, select the task **File Transfer** in the right-hand pane, and drag and drop this onto the server you want to use ASU with. The file transfer window will now open. See Figure 7-10.

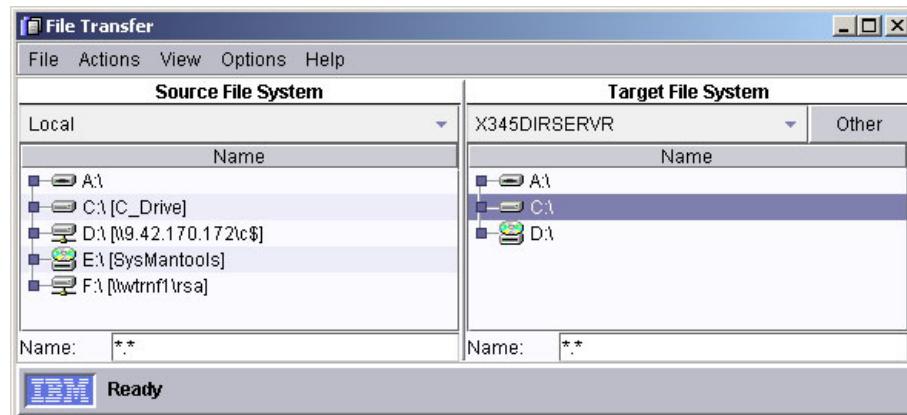


Figure 7-10 File transfer window

3. From the local (left) pane navigate to and expand the directory you downloaded the ASU tool to. See Figure 7-11 on page 255.

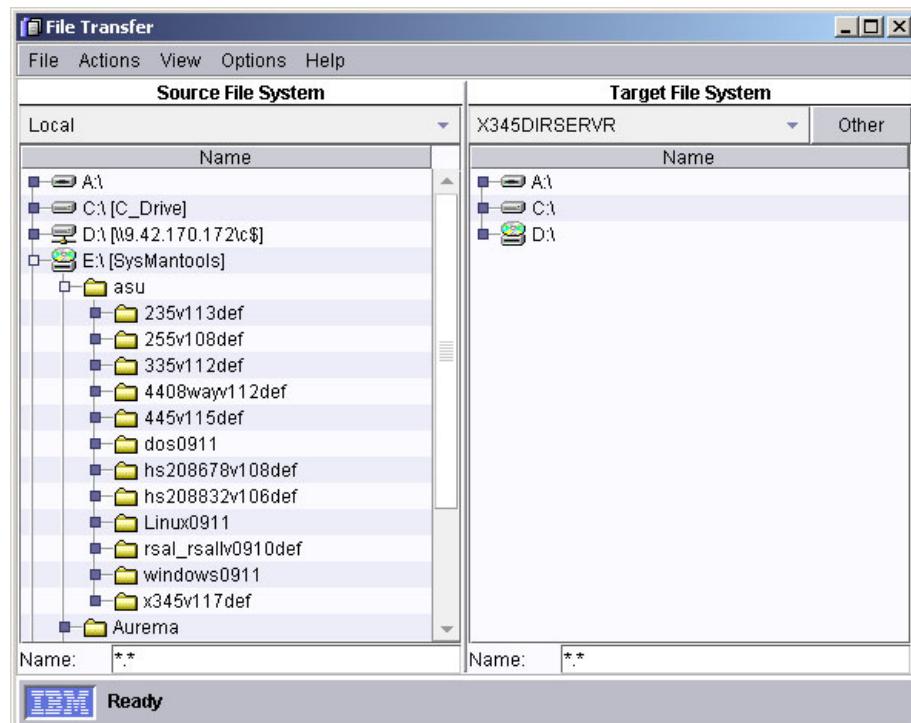


Figure 7-11 ASU download directory location on local

4. Expand the directory on the remote server where you want to copy the ASU files to.
5. Select the ASU files from local system and drag and drop them on the remote directory location.
6. You are now ready to install ASU on this remote server. Refer to the instructions in 6.2.3, “Downloading ASU and definition files” on page 162, to unpack the ASU files; and 6.2.4, “Using the ASU definition files” on page 163, to add the required definition files to ASU.
7. Once you have completed the configuration of ASU, you can now begin to operate remotely.
8. From the director console select the **Remote Session** task and drag and drop it onto the system you want to use ASU with. The remote session will open. You can now begin to work remotely and issue ASU commands to the server. See Figure 7-12 on page 256 for an example of using the IBM Director remote session task to issue ASU commands remotely.

```
C:\ASU\windows0911>asu patchlist
Patch 1: <XX[00->99] (RSA)>
Patch 2: <GE[57->57] (BIOS)>

C:\ASU\windows0911>asu version
eserver xSeries Advanced Settings Utility 0.9.11 Feb 12 2004
IBM Corporation
eserver xSeries Engineering Software

C:\ASU\windows0911>asu set RSAString_loginId3 Leitenberger
RSAString_LoginId3=Leitenberger

C:\ASU\windows0911>asu set RSAString_Password3 PASSWORD
RSAString_Password3=

C:\ASU\windows0911>asu set RSAString_loginId4 Bain
RSAString_LoginId4=Bain

C:\ASU\windows0911>asu set RSAString_Password4 PASSWORD
RSAString_Password4=
```

Figure 7-12 IBM Director remote session running ASU remotely

7.8 Remote BIOS and firmware updates

Every environment should have a change management procedure in place. This will ensure that your servers are always updated to the latest release of BIOS, firmware, and device drivers.

There are a number of ways to upgrade the service processor firmware and system BIOS of your servers:

- ▶ MPCLI (described in 7.8.1, “Using MPCLI to upgrade firmware” on page 257)
- ▶ IBM Director software distribution (described in 7.8.2, “Using IBM Director to upgrade firmware” on page 259)
- ▶ UpdateXpress RemoteUX (described in 7.8.3, “Using UpdateXpress RemoteUX to update firmware” on page 266)
- ▶ RSA II Web interface

- ▶ RSA II telnet/terminal interface
- ▶ Remote Deployment Manager

In this scenario example, we describe the first three methods. Table 7-1 lists what updates are possible with these five tools.

Table 7-1 Methods to remotely update SP firmware and system BIOS

Method	Update SP firmware	Update system BIOS
MPCLI	Yes	No
IBM Director Software Distribution	Yes	Yes
UpdateXpress RemoteUX	Yes	Yes
RSA II Web interface	Yes	No
RSA II telnet/terminal interface	Yes	No
Remote Deployment Manager	Yes	Yes

7.8.1 Using MPCLI to upgrade firmware

When using MPCLI you are only able to upgrade the firmware of the RSA, RSA II, and BladeCenter management module.

Download the firmware from:

<http://www.pc.ibm.com/support>

The files required are available as follows:

- ▶ BladeCenter management module: The BCMM firmware update PKT files are downloadable as a ZIP file. Be sure to download the specific management module firmware update for your configuration.
- ▶ RSA: The RSA firmware update files are downloadable as EXE files, which, when executed, will create a diskette containing the PKT files. There are two EXE files, one for each diskette required for the upgrade. Be sure to download the specific RSA firmware update for your server.
- ▶ RSA II: The RSA II firmware update PKT files are downloadable as a ZIP file. Be sure to download the specific RSA II firmware update for your server.

For our scenario we are going to remotely upgrade the BladeCenter management module firmware from Version 1.14 to Version 1.15:

1. Click **Start → Programs → IBM → MPCLI** to start the MPCLI.

2. When updating the RSA, RSAII, or BCMM firmware, you are required to upgrade the following three components:
 - Main application: CNETMNUS.PKT
 - Boot ROM: CNETBRUS.PKT
 - Remote control: CNETRGUS.PKT
3. The MPCLI commands required to perform this update are as shown in Example 7-6.

Note: You should substitute your own settings for the IP address, user ID, password, and directory location for the PKT files.

Example 7-6 Commands to update the firmware of the management module

```
mp> logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
mp> fwupdate -mn d:\bladecenter\CNETMNUS.PKT
mp> fwupdate -br d:\bladecenter\CNETBRUS.PKT
mp> fwupdate -vnc d:\bladecenter\CNETRGUS.PKT
mp> restartmp
mp> logoff
```

The output of each command is as shown in Example 7-7.

Example 7-7 Output from the firmware update

```
mp> logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
SUCCESS: logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
mp> fwupdate -mn d:\bladecenter\CNETMNUS.PKT
Interruptiong the firmware update can damage your system!
Please DO NOT cancel the operation while in progress.
FIRMWARE UPDATE: Started.
You must update ALL available firmware for Management Module and then must issue'restartmp' from the command line in order for 'fwupdate' to take affect.
mp> fwupdate -br d:\bladecenter\CNETBRUS.PKT
Interruptiong the firmware update can damage your system!
Please DO NOT cancel the operation while in progress.
FIRMWARE UPDATE: Started.
You must update ALL available firmware for Management Module and then must issue'restartmp' from the command line in order for 'fwupdate' to take affect.
mp> fwupdate -vnc d:\bladecenter\CNETRGUS.PKT
Interruptiong the firmware update can damage your system!
Please DO NOT cancel the operation while in progress.
FIRMWARE UPDATE: Started.
You must update ALL available firmware for Management Module and then must issue'restartmp' from the command line in order for 'fwupdate' to take affect.
```

```
mp> restartmp
SUCCESS: restartmp
PASSED: The management processor has been successfully restarted. Please Logoff and
reconnect.
mp> logoff
SUCCESS: logoff
```

4. The BladeCenter MM should now be at the upgraded level.

7.8.2 Using IBM Director to upgrade firmware

The added advantage of using IBM Director is that you can schedule when you want to perform the upgrade, and you can also upgrade multiple servers at one time.

