



M07

Remote Management Adapters

Jason Brunson & Bob Zuber

IBM **@server** xSeries
Technical Conference

Aug. 9 - 13, 2004

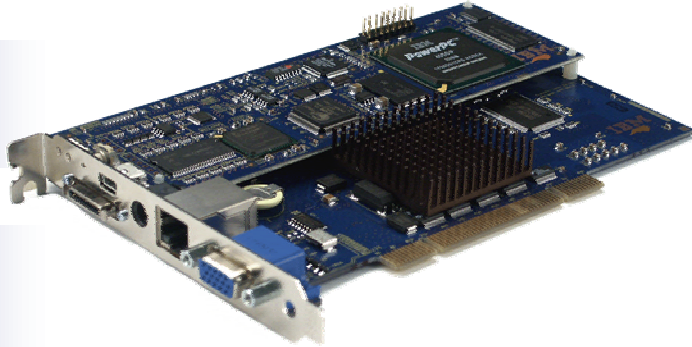
Chicago, IL



Agenda

- RSA II / MM Feature Overview
- System Support
- Management Module Overview
- Recently Added Functions
- LDAP Support/Configuration
- Port Configuration
- Serial-Over-LAN
- New Management Adapters
- Service Processor Tools
- Additional Resources

RSA II/MM Feature Overview



- ...simplifies systems management by providing around-the-clock remote access to the supported xSeries server.
 - Remote management independent of the server status
 - Full remote control of hardware and operating systems
 - Remote update of the xSeries server and RSA firmware
 - Easy-to-use Web-based management from standard Web browsers
 - Environmental Monitoring
 - Predictive Failure Notification
 - View VPD / Error Logs