In this scenario we upgrade all the firmware for the x345. This includes the following:

- ▶ x345 System BIOS
- ▶ x345 ISMP firmware
- ▶ x345 Diagnostics
- ▶ x345 RSA II firmware

We make the following assumptions with this scenario:

- ▶ You already have an IBM Director management server installed in your environment.
- ▶ You have already installed IBM Director Agent on the server you want to upgrade.
- ▶ You have IBM Director console installed at your remote location, for example, on your laptop, and you are able to connect to the IBM Director server.
- ▶ You are able to discover the IBM Director Agent from the IBM Director management server.

Refer to the *IBM Director Installation Guide* for details on installation of the agent and server portions of IBM Director.

Additionally, you will need to download the latest release of UpdateXpress. This is available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-53046.html>

UpdateXpress is a CD-ROM containing a self-starting program that allows you to maintain your system firmware and Windows device drivers at the most current levels defined on the CD, thus helping to avoid unnecessary outages.

UpdateXpress automatically detects current device driver and firmware levels and presents them to the user. It then gives you the option of selecting specific upgrades or allowing UpdateXpress to update all of the system levels it detected as needing upgrades.

The update files contained on the UpdateXpress CD can also be imported into IBM Director's Software Distribution task. This is the method we are going to use in this scenario.

Follow the steps below to upgrade the x345's firmware:

1. Insert the UpdateXpress CD into your CD drive at your remote location.
2. Open the IBM Director console and log in to your Director server.
3. Select the Software Distribution task, right-click the task, and select **Open**. The Software distribution manager window opens. Expand the Wizards file. See Figure 7-13 for details.

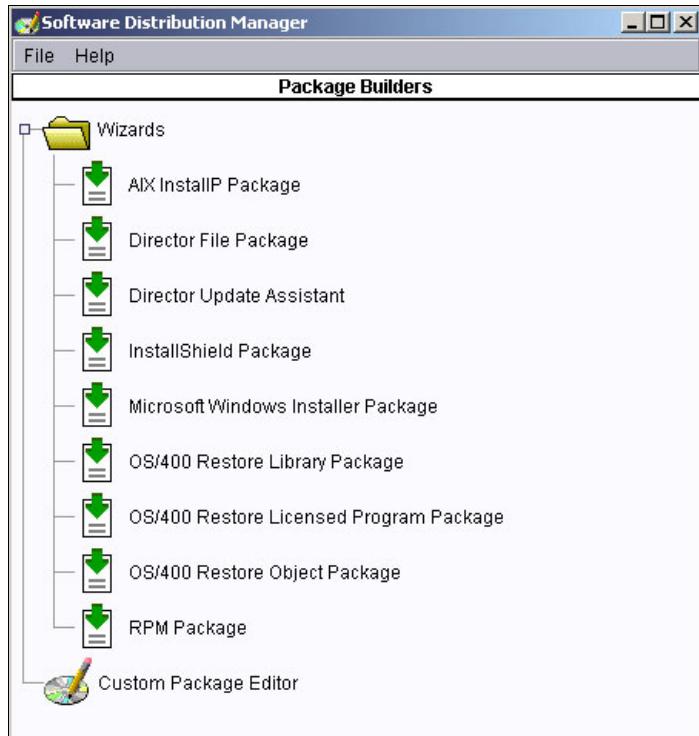


Figure 7-13 Software distribution manager window

4. Double-click **Director Update Assistant**. The Director Update Assistant window opens. See Figure 7-14 on page 261 for details.



Figure 7-14 Director Update Assistant window

5. Select **Get files from the local system**.
6. Click **Browse**. This opens the root directory search window.
7. Navigate to the CD-ROM drive where UpdateXpress is located, and select **index.xml** in the root directory and click **OK**.
8. Click **Next** to continue.
9. Scroll down the list of packages until you get to the folder named IBM eServer xSeries 345 and expand the tree. The view will look like Figure 7-15 on page 262.

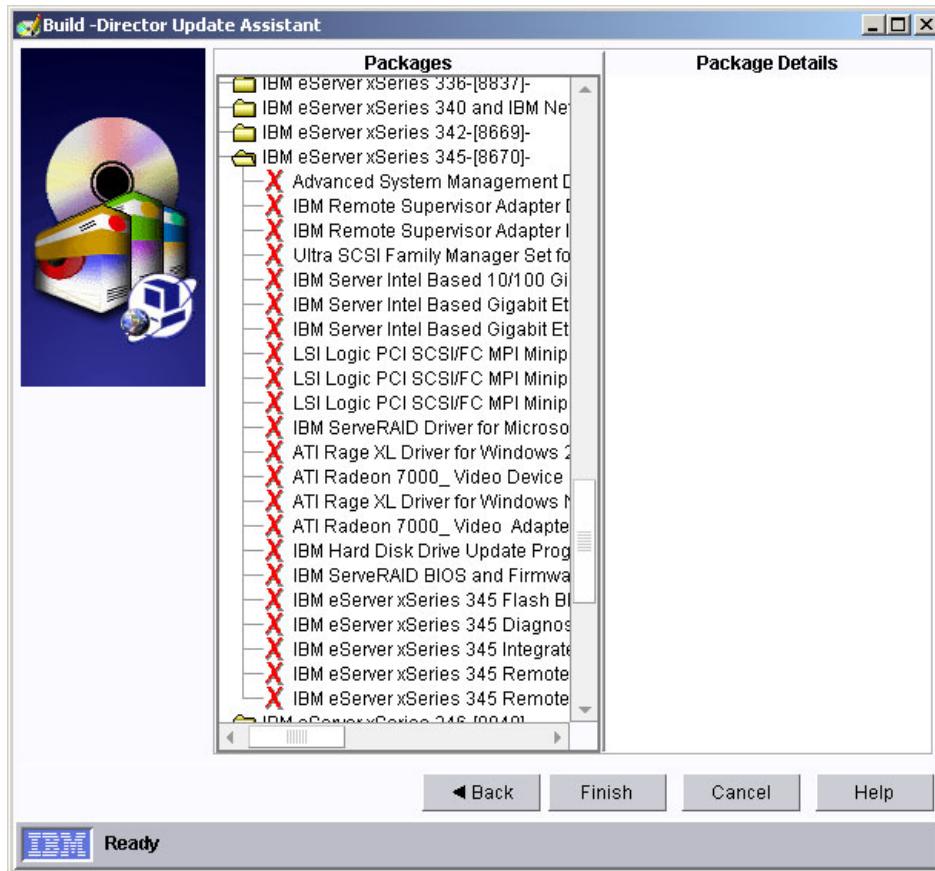


Figure 7-15 x345 files available for downloading

10. Locate the required updates you wish to perform. Right-click the **X** next to the firmware update and click **Select Item**. The **X** will now change to a **✓**.
11. Once all the required firmware updates are selected, click **Finish**.
12. These updates will now be processed and added into the IBM Director Software Distribution task and will become available to update the servers.
13. Once all the images have been processed, this window will close automatically and will return to the Software Distribution Manager window, Figure 7-13 on page 260. Select **File → Close** to close this window and return to the IBM Director console.
14. Select the Software Distribution task, and expand the tree to see the new images. See Figure 7-16 on page 263 for details.

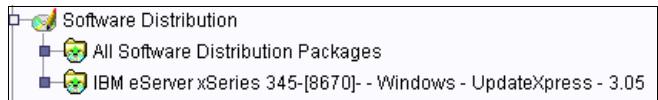


Figure 7-16 Imported firmware for x345 from UX v3.05a CD

15. Expand the x345 tree and you will see the entries you selected in step 10 on page 262. See Figure 7-17. These can now be pushed to your managed systems and executed immediately or later using the IBM Director scheduler. Or execute the option now, once dragged onto your managed systems.

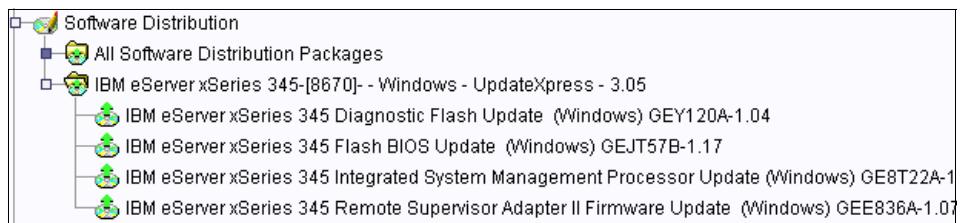


Figure 7-17 Firmware details for the x345

16. You are now ready to perform the update of the x345 server.
17. Select the root task for the four x345 firmware updates, and drag and drop it onto the x345 server (for single update). If you had a group of x345 servers you wanted to update, you could drag and drop the firmware updates onto a group icon for the x345 servers.
18. You will be presented with the question in Figure 7-18. Click **Schedule** if you want to schedule the firmware upgrade for another time, or click **Execute Now** if you want to update the firmware immediately.



Figure 7-18 Update question to schedule or execute now

19. If you clicked **Schedule** you will be presented with the window in Figure 7-19. Here you will enter the details of your new scheduled job.

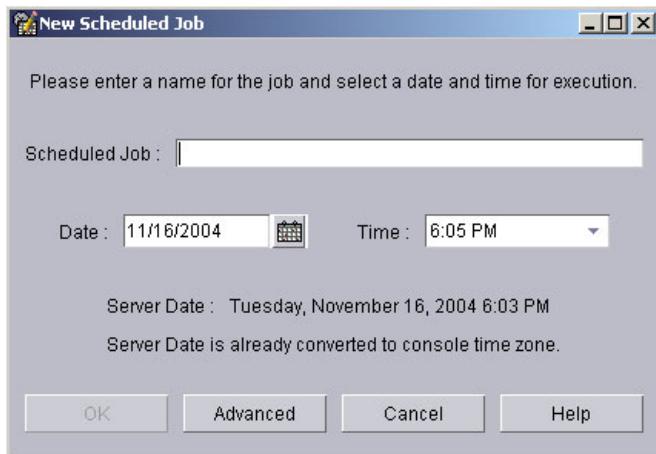


Figure 7-19 New Scheduled Job

20. Type in an appropriate name for your scheduled job. We have used x345 firmware updates, and select a time for the job to execute. See Figure 7-20.

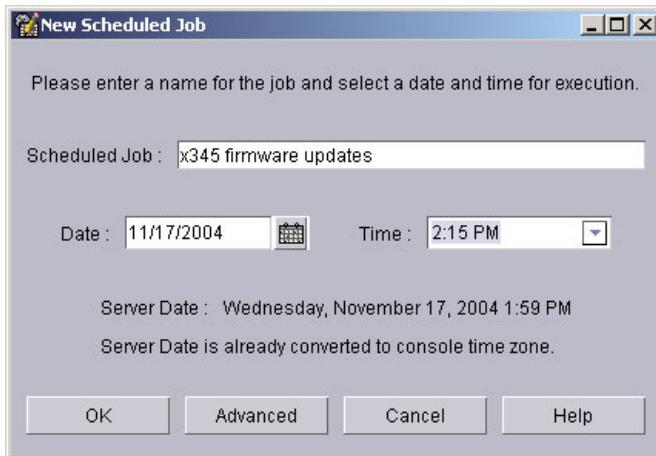


Figure 7-20 Job details

21. Once you are satisfied with your scheduled time click **OK**.
22. You will be prompted to confirm that the scheduled task be saved. Click **OK**.
23. Your job is now applied to your server. To check this, you can change the view in the middle pane of the main IBM Director console windows to show all

scheduled jobs and which servers they are associated with. To do this, right click in a free space in the middle pane and click **Associate by Job**.

24. When the tree box appears next to the Agent you should expand this to see the applied jobs. See Figure 7-21 for details.



Figure 7-21 Associate by job

25. Once the job is complete you can look at the execution history. You get to this by selecting the scheduler icon  from the IBM Director icon menu.
26. Locate your job and right-click it. This will open a menu. Click **Open Execution History**.
27. From this window select **File → View Log**.
28. This will open up the job execution history. The viewing detail is set to low by default, but you can change this to be high detail by selecting **View → Detail → High**. You will then receive the complete breakdown of the execution history, as seen in Figure 7-22 on page 266.

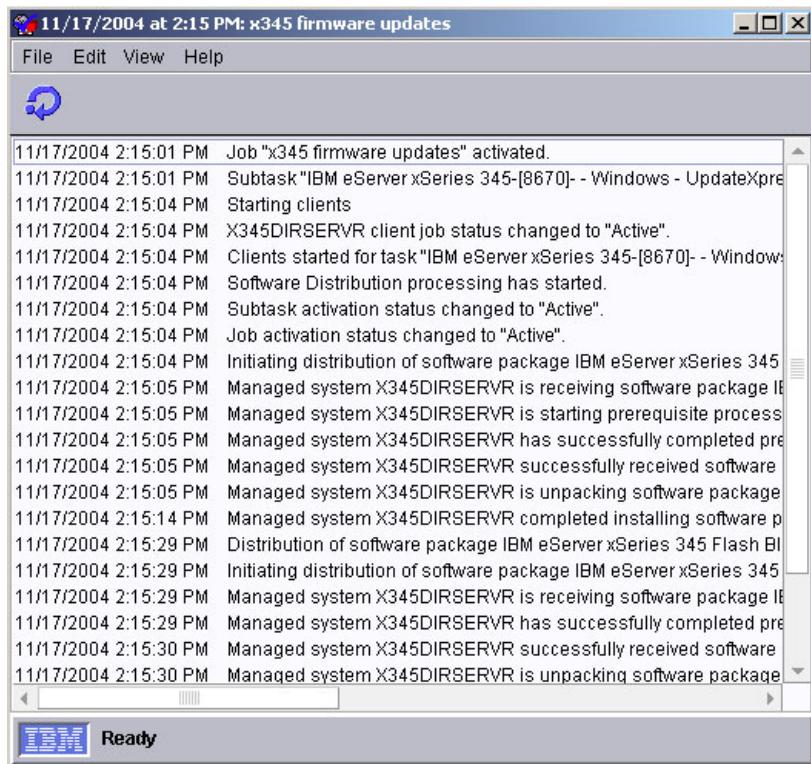


Figure 7-22 Viewing high detail for job execution history

7.8.3 Using UpdateXpress RemoteUX to update firmware

UpdateXpress is a CD-ROM containing a autostart program that allows you to maintain your system firmware and Windows device drivers at the most current levels defined on the CD, thus helping to avoid unnecessary outages.

UpdateXpress is available from:

<http://www.ibm.com/pc/support/site.wss/MIGR-53046.html>

UpdateXpress automatically detects current device driver and firmware levels and presents them to the user. It then gives you the option of selecting specific upgrades or allowing UpdateXpress to update all of the system levels it detected as needing upgrades.

There are three ways to use the UpdateXpress CD:

- ▶ Locally at the server by booting from the CD
- ▶ Locally by loading the CD (autorun) from Windows
- ▶ Remotely using the RemoteUX command-line utility on the CD

This section describes the use of RemoteUX.

RemoteUX works only with Windows-based servers and connects to them remotely via the administrative shares (C\$, ADMIN\$). Firmware updates are performed by writing data to available sectors on the first track of a disk in the remote server using PowerQuest Virtual Boot Environment.

Note: RemoteUX only works on Windows workstations and only with remote servers running Windows NT 4.0, Windows 2000 Server, and Windows Server 2003.

Figure 7-23 shows a typical network diagram for running UpdateXpress remotely.

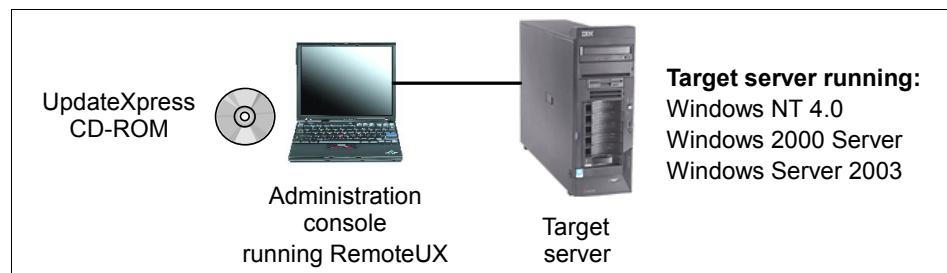


Figure 7-23 Running UpdateXpress remotely

The UpdateXpress CD-ROM is either in a drive on the local administrator workstation or copied to a network share. If you are using the network share option, then you specify its location as part of the RemoteUX command.

Tip: In this section we describe the process of using RemoteUX from the CD-ROM or a network share containing all the files from the CD-ROM. If you wish to use a network share, but want to minimize the space used, follow the instructions in the document “Automating System Firmware Updates with RemoteUX and UpdateXpress Version 3.02A”, available from the following URL, to delete unnecessary files.

<http://www.ibm.com/pc/support/site.wss/MIGR-54033.html>

The syntax for RemoteUX is:

`remoteux \\targetserver parameters command`

The options specify how to connect and where the UpdateXpress files are to be sourced from.

The parameters are shown in Table 7-2. If no parameters are specified, the following are used:

- ▶ UpdateXpress files are in the current local directory.
- ▶ Use c\$\temp on the remote server for temp space.
- ▶ Log in to the remote server using the current user ID/password.

Table 7-2 RemoteUX parameters

Options	Meaning
-r:path -remote:path	Specifies the staging or working directory path of the target server. The default is C\$\temp. Format is shareName\path.
-l:path -local:path	Specifies the path where the UpdateXpress CD image is stored. The default is the current directory.
-n -nowait	Specifies that RemoteUX not wait for the remote process to complete before exiting. For updates that require a system restart (firmware updates), waiting means exiting the RemoteUX application as soon as the update is scheduled or fails to schedule because of an error.
-u:user -user:user	Specifies the administrator user ID to connect to the remote server. The default is the current user name.
-p:password -pwd:password -p:*	Specifies the password to use to connect. Specifying the * instructs RemoteUX to prompt you to enter a password.

The commands you can issue let you query what levels of firmware and drivers are already installed, and to apply updates.

The possible commands are shown in Table 7-3.

Table 7-3 RemoteUX commands

Commands	Meaning
-c -compare	Compares and displays the firmware and device driver levels on the remote system with what is available on the UpdateXpress CD.
-e -examine	Displays the current firmware and driver levels. It also reports the model number of the remote server.
-pkg:pkg.exe -package:pkg.exe	Remotely run pkg.exe, which is a “Package for the Web” package. Only one update can be pending on a remote server at a time. Use the -local parameter to specify the local directory if necessary. Use -a to pass additional arguments to the package file.

Commands	Meaning
-a args	Passes optional arguments to the package update. A frequently used argument list is -a -r, which performs an immediate restart after scheduling the update package. This causes your system to reboot after applying the update. See Table 7-4 for a complete list.
-d -drivers	Updates device drivers on the remote server. This pushes the suitable device drivers from the CD to the target, and then remotely launches UpdateXpress. UpdateXpress identifies the updates that each system requires and automatically updates the server.
-f -firmware	Updates all firmware on the remote server. This pushes the firmware updates from the CD to the target. A reboot is scheduled to apply the updates, or you can force an immediate reboot with the -f -a -r parameters.
-g -getlog	Get the ux.log file from the remote server. This file is c\$\uxlog\ux.log on the remote server.
-clr -clearlog	Delete the ux.log file on the remote server.