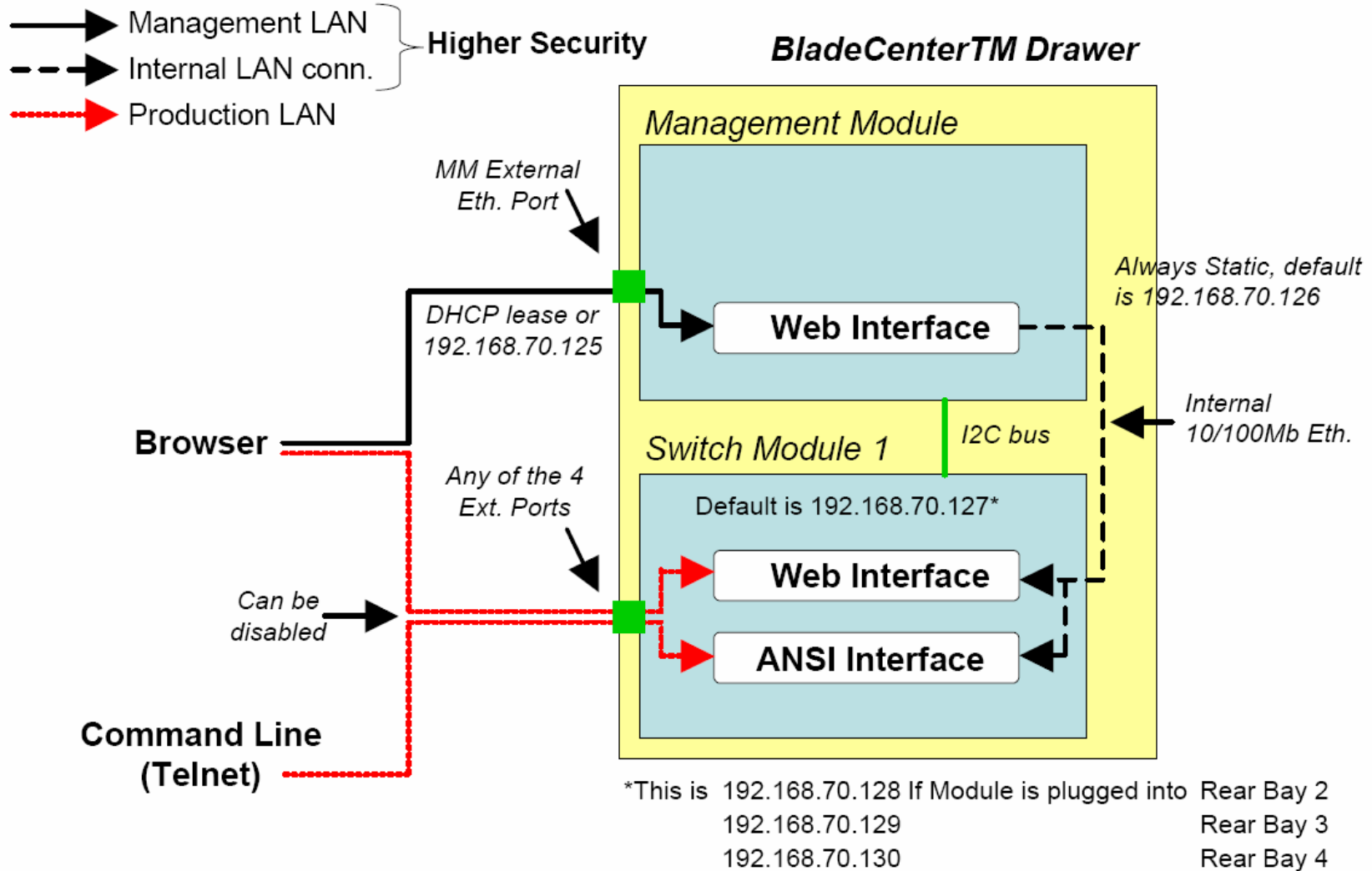
Service Processor System Chart

System	Basic	BMC	RSA	RSA-II	RSA-II (DC) Daughter Card
x205	ASF 1.0 only		Option	Option	N/A
x225 Old Models	ASF 1.0 only		Option	No support	N/A
x225 New Models	ASF 1.0 only		Option	Option	N/A
x206	ASF 2.0 only		N/A	Option	N/A
x226	ASF 2.0 only		N/A	Option	N/A
x306	ASF 2.0 only		N/A	Option	N/A
x235		Non-IPMI (H8)	Option	Option	N/A
x255		Non-IPMI (H8)	Option	Option	N/A
x335		Non-IPMI (H8)	Option	Option (no C2T)	N/A
x345		Non-IPMI (H8)	Option	Option	N/A
e325		OEM IPMI (Qlogic/MSI)	N/A	TBD Option	TBD Option
x236		IBM IPMI (H8/OSA)	N/A	Option (Daughter Card)	Option (Daughter Card)
x336		IBM IPMI (H8/OSA)	N/A	Option (Daughter Card)	Option (Daughter Card)
x346		IBM IPMI (H8/OSA)	N/A	Option (Daughter Card)	Option (Daughter Card)
x365			N/A	Standard	N/A
x445			Standard	Option	N/A
x445			N/A	Standard	N/A
x455			Standard	No support	N/A

Management Module



Management Module Connectivity





Capabilities Unique to the Management Module

- Power controls for all 14 blades
- Video Redirect for any of the 14 blades
- Configuration of I/O Modules (Ethernet/Fibre Switch Modules)
- Diagnostics and power controls for I/O Modules
- Configuration of boot sequence for each blade
- Set local media tray, KVM and power button access.
- Lock down feature to disable local power switch on system
- View hardware logs and system health for all 14 blades in a single log view.
- On Demand- Pay as you grow option.



Management Module Screen Shots

192.168.5.155 BladeCenter Management Module - Microsoft Internet Explorer

BladeCenter Management Module

Bay 1: SYSMANMM

- Monitors
 - System Status
 - Event Log
 - LEDs
 - Hardware VPD
 - Firmware VPD
- Blade Tasks
 - Power/Restart
 - On Demand
 - Remote Control
 - Firmware Update
 - Configuration
 - Serial Over LAN
- IO Module Tasks
 - Power/Restart
 - Management
 - Firmware Update
- MM Control
 - General Settings
 - Login Profiles
 - Alerts
 - Port Assignments
 - Network Interfaces
 - Network Protocols
 - Security
 - Configuration File
 - Firmware Update
 - Restore Defaults
 - Restart MM
- Log Off

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
1	Blade 1	BIOS	BRE131AUS	02/24/2004	1.07
		Diagnostics	BRV18AUS	10/17/2003	1.03
		Blade sys. mgmt. proc.	BRB73DA	n/a	30
2-3	KPR6500	BIOS	BSE117AUS	02/24/2004	1.04
		Diagnostics	BSY113AUS	02/11/2004	1.02
		Blade sys. mgmt. proc.	BRB73DA	n/a	30
4	Blade 5	BIOS	BRE131AUS	02/24/2004	1.07
		Diagnostics	BRV18AUS	10/30/2002	1.00
		Blade sys. mgmt. proc.	BRB73DA	n/a	30
5	SNWZJ1LUL43B19G	BIOS	FW04251120	06/17/2004	
		Blade sys. mgmt. proc.	BQRT16A	n/a	16
6	SNWZJ1LUL43B140	BIOS	BFV0413000	03/23/2004	
		Blade sys. mgmt. proc.	BQRT15A	n/a	15

IO Module Firmware VPD

Bay	Type	Firmware Type	Build ID	Released	Revision
1	Ethernet SM	Boot ROM	BRESMB4G	11/30/2002	04
		Main Application 1	BRESMR4G	05/13/2004	92
2	Ethernet SM	Boot ROM	BRESMB4G	11/30/2002	04
		Main Application 1	BRESMR4G	05/13/2004	92
4	Optical PM	Boot ROM	BROROP4M	08/26/2003	07

Management Module Firmware VPD

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	SYSMANMM	Main application	BRE759F	CNETMUS.PKT	04-14-04	16

192.168.5.238 - BladeCenter Remote Control - Microsoft Internet Explorer

Change KVM/Media Tray Owner

Change KVM owner: Blade4 - HS40DAU → Change media tray owner: Blade4 - HS40DAU

Remote Disk

Select File... Write Protect Mount Drive Refresh List

Remote Console

Blade4 - HS40DAU

JS 104 key Ctrl Alt Tab F1 Insert Caps Lock Num Lock Scroll Lock

Welcome to Windows
Microsoft Windows Server 2003 Standard Edition
Copyright © 1986-2003 Microsoft Corporation
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