The -a command lets you pass parameters to the “Package for the Web” package. The syntax is as follows.

For driver updates the optional arguments are:

`[-s] [-a [-s] | [-x directory]]`

For firmware updates the optional arguments are:

`[-s] [-a [-s] | [-r] | [-c] | [-x directory] | [-xd]]`

Notice that the -a argument is used to pass to the install package.

Table 7-4 Parameters for the -a command

Argument	Driver	Firmware	Meaning
-s	Yes	Yes	Installs the package software silently and does not prompt you if files need to be over written in the %temp% directory.
-a	Yes	Yes	Passes all package subsequent commands to the install package.

Argument	Driver	Firmware	Meaning
-s	Yes	Yes	(The second -s parameter) Installs the update silently and unattended. Drivers are installed immediately, however a reboot may be required before updates are applied. For firmware, the update is scheduled to run on the next reboot. A reboot can be forced with the -r option.
-x dir	Yes	Yes	Extracts the update to a directory. The default is remote server's %TEMP% directory.
-r	No	Yes	Schedules the update (can be used with or without the -s option) and reboots immediately.
-c	No	Yes	Cancel any scheduled firmware update and write an entry to the log file.

Tip: Only one firmware package can be scheduled at one time. If a firmware update needs to be applied instead of the currently scheduled firmware update package, cancel the current update package by running the -c option on any firmware package; then run the applicable firmware package.

For example, to view the current levels of firmware and drivers on a remote xSeries 345 and compare them to the UpdateXpress CD, use the following command:

```
remoteux \\9.42.171.144 -u:Administrator -p:* -c
```

Example 7-8 Results of the compare command

```
H:\UX\Disk 1>remoteux \\9.42.171.144 -u:Administrator -p:* -c
RemoteUX V1.2 for Windows 2003/2000/NT4
Password:
Connecting to remote service....
Remote Machine=\\9.42.171.144 Model Number=8670 Server Type=xSeries 345
Copying examination tools to remote server.
Please wait.....
Comparing system levels in server \\9.42.171.144 started at 10:45 AM on 03/21/20
05 against UpdateXpress 3.06
NOTE: Some versions of the IBM Service Processor may not be compatible with this
utility.
```

Type	Name	System Level	CD Level	New
F	POST/BIOS	61A	60A	
F	System diagnostics	T20	T20	
F	ISMP	20A	22A	X
D	symmpi.sys	1.08.18.00	1.09.06.00	X
F	IBM RSA II Firmware	GEE840A	GEE836A	
D	e1000325.sys	6.3.6.31	7.3.13.0	X
D	IBM RSA II Driver	5.33	5.32	

The first column of the output of the compare command specifies if the entry is firmware or driver. The last column indicates which entries are eligible to be updated by your version of UpdateXpress. In the above example, one firmware (ISMP) needs updating and two drivers (the LSI Logic SCSI driver, symmpi.sys and the Intel Gigabit driver, e1000325.sys) need updating.

To update the firmware of the remote server, issue the **-f** (or **-firmware**) command:

```
remoteux \\9.42.171.144 -u:Administrator -p:* -f
```

Example 7-9 Output from the firmware command to update all firmware on the remote server

```
Connecting to remote service....
Remote Machine=\\9.42.171.144 Model Number=8670 Server Type=xSeries 345

Copying required UpdateXpress source to \\9.42.171.144.
Please wait.....
Running UpdateXpress on the remote machine...
Completed running UpdateXpress on the remote machine
```

Firmware typically requires a reboot. To confirm this, get the UpdateXpress log using the **-getlog** command.

Example 7-10 Output from the getlog command before the reboot

```
Connecting to remote service....
Remote Machine=\\9.42.171.144 Model Number=8670 Server Type=xSeries 345
03:10:2005 13:31:34,Update=BIOS,New=1.19,Status=Success,ReturnCode=0
[Remote UpdateXpress Firmware Update]
Scheduled at 17:15:32 - 03:21:2005 returns=0
```

Notice from the above output that the update is scheduled at a later time. You cannot control the scheduled time, but you can reboot the server manually

sooner if you wish. Alternatively, you could have specified a reboot to happen immediately:

```
remoteux \\9.42.171.144 -u:Administrator -p:* -f -a -r
```

After the reboot and the update, the **-getlog** command contains the following (Example 7-11).

Example 7-11 Output from the getlog command after the update is applied

```
Connecting to remote service.....  
Remote Machine=\\9.42.171.144 Model Number=8670 Server Type=xSeries 345  
03:10:2005 13:31:34,Update=BIOS,New=1.19,Status=Success,ReturnCode=0  
[Remote UpdateXpress Firmware Update]  
Scheduled at 17:15:32 - 03:21:2005 returns=0  
  
03:21:2005 12:38:12,Update=Tape drive microcode,Old=,New=Many, Status=No supported  
tape device found,Error,ReturnCode=2  
03:21:2005 12:38:12,Update=SCSI hard disk drive microcode,Old=,New=Many,  
Status=Error, ReturnCode=1  
03:21:2005 12:38:12,Update=RSA II Video BIOS,Old=Unknown,New=001, Status=Error,  
ReturnCode=2  
03:21:2005 12:38:12,Update=Integrated Systems Management,Old=20A,New=22A,  
Status=Success, ReturnCode=0  
12:38:12.42p 03-21-2005, Update=RemoteUX Firmware, Status=Complete, ReturnCode=0
```

As you can see from the log (and as was seen during the update process), a number of updates were attempted. The return codes are listed in the specific sections of Table 7-5:

- ▶ Tape drive microcode: No tape drives found (RC=2)
- ▶ SCSI disk drive microcode: Failed (RC=1)
- ▶ RSA II video BIOS: Failed (RC=2)
- ▶ ISMP service processor: Updated successfully (RC=0)

Table 7-5 lists the update packages return codes.

Table 7-5 .UpdateXpress packages return codes

Return code	Meaning
IBM service processor driver	
0	Success, no reboot required
1	Success, reboot required
2	Error, install failed

Return code	Meaning
8	No hardware found
Tape drive firmware	
0	Success
1	Error, Tape device update failure
2	No supported tape devices found
3	Tape device already up to date
4	Unrecoverable error unrelated to the tape device
5	Operator canceled automatic update
6	Tape device needs update by an alternate method
7	Tape device needs update in DOS only mode
8	Tape device in use by another program
9	Tape device is inaccessible
Hard drive microcode firmware	
0	Success
1	Error, Hard drive device update failure
3	Hard drive device already up to date

Table 7-6 lists the RemoteUX return codes.

Table 7-6 Remote UpdateXpress return codes

Return code	Meaning
0	UpdateXpress successfully started (See note 1)
2	Error, file not found (See note 2)
3	Error, path not found (See note 2)
5	Error, access denied (See note 2)
39	Error, disk full (See note 2)

Return code	Meaning
Notes:	
<ol style="list-style-type: none"> When UpdateXpress returns a non-zero code, it displays a message explaining the error code. A return code of 0 does not always indicate that the update has been successfully applied, only that it has been successfully scheduled. Review the log file for results of the update. 	

For more information about how UpdateXpress works and ways to determine the cause when failures occur, see the online help available by launching index.htm from the UpdateXpress CD-ROM.

Note: You should periodically clear the log file using the **-clearlog** command. When the file size reaches 4 MB, the output of updates will not be written to the file.

7.9 UpdateXpress firmware update scripts for BladeCenter

UpdateXpress Firmware Update Scripts for BladeCenter (UXBC) is a process that enables firmware updates for the components listed below to be run in a remote, unattended fashion on a single BladeCenter chassis:

- ▶ Management modules (one or two)
- ▶ 4-Port Ethernet Switch Module
- ▶ Nortel Layer 2-7 Gigabit Ethernet Switch Module

The scripts update all the supported components in the chassis to the specified firmware. You cannot select components within the chassis to update.

Command line parameters needed to launch the update process will be required before starting. The solution consists of a top level script (ChassisUpdate.py) written in the Python scripting language, which drives other subscripts to run.

Requirements

UXBC is controlled and run through Python scripts. The Python interpreter (Version 2.3 or later) must be installed only on the administrative system. You can download the Python interpreter for your operating system from the Web:

<http://www.python.org>

A TFTP server is required for you to obtain the firmware updates of the modules, such as switches. The TFTP server can be installed anywhere on the network that is accessible to the switches that need to be updated.

One possible TFTP server, if you do not have one is SolarWinds TFTP Server, is available from:

http://www.solarwinds.net/Tools/Free_tools/TFTP_Server/

We recommend that the UXBC scripts be run on a LAN behind a firewall. All media and transmission types that reliably support TCP/IP and FTP in a LAN environment are supported.

The UXBC scripts can be run from the following operating systems installed on the administrative system:

- ▶ Windows 2000
- ▶ Windows XP
- ▶ Windows Server 2003
- ▶ Red Hat Enterprise Linux 2.1
- ▶ Red Hat Enterprise Linux 3.0
- ▶ SUSE LINUX Enterprise Server 8.0

Getting started

There is no installation of the scripts. In a Windows environment, no additional registry entries or shared DLLs are required.

To get the UXBC code, download the zipped file from the IBM support Web site:

<http://www.ibm.com/pc/support/site.wss/MIGR-57201.html>

Extract the contents of the zipped file and make sure that the unzip process preserves the case and file permissions. All files with PY extensions must be executable.

When the UXBC file is unzipped, the following directories are created (for example, when unzipped to the C:\ directory):

c:\BladeCenterUpdates	Root directory
c:\BladeCenterUpdates\Common	Common functions/definitions
c:\BladeCenterUpdates\IOModules	Scripts for I/O modules such as switches
c:\BladeCenterUpdates\MM	Scripts pertaining to the management module

Tip: The sample response file BladeCenterUpdates.rsp located in c:\BladeCenterUpdates\ is printed in Example 7-12 for reference. Keep this file handy for reference when you are creating your custom response file; it includes additional information about the parameters in the file.

Example 7-12 BladeCenterUpdates.rsp file

```
# BladeCenterUpdates.rsp
# UpdateXpress firmware update scripts for BladeCenter response file
# Copyright IBM Corporation, 2004
# The format of this file is straight forward. Lines begining with a # # are
considered comments and ignored. Lines beginning with white space are also ignored.
Every option is specified using a key-value pair seperated by an = character. Keys
cannot be used without values associated with them (e.g. mmipaddr= is not a valid
key-value pair, mmipaddr=192.168.1.1 is).
# Some of the options are mandatory. Others are mandatory only with certain
BladeCenter configurations (e.g. Firmware update filenames are mandatory for switches
to get updated). Most options have a default value that is used if the option is not
specified. The defaults are listed in the description of each option below.

### MANDATORY Fields ###
# These fields must be specified.
# This is a mandatory field that specifies the hostname or the dotted IP address of
the BladeCenter Management Module.
# ex. mmipaddr=10.1.1.100 or mmipaddr=hostname.host.com
mmipaddr=

### OPTIONAL Fields ###
# These fields may be necessary depending on the BladeCenter configuration.
# This is an optional field that specifies the username for the BladeCenter
Management Module. If not specified (i.e. commented out), the defaultusername
(USERID) is assumed. Otherwise, a value MUST be specified.
## ex. mmuser=USERID
#mmuser=

# This is an optional field that contains the password of the specified username for
the BladeCenter Management Module. If not specified If not specified (i.e. commented
out), the default password (PASSWORD) is assumed. Otherwise, a value MUST be
specified.
#
# ex. mmpass=PASSWORD
#mmpass=

# This is an optional field that is the fully qualified path to the BladeCenter
Management Module firmware update files. By default the scripts will look in the
current directory for the firmware. To use this field, remove the comment character
(#) and add the fully qualified path. Note: Packet files must be in ALLCAPS, and
must be named CNETBRUS.PKT, CNETMNUS.PKT, and CNETRGUS.PKT
#
# ex. mmFileLocation=c:\images
```

```

#mmFileLocation=

# The IP address of the TFTP server containing the firmware update files. This address
MUST be specified as a valid dotted IP address, hostnames are not allowed. This
field is required for updating any switch in the BladeCenter.

# ex. tftpipaddr=192.168.1.2
#tftpipaddr=

# This is an optional field that contains the username for the first I/O module. If not
specified (i.e. commented out), the default username (USERID) is assumed. Otherwise,
a value MUST be specified.
#
# ex. ioluser=USERID
#ioluser=

# This is an optional field that contains the password for the username of the first
I/O module. If not specified (i.e. commented out), the default password (PASSWORD)
is assumed. Otherwise, a value MUST be specified.
#
# ex. iolpass=PASSWORD
#iolpass=

# The full path(s) and filename(s) of the first I/O module FLASH file(s) on the TFTP
server. If only one filename necessary use io1Filename1 and leave io1Filename2
commented out.
#
# ex. io1Filename1=ibmrnrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io1Filename1 and the
boot image by io1Filename2.
#
# ex. io1Filename1=GbESM-AOS-20.1.1.0-os.img
#      io1Filename2=GbESM-AOS-20.1.1.0-boot.img
#io1Filename1=
#io1Filename2=

# This is an optional field that contains the username for the second I/O module. If
not specified (i.e. commented out), the default username (USERID) is assumed.
Otherwise, a value MUST be specified.
#
# ex. io2user=USERID
#io2user=

```

```

# This is an optional field that contains the password for the username of the second
I/O module. If not specified (i.e. commented out), the default password (PASSWORD) is
assumed. Otherwise, a value MUST be specified.
#
# ex. io1pass=PASSWORD
#io2pass=

# The full path(s) and filename(s) of the second I/O module FLASH file(s) on the TFTP
server. If only one filename necessary use io2Filename1 and leave io2Filename2
commented out.
#
# ex. io2Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io2Filename1 and the
boot image by io2Filename2.
#
# ex. io2Filename1=GbESM-AOS-20.1.1.0-os.img
#      io2Filename2=GbESM-AOS-20.1.1.0-boot.img
#io2Filename1=
#io2Filename2=

# This is an optional field that contains the username for the third I/O module. If
not specified (i.e. commented out), the default username (USERID) is assumed.
Otherwise, a value MUST be specified.
#
# ex. io3user=USERID
#io3user=

# This is an optional field that contains the password for the username of the third
I/O module. If not specified (i.e. commented out), the default password(PASSWORD) is
assumed. Otherwise, a value MUST be specified.
#
# ex. io3pass=PASSWORD
#io3pass=

# The full path(s) and filename(s) of the third I/O module FLASH file(s) on the TFTP
server. If only one filename necessary use io3Filename1 and leave io3Filename2
commented out.
#
# ex. io3Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io3Filename1 and the boot
image by io3Filename2.
#
# ex. io3Filename1=GbESM-AOS-20.1.1.0-os.img

```

```
#      io3Filename2=GbESM-AOS-20.1.1.0-boot.img
#io3Filename1=
#io3Filename2=

# This is an optional field that contains the username for the fourth I/O module. If
not specified (i.e. commented out), the default username (USERID) is assumed.
Otherwise, a value MUST be specified.
#
# ex.  io4user=USERID
#io4user=

# This is an optional field that contains the password for the username of the fourth
I/O module. If not specified (i.e. commented out), the default password (PASSWORD)
is assumed. Otherwise, a value MUST be specified.
#
# ex.  io4pass=PASSWORD
#io4pass=

# The full path(s) and filename(s) of the fourth I/O module FLASH file(s) on the TFTP
server. If only one filename necessary use io4Filename1 and leave io4Filename2
commented out.
#
# ex.  io4Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io4Filename1 and the
boot image by io4Filename2.
#
# ex.  io4Filename1=GbESM-AOS-20.1.1.0-os.img
#      io4Filename2=GbESM-AOS-20.1.1.0-boot.img
#io4Filename1=
#io4Filename2=

# This option specifies that if the Management Module is configured via DHCP,
FLASHing of the I/O modules should occur automatically even if it is not possible to
FLASH the Management Module. To enable, simply uncomment the following line. To
disable, comment the line or specify FALSE.
#continueIO=TRUE

# Some management applications may cause the 6090 TCP port of the Management Module
to remain in a locked state and inaccessible by applications, such as these scripts.
If you uncomment the forceMMreboot option, you will permit these scripts to reboot
the Management Module and release this port. To enable, simply uncomment the
following line. To disable, comment the line or specify FALSE.
#forceMMreboot=TRUE
```

Complete the following steps to obtain the firmware updates for use with the UpdateXpress Firmware Update Scripts for BladeCenter:

1. Download the latest firmware update for the management modules from the IBM Support Web site:
BladeCenter: <http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
BladeCenter T: <http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>
2. Unzip the package and place all files with file extension .PKT in any location that the administrative system can access, except the BladeCenterUpdates directory (because you will overwrite the readme file). You may then move all the .PKT files to the default directory of the UXBC package (BladeCenterUpdates).
If you place the .PKT files in an alternative location, make a note of the path; you will need this information to fill in the response file later on.
3. Download the latest firmware updates for the I/O modules. You can obtain the firmware for the I/O modules from the IBM Support Web site.
4-Port Ethernet Switch Module:
<http://www.ibm.com/pc/support/site.wss/MIGR-50457.html>
Nortel Networks Layer 2-7 GbE Switch Module:
<http://www.ibm.com/pc/support/site.wss/MIGR-53058.html>
4. Unzip the firmware updates to the TFTP server. Record the following information:
 - The path to the unzipped firmware files
 - The names of the I/O module firmware files

Manually creating the BladeCenterUpdates.rsp file

A large amount of information is required to perform the firmware updates of a BladeCenter chassis. The UXBC software obtains the parameters that are needed to perform the updates by using the information from a previously created response file. The default name of this response file is BladeCenterUpdates.rsp.

A sample response file is in the \BladeCenterUpdates directory of the UXBC package and is reproduced in Example 7-12 on page 276.

Review this sample file and modify it for your environment. The sample file has detailed information for each of the fields. If you want to use another file name and path for the response file, specify that name and path on the command line when starting the UXBC process.

Once you have updated the response file, you can run the main script (ChassisUpdate.py). The update process uses the information in the response file as input to the script.

Tip: Once the initial response file is created for any BladeCenter chassis, future firmware update processes using the same response file might require modifications if information such as IP addresses or firmware file names have changed.

Setting the PYTHONPATH environment variable

For the UXBC to run, the PYTHONPATH environment variable must be set to the directory above the BladeCenterUpdates directory. For example:

- ▶ Microsoft Windows command prompt
set PYTHONPATH=c:\uxbcu\
- ▶ Linux BASH environment
export PYTHONPATH=/root/uxbcu

Starting the update process

To start the UXBC process, run **ChassisUpdate.py**. To run the ChassisUpdate script, call the main script directly or call the main script through the Python interpreter. From the command prompt, type one of the following commands and press Enter. These commands are case-sensitive.