192.168.5.238 BladeCenter Management Module - Microsoft Internet Explorer

BladeCenter Management Module

Bay 1: BC1MM

- Monitors
 - System Status
 - Event Log
 - LEDs
 - Hardware VPD
 - Firmware VPD
- Blade Tasks
 - Power/Restart
 - On Demand
 - Remote Control
 - Firmware Update
 - Configuration
 - Serial Over LAN
- IO Module Tasks
 - Power/Restart
 - Management
 - Firmware Update
- MM Control
 - General Settings
 - Login Profiles
 - Alerts
 - Port Assignments
 - Network Interfaces
 - Network Protocols
 - Security
 - Configuration File
 - Firmware Update
 - Restore Defaults
 - Restart MM
- Log Off

Event Log

Monitor log state events

Severity	Source	Date
Error	BLADE_01	08/06/04
Warning	BLADE_02	08/05/04
Info	BLADE_03	08/03/04

Note: Hold down Ctrl to select more than one option. Hold down Shift to select a range of options.

Filters: None

Index	Seq	Source	Date/Time	Text
1	I	SERVPROC	08/06/04, 16:14:12	Remote Login Successful. Login ID: 'USERID' from WEB browser at IP@=192.168.5.225
2	I	SERVPROC	08/05/04, 14:52:22	Remote Login Successful. Login ID: 'tenaburg' from WEB browser at IP@=192.168.1.200
3	I	BLADE_04	08/05/04, 14:48:19	(HS40DAU) Blade System Mgmt Processor Reset
4	I	BLADE_04	08/05/04, 14:48:19	(HS40DAU) Blade Server Powered Up
5	I	SERVPROC	08/05/04, 14:48:09	Blade Server 4 was installed.
6	I	SERVPROC	08/05/04, 14:48:19	Blade Server 4 was removed.
7	I	BLADE_04	08/05/04, 14:46:16	(HS40DAU) Blade Server Powered Down
8	I	SERVPROC	08/05/04, 14:45:16	Blade Server 11 was installed.
9	I	SERVPROC	08/05/04, 14:44:32	Blade Server 11 was removed.
10	I	SERVPROC	08/05/04, 09:52:04	Remote Login Successful. Login ID: 'CONCENTRA' from WEB browser at IP@=192.168.1.84
11	I	BLADE_11	08/05/04, 09:49:51	(SNWZJ1T573B1M14M) Blade Server Powered Up
12	I	BLADE_11	08/05/04, 09:49:46	(SNWZJ1T573B1M14M) User: USERID attempting to power on blade.
13	I	BLADE_04	08/05/04, 09:49:43	(HS40DAU) Blade System Mgmt Processor Reset
14	I	BLADE_04	08/05/04, 09:49:43	(HS40DAU) Blade Server Powered Up
15	I	BLADE_04	08/05/04, 09:49:43	(HS40DAU) User: USERID attempting to power on blade.

192.168.5.155 BladeCenter Management Module - Microsoft Internet Explorer

BladeCenter Management Module

Bay 1: SYSMANMM

- Monitors
 - System Status
 - Event Log
 - LEDs
 - Hardware VPD
 - Firmware VPD
- Blade Tasks
 - Power/Restart
 - On Demand
 - Remote Control
 - Firmware Update
 - Configuration
 - Serial Over LAN
- IO Module Tasks
 - Power/Restart
 - Management
 - Firmware Update
- MM Control
 - General Settings
 - Login Profiles
 - Alerts
 - Port Assignments
 - Network Interfaces
 - Network Protocols
 - Security
 - Configuration File
 - Firmware Update
 - Restore Defaults
- Log Off

Blade Policy Settings

These settings apply to all blade bays (including the empty bays).

Local power control: Enabled
Local KVM control: Enabled
Local media tray control: Enabled
Wake on LAN: Enabled

Save

Boot Sequence

Follow the links in the Name column to edit the boot sequence settings of individual blade servers.

Bay	Name	1 st Device	2 nd Device	3 rd Device	4 th Device
1	Blade 1	Network - PXE	CD-ROM	Floppy	Hard drive 0
2					
3	KPR6500	Network - PXE	Floppy	CD-ROM	Hard drive 0
4	Blade 5	Network - PXE	CD-ROM	Floppy	Hard drive 0
5	SNWZJ1LUL43B19G	Hard drive 0	No device	No device	No device
6	SNWZJ1LUL43B140	Network - BOOTP	Hard drive 0	No device	No device
7	No blade present				
8	No blade present				



Recently Added Functions to the RSA II & MM

- SSH
- LDAP/LDAPS Support
- Configurable Ports
- More Granular Security Settings
- Customizable Keyboard Macros (RSA II Only)
- Serial Over LAN
- ASU utility for command line configuration
- RSA II support for NetWare 6.5 on select systems



LDAP Support- Today

Directories Supported:

- Active Directory for Windows 2000
- Active Directory for Windows 2003
- Novell eDirectory version 8.7.1

Service Processor Type	Servers Supported
Management Module	N/A
RSA II	X235, x255, x335, x345, x365, x445
RSA I	X360, x440, x445, x450, x455

LDAP Configuration

[Permissions](#)

The screenshot illustrates the LDAP configuration process in the IBM BladeCenter Management Module. It shows three overlapping browser windows. The top window shows the main navigation menu. The middle window shows the 'Login Profiles' page with a table of profiles:

Login ID	Access
1. _USERID	Read/Write
2. _lenaburg	Read/Write
3. _xcat	Read/Write
4. _TEST	Read/Write
5. _wwigley	Read/Write
6. ~ not used ~	
7. _shanson	Read/Write
8. ~ not used ~	
9. ~ not used ~	
10. ~ not used ~	
11. ~ not used ~	
12. _gregc	Read/Write

The bottom window shows the 'Global Login Settings' dialog box. The 'User authentication method' dropdown is set to 'LDAP first, then Local'. Other options include 'Local only', 'LDAP only', 'Local first, then LDAP', and 'LDAP first, then Local'. The 'madmin Properties' dialog box is also visible on the right side of the screen.

Enabling SSL/SSH

The image shows a stack of Microsoft Internet Explorer browser windows. The top window displays the configuration page for the Remote Supervisor Adapter II. The page includes sections for Trusted CA Certificates, Secure Shell (SSH) Server, and SSH Server Key Management. The SSH Server dropdown menu is set to 'Enabled'. The page also contains copyright information for Eric Young (eay@cryptsoft.com) and a license notice for OpenSSL.

Remote Supervisor Adapter II

Trusted CA Certificate 2

Trusted CA Certificate 3

Secure Shell (SSH) Server

SSH Server:

SSH Server Key Management

SSH server key status: SSH Server key is installed.

This product may contain OpenSSL software. OpenSSL bears the following license terms.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

Custom Login Profiles

The screenshot displays the BladeCenter Management Module web interface in Microsoft Internet Explorer. The browser address bar shows the URL: `http://192.168.5.238/private/main.ssi`. The page title is "BladeCenter Management Module".

The left navigation pane shows the following structure:

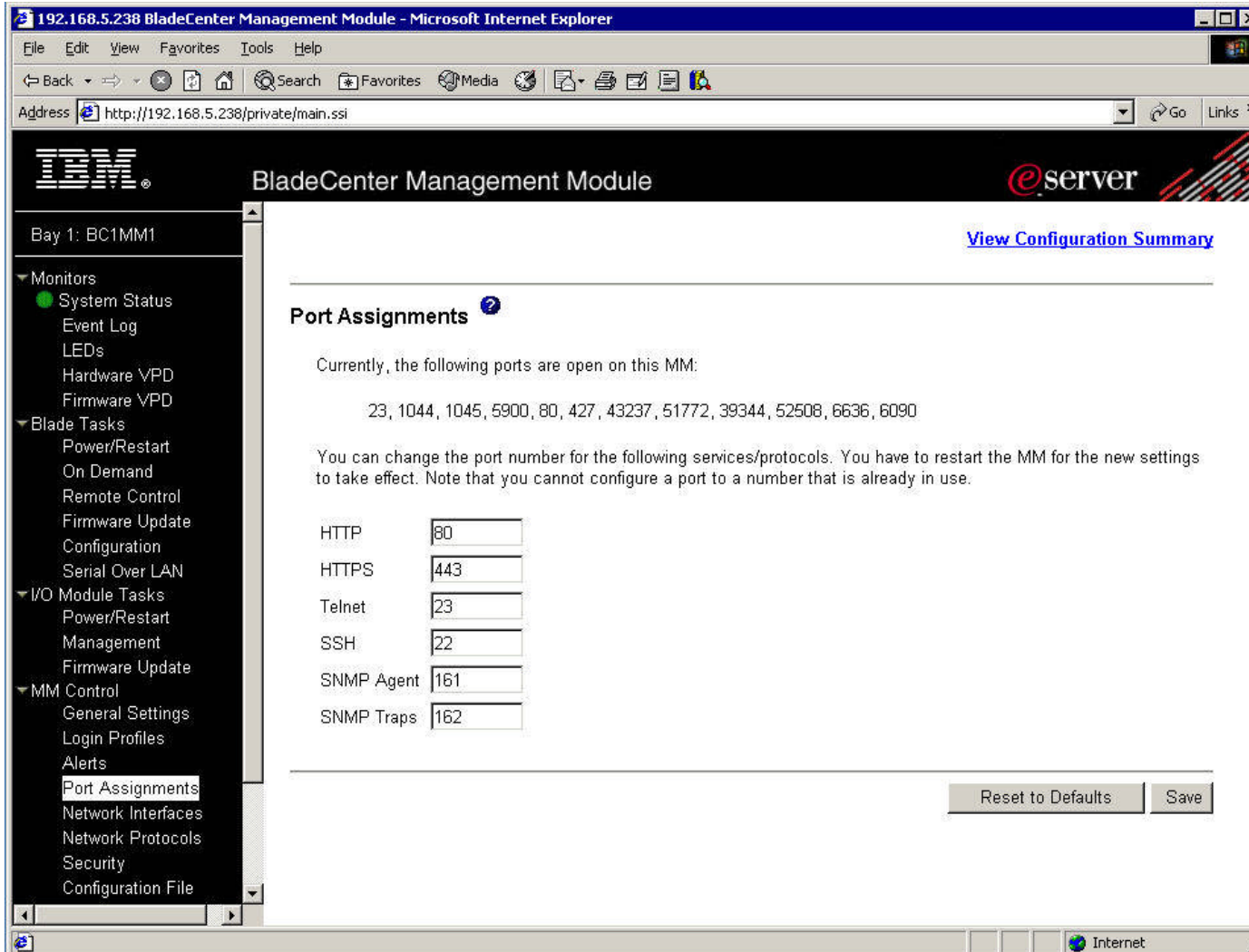
- Bay 1: BC1MM1
 - Monitors
 - System Status
 - Event Log
 - LEDs
 - Hardware VPD
 - Firmware VPD
 - Blade Tasks
 - Power/Restart
 - On Demand
 - Remote Control
 - Firmware Update
 - Configuration
 - Serial Over LAN
 - I/O Module Tasks
 - Power/Restart
 - Management
 - Firmware Update
 - MM Control
 - General Settings
 - Login Profiles**
 - Alerts
 - Port Assignments
 - Network Interfaces
 - Network Protocols
 - Security
 - Configuration File