Important: Do not run ChassisUpdate.py from a blade that is in the BladeCenter chassis that you are updating. Because firmware updates are performed on components that are part of the support structure of the BladeCenter system, the firmware update process must be run from a completely independent system.

- ▶ To call the main script, enter:
`ChassisUpdate.py options`
- ▶ To call the main script through the Python interpreter, enter:
`python ChassisUpdate.py options`

The options of the **ChassisUpdate** command are listed in Table 7-7 on page 282.

Table 7-7 Command line options for the ChassisUpdate script

Option (any listed variation is valid)	Description
--responseFile <file> -r <file>	Specify a response file, where <file> specifies the path and name of the response file. If you do not specify a response file, the default response file name and path is used, BladeCenterUpdates.rsp.
-V --version	Display the version number of the script (Note: -V has a capital V, as opposed to -v, which is for verbose mode).
-h --help -?	Display help.
-v --verbose	Display information about the update process as it runs.

Return codes

All information about the firmware update process is logged to the BladeCenterUpdates.log file. Log file entries are in the format:

<time_and_date> - <message>

The ChassisUpdate script has the following return codes (Table 7-8).

Table 7-8 Return codes from ChassisUpdate

Return code	Meaning
-1	General update failure.
0	The update was successfully completed.
1	An invalid IP address was given for the specified telnet connection.
2	There was a socket error when attempting to start a telnet session.
3	An invalid response was received from the telnet session.
4	An invalid login name or password was specified for the telnet session.
5	An invalid IP address was given for the management module.
6	There was a socket error when attempting to connect to the BCMM.
7	There was an unknown error when attempting to connect to the BCMM.
8	The encryption keys returned from the BCMM are invalid.

Return code	Meaning
9	An invalid login name or password was specified for the BCMM.
10	An invalid response was received from the BCMM.
11	The limit of three retries was exceeded when sending a command to the BCMM.
12	An unknown command type for the management module was specified.
13	The length of the management module command and the response do not match.
14	The command sent and the command received from the BCMM do not match.
15	There was an error sending data to the BCMM.
16	An invalid slot number for the BladeCenter chassis was specified.
17	An invalid code level to query was specified.
18	The specified management module packet file was not found.
19	An invalid packet file was specified.
20	The packet file contains an invalid header.
21	The TFTP download timed out.
22	The TFTP server was not found.
23	The connection with the TFTP server was lost.
24	TFTP server IP address is invalid.
25	Connection to the I/O module failed.
26	An update image file was not found.
27	The image file is invalid.

Limitations

UXBC has the following limitations:

- ▶ Management modules
 - If there are redundant management modules and the IP addresses are obtained through DHCP, it will not be possible to update the management modules if the existing firmware level is lower than 57 K.

- Depending on the code levels detected, you could have multiple management module restarts during the update process. It will not be possible to downlevel the firmware of the management modules via the UXBC tool.
- The management module password in the response file (mmpass in the sample response file, Example 7-12 on page 276) must be greater than 5 but less than 16 alphanumeric characters.
- ▶ IBM ESM configuration
 - ESM switch configuration settings can be reset when updating from a firmware level earlier than 0.081 (Version 1.04) to a firmware level at or later than 0.081. Link aggregation settings are lost during this firmware update and are reset back to the default values.
 - If link aggregation settings or port trunking are configured to be different from the default settings, do not use UXBC unless you can manually reconfigure the switch afterward.
 - In a small percentage of cases the UXBC tool may not be able to confirm that the firmware update for the ESM switch completed. In this case the BladeCenterUpdates.log file will have a warning stating that Update completion could not be verified. In every test that was conducted where the UXBC tool was not able to verify that the flashing completed, the ESM switch had successfully been updated. However, you should manually verify that the ESM switch is at the correct level.
- ▶ General

Running multiple instances of the ChassisUpdate script to more than one BladeCenter chassis at a time from an administrative system can produce undesirable results and is not supported.

Abbreviations and acronyms

ADS	Active Directory Service	EEPROM	electrically erasable programmable read only memory
ADSI	Active Directory Service Interfaces	EMEA	Europe, Middle East, Africa
ANSI	American National Standards Institute	EMS	Emergency Messaging Service
ASCII	American National Standard Code for Information Interchange	ESM	Ethernet switch modules
ASF	Alert Standard Format	EXA	Enterprise X-Architecture™
ASM	advanced system management	GUI	graphical user interface
ASMA	Advanced System Management Adapter	HDD	hard disk drive
ASMP	Advanced System Management Processor	HID	human interface device
ASR	automatic server restart	IBM	International Business Machines Corporation
ASU	Advanced Settings Utility	ICMB	Intelligent Chassis Management Bus
BCMM	BladeCenter management module	ICMP	internet control message protocol
BIOS	basic input output system	IP	internet protocol
BMC	Baseboard Management Controller	IPMB	Intelligent Platform Management Bus
BOOTP	boot protocol	IPMI	Intelligent Platform Management Interface
CD-ROM	compact disk read only memory	IRQ	interrupt request
CIM	Common Information Model	ISM	integrated system management
CLI	command-line interface	ISMP	Integrated System Management Processor
CPU	central processing unit	ISO	International Organization for Standards
CSR	Certificate Signing Request	ITSO	International Technical Support Organization
CTS	clear to send	IXA	Integrated xSeries Adapter
DEN	Directory Enabled Network	KVM	keyboard video mouse
DHCP	Dynamic Host Configuration Protocol	LAA	locally administered address
DIMM	dual inline memory module	LAN	local area network
DLL	dynamic linked library	LDAP	Lightweight Directory Access Protocol
DMI	Desktop Management Interface	LDAPS	secure LDAP
DMTF	Distributed Management Task Force	LED	light emitting diode
DN	distinguished name	MAC	media access control
DNS	Domain Name System		
DOS	disk operating system		
DSA	digital signature algorithm		

MB	megabyte	SNMP	Simple Network Management Protocol
MCSE	Microsoft Certified Systems Engineer	SOL	serial over LAN
MMC	Microsoft Management Console	SP	service processor
MPA	Management Processor Assistant	SSH	secure shell
MPCLI	management processor command line interface	SSL	secure sockets layer
MTU	maximum transmission unit	UDF	Universal Disk Format
NEBS	network equipment building system	UPN	User Principal Name
NIC	network interface card	UPS	uninterruptible power supply
NMI	non-maskable interrupt	URL	Uniform Resource Locator
OEM	other equipment manufacturer	USB	universal serial bus
OOB	out of band	UX	UpdateXpress
OS	operating system	VESA	Video Electronics Standards Association
PCI	Peripheral Component Interconnect	VPD	vital product data
PET	Platform Event Trap	VRM	voltage regulator module
PKT	packet	WAN	wide area network
PPP	point-to-point protocol	WEBEM	Web-based Enterprise Management
PXE	preboot execution environment	WOL	wake on LAN
RAID	redundant array of independent disks	XON	transmitter on
RAM	random access memory		
RDM	Remote Deployment Manager		
RFC	request for comments		
RISC	reduced instruction set computing		
ROM	read-only memory		
RPM	Red Hat Package Manager		
RSA	Remote Supervisor Adapter		
SAC	Special Administration Console		
SAN	storage area network		
SCSI	small computer system interface		
SLES	SUSE LINUX Enterprise Server		
SLP	Service Location Protocol		
SMASH	Systems Management Architecture for Server Hardware		
SMBIOS	system management BIOS		
SMI	Structure of Management Information		
SMTP	Simple Mail Transfer Protocol		

Related publications

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

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 291. Note that some of the documents referenced here may be available in softcopy only.

- ▶ *IBM @server xSeries BMC — Firmware and Drivers Cheatsheet*, TIPS0532
- ▶ *Implementing Systems Management Solutions using IBM Director*, SG24-6188
- ▶ *Netfinity Server Management*, SG24-5208
- ▶ *Remote Supervisor Adapter II Family — Firmware and Drivers Cheatsheet*, TIPS0532
- ▶ *Service Processors Supported in IBM Netfinity and IBM @server xSeries Servers*, TIPS0146

Other publications

These publications are also relevant as further information sources:

- ▶ *Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User’s Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-57091.html>
- ▶ *IBM Remote Supervisor Adapter II Technical Update for Linux*, 2nd Edition
<http://www.ibm.com/pc/support/site.wss/MIGR-50314.html>
- ▶ *BladeCenter Management Module User’s Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-45153.html>
- ▶ *BladeCenter Management Module Installation Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-52227.html>

- ▶ *BladeCenter and BladeCenter T Management Module Command-Line Interface Reference Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-54667.html>
- ▶ *BladeCenter and BladeCenter T Serial over LAN Setup Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-54666.html>
- ▶ *Lightweight Directory Access Protocol User's Guide for IBM @server BladeCenter Management Module and IBM Remote Supervisor Adapters*
<http://www.ibm.com/pc/support/site.wss/MIGR-55014.html>
- ▶ *Management Command Line Interface User's Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>
- ▶ *OSA System Management Bridge User's Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-57816.html>
- ▶ *IBM Director Installation Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-50460.html>
- ▶ *IBM Director Systems Management Guide*
<http://www.ibm.com/pc/support/site.wss/MIGR-50461.html>
- ▶ *Whitepaper: Automating System Firmware Updates with RemoteUX and UpdateXpress*
<http://www.ibm.com/pc/support/site.wss/MIGR-54033.html>
- ▶ *Technical update: Connecting an x335 to an ASM interconnect network*
<http://www.ibm.com/pc/support/site.wss/MIGR-54747.html>
- ▶ *IPMI Version 1.5 specification*
ftp://download.intel.com/design/servers/ipmi/IPMIV1_5rev1_1-012904marcup.pdf
- ▶ *Active Directory Programmer's Guide*
<http://go.microsoft.com/fwlink/?LinkId=142>

Online resources

These Web sites and URLs are also relevant as further information sources:

IBM Web pages

- ▶ BladeCenter Standby Capacity on Demand
http://www.ibm.com/servers/eserver/bladecenter/scod/more_info.html

- ▶ ServerProven System Management Upgrades
<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>
- ▶ Software and device drivers matrix for xSeries and BladeCenter
<http://www.ibm.com/pc/support/site.wss/MIGR-4JTS2T.html>
- ▶ RETAIN tip H177279, RSA II PS/2 mouse does not work during Red Hat Linux installation
<http://www.ibm.com/pc/support/site.wss/MIGR-50413.html>
- ▶ BladeCenter 4-Port Ethernet Switch Module Firmware
<http://www.ibm.com/pc/support/site.wss/MIGR-50457.html>
- ▶ UpdateXpress CD
<http://www.ibm.com/pc/support/site.wss/MIGR-53046.html>
- ▶ BladeCenter Nortel Networks Layer 2-7 GbE Switch Module Firmware
<http://www.ibm.com/pc/support/site.wss/MIGR-53058.html>
- ▶ Management Processor Command Line Interface Utility
<http://www.ibm.com/pc/support/site.wss/MIGR-54216.html>
- ▶ Management Module Firmware for BladeCenter
<http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
- ▶ Management Module Firmware for BladeCenter T
<http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>
- ▶ RSA II remote mounting issues with Linux
<http://www.ibm.com/pc/support/site.wss/MIGR-55671.html>
- ▶ Advanced Settings Utility for Microsoft Windows
<http://www.ibm.com/pc/support/site.wss/MIGR-55019.html>
- ▶ Advanced Settings Utility for Linux
<http://www.ibm.com/pc/support/site.wss/MIGR-55020.html>
- ▶ Advanced Settings Utility for DOS
<http://www.ibm.com/pc/support/site.wss/MIGR-55021.html>
- ▶ Advanced Settings Utility definition files for RSA and RSA II
<http://www.ibm.com/pc/support/site.wss/MIGR-55027.html>
- ▶ Advanced Settings Utility definition files for x345
<http://www.ibm.com/pc/support/site.wss/MIGR-55778.html>

- ▶ Advanced Settings Utility definition files for x235
<http://www.ibm.com/pc/support/site.wss/MIGR-55803.html>
- ▶ Advanced Settings Utility definition files for x335
<http://www.ibm.com/pc/support/site.wss/MIGR-55804.html>
- ▶ Advanced Settings Utility definition files for x445
<http://www.ibm.com/pc/support/site.wss/MIGR-55944.html>
- ▶ Advanced Settings Utility definition files for x255
<http://www.ibm.com/pc/support/site.wss/MIGR-56393.html>
- ▶ Advanced Settings Utility definition files for BladeCenter HS20 8832
<http://www.ibm.com/pc/support/site.wss/MIGR-56555.html>
- ▶ Advanced Settings Utility definition files for x440
<http://www.ibm.com/pc/support/site.wss/MIGR-56858.html>
- ▶ Advanced Settings Utility definition files for BladeCenter HS20 8678
<http://www.ibm.com/pc/support/site.wss/MIGR-56860.html>
- ▶ IBM Director 4.20.2
<http://www.ibm.com/pc/support/site.wss/MIGR-57057.html>
- ▶ UpdateXpress firmware update scripts for BladeCenter
<http://www.ibm.com/pc/support/site.wss/MIGR-57201.html>
- ▶ IBM UpdateXpress Server
<http://www.ibm.com/pc/support/site.wss/MIGR-57426.html>
- ▶ System Management Bridge utility
<http://www.ibm.com/pc/support/site.wss/MIGR-57729.html>

Other Web pages

- ▶ Distributed Management Task Force standards
<http://www.dmtf.org/standards>
<http://www.dmtf.org/standards/smash>
- ▶ Intelligent Platform Management Interface
<http://www.intel.com/design/servers/ipmi>
- ▶ Java Runtime Environment download
<http://www.java.com/en/download/manual.jsp>
- ▶ CD-ROM ISO tools
<http://www.smart-projects.net/isobuster>

- ▶ <http://www.magiciso.com>
- ▶ PuTTY telnet/SSH client
<http://www.chiark.greenend.org.uk/~sgtatham/putty>
- ▶ Windows Emergency Management Services
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_topnode.asp
- ▶ Windows Special Administration Console and SAC commands
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp
- ▶ SolarWindws TFTP server
http://www.solarwinds.net/Tools/Free_tools/TFTP_Server
- ▶ Python
<http://www.python.org>

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Numerics

- 13N0382, RSA II-EXA 52
- 59P2984, RSA II 50
- 73P9341, RSA II SlimLine 53

A

- Active Directory 130, 141
- administrator authority
 - eServer BMC 16
 - xSeries BMC 32, 39
- ANSI interface to service processors 220–224
- ASF 5
- ASM interconnect network 48, 55–59
 - gateway 58
 - management module 88
- ASM PCI Adapter
 - ASM interconnect network 55
 - IBM Director 227
 - MPCLI 176
 - supported servers 2
 - telnet interface 221
- ASU 160–175
 - batch command 174
 - commands 164
 - comparison with other tools 160
 - configuring an RSA II 173
 - definition files 162
 - download 162
 - factory defaults 249
 - operating systems 161
 - patchadd command 163
 - remote, using 253
 - resetrsa command 249
 - scripts 174
 - set command 173
 - supported servers 161
 - syntax 164
 - using 173
 - view settings 166
- authentication
 - LDAP 139–156
 - scenario 234
 - xSeries BMC 27, 38

B

- Baseboard Management Controller
 - See* BMC
- BIOS
 - BMC configuration 34
 - BMC event log 35
 - Remote Console Redirection 195
 - SMBridge configuration 195
- BladeCenter
 - BladeCenter Assistant 228
 - default addresses 239
 - management module
 - See* management module
 - On Demand activation 120
 - remote access to modules 239
 - UpdateXpress Scripts 274
 - UXBC 274
- blue screen of death 48
- BMC 7–46
 - compared with ISM Processor 8
 - eServer BMC 9–18
 - adding users 15
 - alert forwarding 16
 - configuring 11
 - connections 9
 - default userid 13
 - destination for alerts 13
 - drivers 17
 - firmware upgrade 10
 - IBM Director 14
 - IBM Director alerts 13
 - IPMI drivers 17
 - lancfg 11
 - MAC address 12
 - padlock icon 15
 - PING command 9
 - features 8
 - supported servers 2
 - xSeries BMC 18–44
 - adding users 27, 38
 - ASM connectors 20
 - bmc_cfg 22
 - channel number 25
 - clock 35

configuration in BIOS 34
connections 19
default gateway 26
default userid 23
destination for alerts 26
destination type 26
disabling 20
drivers 40
event log 35
features 18
firmware update 22
gateway 26
IBM Director 37
 configuring with 37
 sending alerts to 26, 39
IPMI drivers 40
padlock icon 37
PET alerts 26
Physical Platform 37
PING command 19
ports 19, 44
privileges 32
remote control 40
RS-485 connectors 20
RSA II SlimLine, both installed 235
SEL 35
set IP address 24
SMBridge 192–218
SNMP community 27
subnet mask 25
TCP/IP ports 44
user access 30

bmc_cfg 22–34
 adding users 27
 channel number 25
 default gateway 26
 destination address 26
 destination type 26
 privileges 32
 set IP address 24
 SNMP community 27
 subnet mask 25
 user access 30

bootcfg command 206

C

C2T 57
callback authority

xSeries BMC 32
CIM 4
CLIs
 ASU 160–175
 bmc_cfg 22–34
 comparison 158
 MPCLI 175–192
 RemoteUX 266
 securing 236
 SMBridge 192–218
 Telnet interface interface 220–224
console redirection 195
custom authority
eServer BMC 16

D

DEN 5
DMI 5
DMTF 4
drivers
 BladeCenter servers 119
 eServer BMC 17
 RSA II 64
 xSeries BMC 40

E

Emergency Messaging Service 200
encryption 130–139
Ethernet switch modules 239
event log, BMC 35
examples 233–284

F

factory defaults
 management module 127
 RSA II 248
firmware updates
 blade servers 121
 eServer BMC 10
 examples 256
 I/O modules 126
 IBM Director 259
 management module 95
 MPCLI 190, 257
 RemoteUX 266
 RSA II 62
 telnet client 222

UpdateXpress 274
xSeries BMC 22

G

gateway, ASM interconnect network 58

I

IBM Director 225–231
 adding the BMC 14
 adding users
 eServer BMC 15
 xSeries BMC 38
 alerting 229
BladeCenter Assistant 228
BMC configuration
 eServer BMC 14
 xSeries BMC 37
encryption 235
factory defaults 250
File Transfer 254
firmware update 259
Management Processor Assistant 38, 227
MPA 225–228
padlock icon 15, 37
Physical Platform object 15, 37
scheduler 264
industry standards 4
Integrated xSeries Adapter 20
interconnect network 48, 55–59
 management module 88
 RSA II 52
IPMI 5
IPMI drivers
 BladeCenter server 119
 eServer BMC 17
 xSeries BMC 40
ISM Processor
 compared with BMC 8
 features 8, 44
 gateway device 46, 58
 interconnect bus 57
 limitations 45
 MPCLI support 176
 supported servers 2