The main content area is titled "Login Profile 6" and contains the following configuration options:

- Login ID:
- Password:
- Confirm password:
- Authority Level:
 - Supervisor
 - Read-Only
 - Custom
 - User Account Management
 - Blade Server Remote Console Access
 - Blade Server Remote Console and Virtual Media Access
 - Blade and I/O Module Power/Restart Access
 - Ability to Clear Event Logs
 - Basic Configuration (MM, I/O Modules, Blades)
 - Networking & Security Configuration
 - Advanced Configuration (MM, I/O Modules, Blades)

At the bottom of the configuration area, there are buttons for "Reset to Defaults", "Cancel", and "Save".

Port Configuration



The screenshot shows the BladeCenter Management Module web interface in Microsoft Internet Explorer. The browser title is "192.168.5.238 BladeCenter Management Module - Microsoft Internet Explorer". The address bar shows "http://192.168.5.238/private/main.ssi". The page header includes the IBM logo, "BladeCenter Management Module", and the "e server" logo. A navigation menu on the left lists various system components, with "Port Assignments" selected. The main content area displays the "Port Assignments" configuration page. It includes a "View Configuration Summary" link, a list of currently open ports, and a table for configuring port numbers for various services. A note indicates that changes require a restart of the MM. At the bottom right, there are "Reset to Defaults" and "Save" buttons.

192.168.5.238 BladeCenter Management Module - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail News RSS

Address http://192.168.5.238/private/main.ssi Go Links >>

IBM BladeCenter Management Module e server

Bay 1: BC1MM1 [View Configuration Summary](#)

Monitors

- System Status
- Event Log
- LEDs
- Hardware VPD
- Firmware VPD

Blade Tasks

- Power/Restart
- On Demand
- Remote Control
- Firmware Update
- Configuration
- Serial Over LAN

I/O Module Tasks

- Power/Restart
- Management
- Firmware Update

MM Control

- General Settings
- Login Profiles
- Alerts
- Port Assignments**
- Network Interfaces
- Network Protocols
- Security
- Configuration File

Port Assignments ?

Currently, the following ports are open on this MM:

23, 1044, 1045, 5900, 80, 427, 43237, 51772, 39344, 52508, 6636, 6090

You can change the port number for the following services/protocols. You have to restart the MM for the new settings to take effect. Note that you cannot configure a port to a number that is already in use.

HTTP	<input type="text" value="80"/>
HTTPS	<input type="text" value="443"/>
Telnet	<input type="text" value="23"/>
SSH	<input type="text" value="22"/>
SNMP Agent	<input type="text" value="161"/>
SNMP Traps	<input type="text" value="162"/>

Internet



RSA II and MM Port Utilization

RSA II		Management Module
Configurable		
HTTP	80	
HTTPS	443	
Telnet	23	
SSH	22	
SNMP Agent	161	
SNMP Traps	162	
Reserved		
TCP e-mail alerts	25	
UDP DNS resolver	53	
DHCP client connection using UDP	68	
Video Redirect	2000	5900
Remote Disk	1044	
Remote Disk on Card (persistent)	1045	
SLP (Service Location Protocol)	427	
IBM Director commands using TCP/IP	6090	
Partition Management	7070-7074	
IBM Director Alerting using UDP	13991	

Serial-Over-LAN Configuration - MM



192.168.5.238 BladeCenter Management Module - Microsoft Internet Explorer

Address <https://192.168.5.238/private/main.ssi>

IBM BladeCenter Management Module @server

Bay 1: BC1MM1

- Monitors
 - System Status
 - Event Log
 - LEDs
 - Hardware VPD
 - Firmware VPD
- Blade Tasks
 - Power/Restart
 - On Demand
 - Remote Control
 - Firmware Update
 - Configuration
 - Serial Over LAN**
- I/O Module Tasks
 - Power/Restart
 - Management
 - Firmware Update
- MM Control
 - General Settings
 - Login Profiles
 - Alerts
 - Port Assignments
 - Network Interfaces
 - Network Protocols
 - Security
 - Configuration File
 - Firmware Update
 - Restore Defaults
 - Restart MM

Serial Over LAN (SOL)

Use the following links to jump down to different sections on this page.