J

Java runtime 68

L

lancfg utility 11
LDAP 139–156
 authentication attribute 140
 binding method 153
 client 150
 group filter 152
 miscellaneous parameters 152
 MPCLI 180
 schema 143
 testing the configuration 148
 user search base DN 152
Linux
 ASU support 161
 GNOME 73, 105
 KDE 72, 104
management module
 remote CD-ROM 113
 remote control 104
 remote diskette 109
 remote image file 117
MPCLI support 180
OpenLDAP 130
RSA II
 drivers 66
 remote CD-ROM 81
 remote control 70
 remote diskette 78
 remote image files 84
SMBridge 198
telnet 201
XDM 72, 104

M

management LAN 240
management module 87–128
 alerting to IBM Director 229
 authentication with LDAP 139–156
 backup the configuration 236
 blade information 122
 BladeCenter Assistant 228
 certificates 131
 configuration 91, 119
 connectors 88
 default hostname 92
 default IP address 92–93
 DHCP 92
 encryption 130–139

Ethernet interface 98
factory defaults 127
failover 99
features 88
firmware update 95, 97, 257
 I/O module 126
 individual blades 121
global login settings 155
I/O module
 firmware updates 126
 tasks 124
installation 91
IP address, default 92–93
KVM connections 99
KVM control 122
LDAP 139–156
MAC address 92
manual switch over 98–99
mass configuration of userids 245
media tray 103
MIB files 97
MPCLI example 189
MPCLI support 176
network settings 92
policy settings 122
ports 126
power control 122, 124
redundant management module 97
remote access to modules 239
remote control 100–119
 keyboard selector 103
 Linux support 104
 media tray 103
 phase calibration 103
 screen alignment 103
remote media 100, 105–119
 CD-ROM 112
 diskette 108
 image file 115
resetting to factory defaults 127
restarting 94
restore the configuration 238
security 130–139
Serial over LAN 124
SNMP MIB files 97
SSH (secure shell) 135
SSL 130, 235
switch over 99
TCP ports 126
telnet interface 221
user authority 89
userid changes on mass 245
wake on LAN 122
Web interface
 configuration 94
 securing 235
Management Processor Assistant 38, 227–228
MIB files
 management module 97
 RSA II 67
MPCLI 175–192
 batching commands 186
 changing SP settings 179
 commands 185
 comparison with other tools 160
 connecting 184
 create userid 190
 Ethernet configuration example 187
 event log example 189
 event logs 179
 example of use 245
 factory defaults 252
 firmware update 190, 257
 functions 178
 health status 179
 installing 181
 LDAP 180
 Linux
 installation 181
 restrictions 180
 logging on 184
 management module example 189
 power control 179
 restrictions 183
 sample scripts 187
 scenario 245
 scripting 180, 186
 nested scripts 191
 Serial over LAN 180
 SP information example 188
 starting 182
 supported servers 176
 syntax 182
 Windows installation 181

N
network

multiple subnets 243

O

On Demand activation
BladeCenter 120
OpenLDAP 130
operator authority
eServer BMC 16
xSeries BMC 32, 39
OSA SMBridge
See SMBridge
Other OS setting, RSA II 61

P

passwords 234
PET traps 13
PKT files
management module 258
MPCLI, using 189, 257
RSA II 63
ports
management module 126
RSA II 85
xSeries BMC 44
power control
MPCLI 179
SMBridge 203
telnet interface 222
which tool supports 160
PowerQuest 267
PuTTY 137

R

read-only authority
eServer BMC 16
xSeries BMC 39
Red Hat
ASU support 161
management module
remote CD-ROM 115
remote control 104
remote diskette 111
remote image file 118
MPCLI support 180
RSA II
remote CD-ROM 81
remote control 71

remote diskette 79
remote image files 85
SMBridge installation 198
SMBridge support 194
SOL, enabling 211
Redbooks Web site 291
Contact us xii
remote console redirection 195
remote control 69
BMC 40
management module 100–119
RSA II 67–85
remote media
management module 105
CD-ROM 112
diskette 108
image file 115
RSA II 74
CD-ROM 80
diskette 77
image file 82
RemoteUX 266
commands 268
parameters 268
return codes 272
Windows support 267
RSA
See also RSA II
ASU support 161
MPCLI support 176
supported servers 2
telnet interface 224
RSA II 47–86
See also RSA
alerting to IBM Director 229
alerts 48
ASM interconnect network 48, 55–56
ASU support 161
authentication with LDAP 139–156
backup the configuration 236
blue screen of death 48
breakout cables 52
certificates 131
configuration 59
connectors 51
default userid 63
DHCP 61
driver 64
encryption 130–139

event log 48
factory defaults 248
features 48, 50
firmware update 62, 257
gateway for ISM processors 58
global login settings 155
health monitoring 48
IBM Director 227
installation 60
interconnect network 48, 56–57
Java runtime 68
LDAP 139–156
Linux
 installation 66
 remote media 75
mass configuration of userids 245
MIB files 67
MPCLI support 176
network settings 60
Other OS setting 61
ports 85
remote control 67, 69–85
 Linux support 70
remote media 74–85
 diskette 77
 files 82
 remote CD-ROM 80
restore the configuration 238
RSA II-EXA 52
security 130–139
SNMP MIB files 67
SSH (secure shell) 135
SSL 130, 235
static address 61
supported servers 2, 49
system board connector 49
TCP ports 85
telnet interface 221
USB cable 49, 60
userid changes on mass 245
video speed 69
Web interface
 securing 235
 using 219
Windows drivers 65
RSA II SlimLine 53
See also RSA II
ASM interconnect network 55
features 48
supported servers 2

S

SAC commands 205
scenarios 233–284
scripting
 ASU 174
 MPCLI 186
security 130–139
 scenario 234
Serial over LAN
 management module 124
 MPCLI 180
 SMBridge 192, 203
ServerProven 68
service processors
 BladeCenter management module 87–128
 eServer BMC 9–18
 ISM Processor 44–46
 RSA II 47–86
 xSeries BMC 18–44
SMASH 5
SMBIOS 5
SMBridge 192–218
 authentication 202
 BIOS settings 195
 bootcfg command 206
 CLI 193, 216
 commands 203, 217
 comparison with other tools 160
 connecting 201
 console command 203
 console redirection 195
 daemon 199
 EMS 200, 205
 EMS, enabling 206
 event log 204
 exiting SOL 206
 F1 key in telnet 200
 GRUB 213
 installation 196
 LILO 211
 Linux support 194
 ports 197
 power control 203
 PXE boot 195
 Red Hat, enabling SOL 211
 remote console redirection 195

SAC 205
SAC commands 205
SAC support 200
Serial over LAN 203
service 198
telnet clients 200
telnet server 192, 199
timeout values 197
Windows SOL 205
SNMP 6
MIB files
management module 97
RSA II 67
xSeries BMC 27
Special Administration Console 200
SSH (secure shell) 135
SSL 130
standards 4
subnets, multiple 243
supervisor authority
eServer BMC 16
xSeries BMC 39
supported servers 2
RSA II 49
utilities 158
SUSE LINUX
ASU support 162
management module
remote CD-ROM 114
remote control 104
remote diskette 109
remote file image 117
MPCLI support 180
RSA II
remote CD-ROM 81
remote control 71
remote diskette 79
remote image files 84
SOL, enabling 214

T

TCP ports
management module 126
RSA II 85
TCP/IP ports
xSeries BMC 44
telnet interface 220–224
commands 221

comparison with other tools 160
SMBridge 192
TFTP server 160, 274
tools
ASU 160–175
bmc_cfg 22–34
comparison 158
IBM Director 225–231
lancfg 11
MPCLI 175–192
RemoteUX 266
securing 236
SMBridge 192–218
Telnet interface interface 220–224
Web interface 219–220

U

UpdateXpress 259, 266
BladeCenter 274
RemoteUX 266
UXBC 274
user authority
xSeries BMC 32
utilities
ASU 160–175
bmc_cfg 22–34
comparison 158
IBM Director 225–228
lancfg 11
MPCLI 175–192
RemoteUX 266
securing 236
SMBridge 192–218
Telnet interface interface 220–224
Web interface 219–220

W

Web interface 219–220
comparison with other tools 160
securing 235
WEBEM 5
Windows
ASU support 161
bootcfg command 206
EMS 200
enabling 206
eServer BMC drivers 17
management module

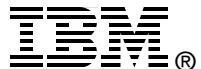
- remote CD-ROM 113
- remote diskette 109
- remote image file 117
- MPCLI support 180
- RSA II
 - drivers 65
 - remote CD-ROM 80
 - remote diskette 78
 - remote image files 84
- SAC 200
- SAC commands 205
- SMBridge
 - installation 196
 - support for 194
- SOL support 205
- xSeries BMC drivers 40

X

- xSeries server
 - support table 2



IBM eServer xSeries and BladeCenter Server Management



IBM *e*server xSeries and BladeCenter Server Management



Redbooks

**Management using
the RSA II adapter,
BMC, and
BladeCenter
Management Module**

**Describes the user
interfaces to use
these hardware
devices**

**Includes scenarios of
how to use the tools**

The systems management hardware that is part of IBM *e*server xSeries and BladeCenter servers serves as an important part of the overall management strategy for customers. This hardware, either integrated into the server or BladeCenter chassis, installed at the factory as an adapter, or available as an option, provides vital information back to the administrator and gives the administrator the ability to remotely control the server, even when the operating system is not running.

This IBM Redbook describes the full range of management hardware currently available for the xSeries and BladeCenter systems. We cover the integrated Baseboard Management Controller, the Remote Supervisor Adapter II family of adapters, and the BladeCenter management module. The user interfaces used to access this hardware are discussed in detail, as is information on how to configure security features such as SSL and authentication features such as LDAP.

This book is aimed at customers, IBM Business Partners, and IBM employees who need to understand the capabilities of our systems management hardware, and how to configure and use them to assist with the management of their servers.

**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**