[Serial Over LAN Status](#)

[Serial Over LAN Configuration](#)

Serial Over LAN Status

Click the checkboxes in the first column to select one or more blade servers; then, click one of the links below the table to enable or disable SOL on the selected blades.

Note: You have to enable the global "Serial over LAN" flag above before enabling SOL on individual blade servers.

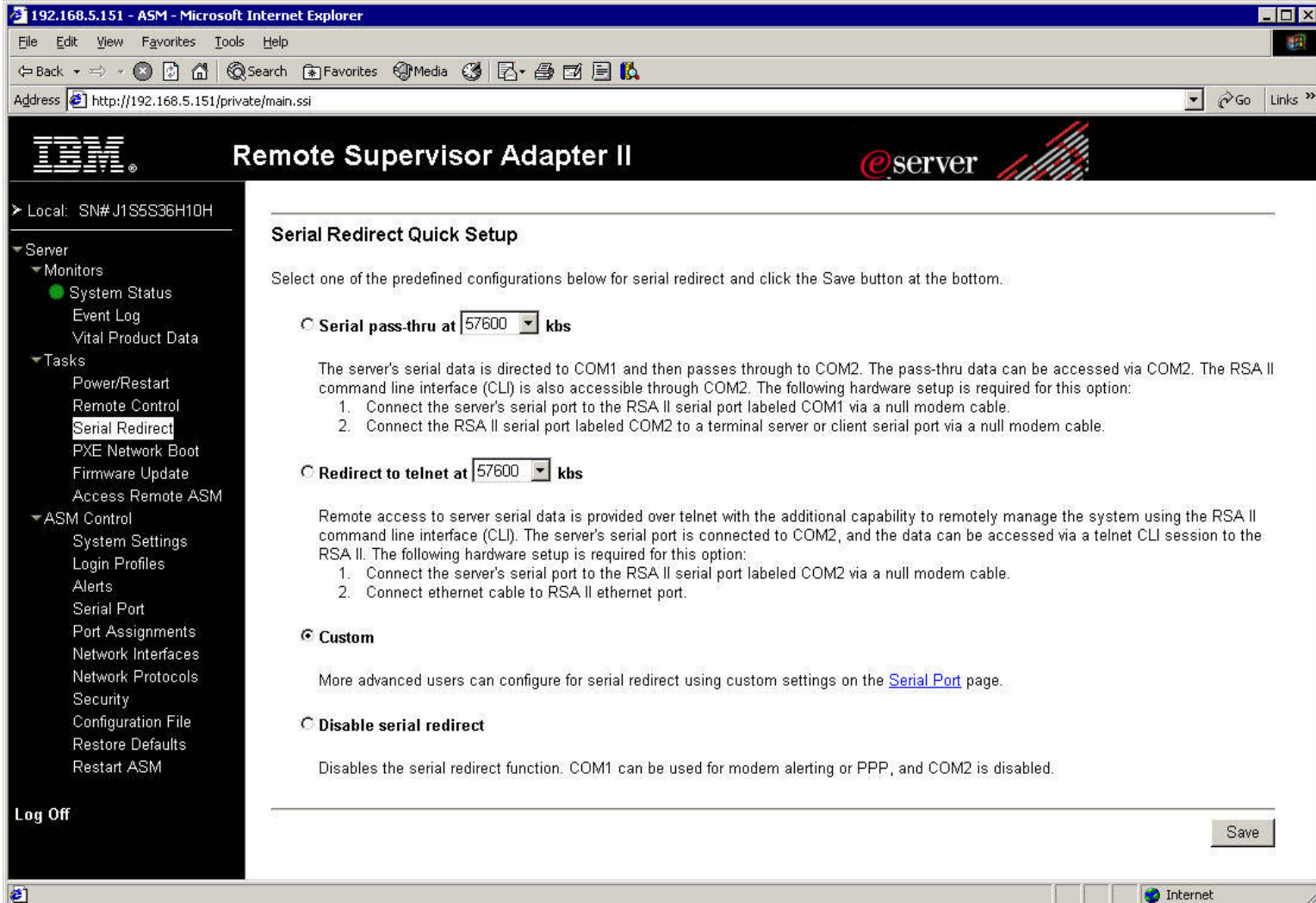
<input type="checkbox"/>	Bay	Name	SOL	SOL Session	BSMP IP Address
<input type="checkbox"/>	1	SN#ZJ1TS73CT1H2	Enabled	Ready	10.10.10.80
<input type="checkbox"/>	2	SN#ZJ1TS73CK153	Enabled	Ready	10.10.10.81
<input type="checkbox"/>	3	SN#ZJ1TS73CH14T	Enabled	Ready	10.10.10.82
<input type="checkbox"/>	4	SN#ZJ1TS73CMLD4	Enabled	Ready	10.10.10.83
	5	No blade present			
<input type="checkbox"/>	6	SN#ZJ1TS73BL19B	Enabled	Not ready	10.10.10.85
<input type="checkbox"/>	7	SN#ZJ1TS73B8198	Enabled	Not ready	10.10.10.86
	8	No blade present			
<input type="checkbox"/>	9	SN#ZJ1TS73BM1DT	Enabled	Not ready	10.10.10.88
	10				
<input type="checkbox"/>	11	SN#ZJ1TS73BM14M	Enabled	Not ready	10.10.10.90
	12				
<input type="checkbox"/>	13	SN#ZJ1TS73BM19M	Enabled	Not ready	10.10.10.92
	14				

[Disable Serial Over LAN](#)

[Enable Serial Over LAN](#)

Done Internet

Serial Redirect Configuration – RSA II



The screenshot shows a web browser window titled "192.168.5.151 - ASM - Microsoft Internet Explorer". The address bar shows "http://192.168.5.151/private/main.ssi". The page header includes the IBM logo, "Remote Supervisor Adapter II", and the "eServer" logo. A left-hand navigation menu lists various system management options, with "Serial Redirect" highlighted. The main content area is titled "Serial Redirect Quick Setup" and contains the following text:

Select one of the predefined configurations below for serial redirect and click the Save button at the bottom.

Serial pass-thru at 57600 kbs

The server's serial data is directed to COM1 and then passes through to COM2. The pass-thru data can be accessed via COM2. The RSA II command line interface (CLI) is also accessible through COM2. The following hardware setup is required for this option:

1. Connect the server's serial port to the RSA II serial port labeled COM1 via a null modem cable.
2. Connect the RSA II serial port labeled COM2 to a terminal server or client serial port via a null modem cable.

Redirect to telnet at 57600 kbs

Remote access to server serial data is provided over telnet with the additional capability to remotely manage the system using the RSA II command line interface (CLI). The server's serial port is connected to COM2, and the data can be accessed via a telnet CLI session to the RSA II. The following hardware setup is required for this option:

1. Connect the server's serial port to the RSA II serial port labeled COM2 via a null modem cable.
2. Connect ethernet cable to RSA II ethernet port.

Custom

More advanced users can configure for serial redirect using custom settings on the [Serial Port](#) page.

Disable serial redirect

Disables the serial redirect function. COM1 can be used for modem alerting or PPP, and COM2 is disabled.

A "Save" button is located at the bottom right of the configuration area.



New Management Adapters

- **Baseboard Management Controller**

- New embedded service processor for new xSeries servers
- Initial systems to include the controller are x236, x336, and x346
- IPMI 1.5 compliant
- Has the following capabilities:

- **Monitoring**

- System voltages
- Battery voltage
- System temperature
- Fan tachometer monitor
- Power Good signal
- Fan speed control
- NMI detection
- SMI detection and generation

- **Power Controls**

- System power on/off
- System reset

- **System ID and planar version detection**

- **LED Controls**

- Control of Lightpath LEDs
- System LEDs control (pwr, HDD activity, alert, heartbeat, etc)

- **Serial Port text redirection**



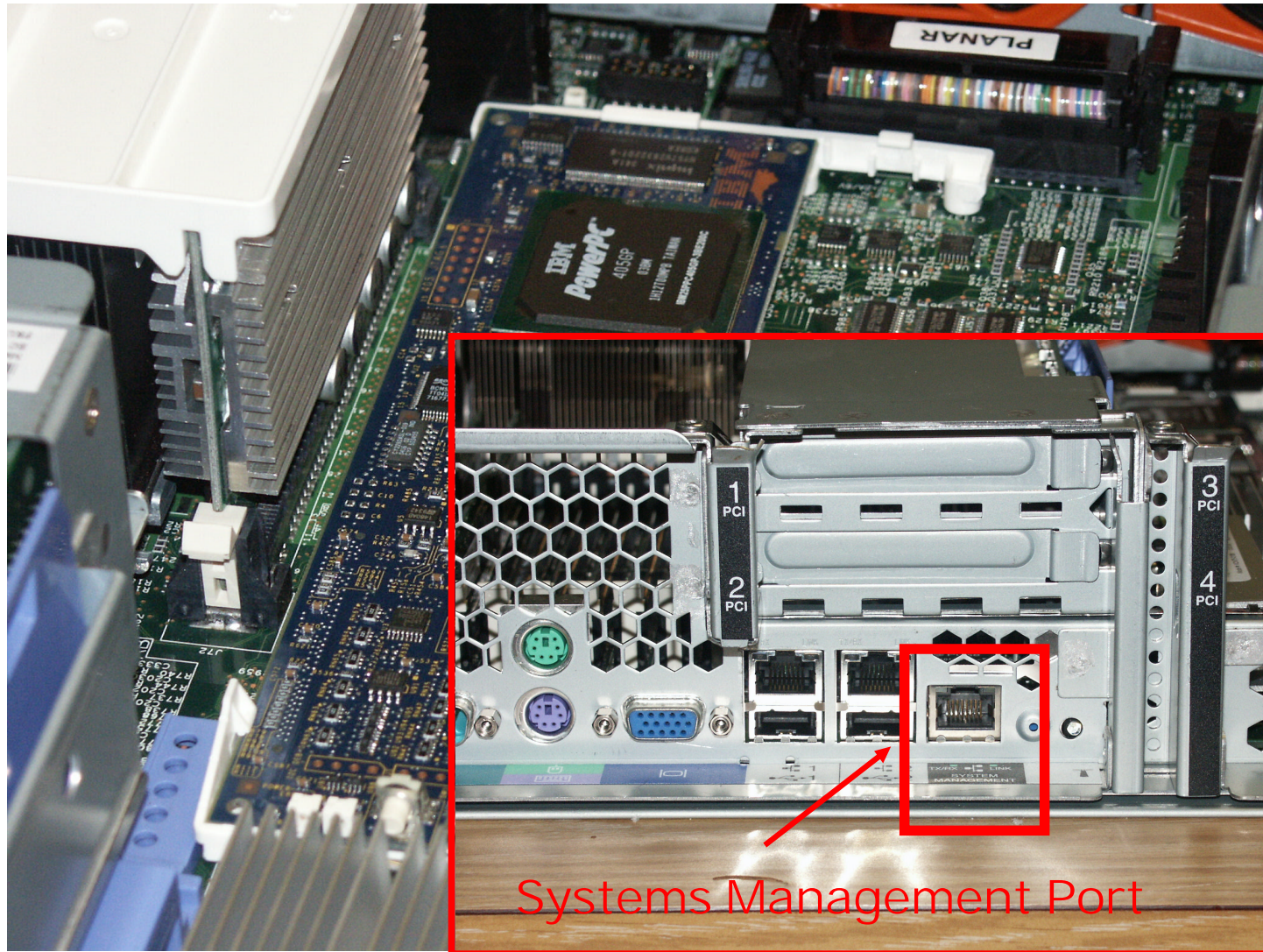
New Management Adapters (cont.)

- **Remote Supervisor Adapter II Slim-line Adapter**

- Option for x236, x336, and x346
- Adds the following capabilities:

- Web Server
- Graphical Console Redirection
- Blue Screen Capture
- Save/Restore Configuration
- Remote Boot from floppy and CD
- PXE Network Boot
- VPD
- IPMI support to Vulture (dot commands external)
- DHCP, DNS, PPP, SSL, LDAP
- Login Profiles
- Full SNMP
- Director alerts
- Pager alerts
- e-mail alerts via SMTP
- Event Log
- Power Control
- Device Drivers for in-band management
 - Windows
 - Linux

RSA-II Slimline Adapter



Systems Management Port



Service Processor Tools

- **Management Processor Command Line Interface (MPCLI)**

- ü Provides remote and local access

- ü Provides the ability to:

- Ø configure the RSA, RSA II and MM (i.e. IP Address, SNMP, Accounts)

- Ø query information from the adapter (i.e. temperatures, voltages, logs)

- Ø power system (power off, power on, restart)

- ü Supported on both Linux and Windows

- **Advanced Settings Utility (ASU)**

- ü Provides the ability to make CMOS configuration changes via command line

- ü Provides the ability to make configuration changes to the RSA/RSA II via command line (requires RSA/RSA II device driver be loaded and rsa.def file to be applied to ASU tool.)

- ü Supported under DOS, Windows and Linux (RSA config. Windows/Linux only)



Service Processor Tools (cont.)

- **BladeCenter Command line interface**

- ü Available over Telnet or SSH

- ü Allows for the following against the BladeCenter

- Ø Configuration of MM settings (i.e. DNS, IP, Alert Actions, Users)

- Ø Power controls against blades (power on/power off)

- Ø Query for health information

- Ø Read and manipulate logs

- Ø Read environmental data

- **RSA II Command line interface**

- ü Serial Console redirect

- ü Power control (power on, power off, and reset

- ü Restsart the RSA II.



Service Processor Tools (cont.)

- **BMC_CMD.EXE**

- ü Command line utility used to configure the BMC

- ü Allows for the following against the BMC

- Ø IP Setting (MAC Address, IP Address, Subnet Mask)

- Ø Account Settings

- Ø Trap destination settings

```
BMC Config Utility V1.12.0.15, (C)2004 OSA Technologies, Inc.

1.  Get Device ID
2.  IPM Device "Global" Commands Group
3.  BMC Device and Messaging Commands Group
4.  Chassis Device Commands Group
5.  SDR Device Commands Group
6.  SEL Device Commands Group
7.  LAN Device Commands Group
8.  Serial/Modem Device Commands Group
9.  Manual Command Configuration

(h)Help (e)Exit

=> Enter your choice:
```



Additional Resources

- MPCLI (Management Processor Command Line Interface 2.01)

- Users Guide:

- <http://www-1.ibm.com/support/docview.wss?uid=psg1MIGR-54214>

- Code:

- <http://www-3.ibm.com/pc/support/site.wss/MIGR-54216.html>

- ASU (Advanced Settings Utility)

- DOS

- <http://www-306.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55021>

- Linux

- <http://www-306.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55020>



Additional Resources (cont.)

- Windows

<http://www-306.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55019>

- def files to patch the ASU tool will be on the download sight for each specific system's firmware and device driver page.

- RSA II and Management Module Documentation

✓ RSA II Installation Guide for Windows 2000/2003 - 235, 255, 345:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-50986>

✓ RSA II Installation Guide for Linux – 205, 235, 255, 345:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-50987>



Additional Resources (cont.)

RSA II and Management Module Documentation (cont.)

- ✓ RSA II Technical Update- Linux:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-50314>

- ✓ LDAP User's Guide for RSA and Management Module:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55014>

- ✓ RSA II User Guide:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-50315>

- ✓ RSA II-EXA Installation Guide for x445:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-53760>

- ✓ RSA II-EXA Technical Update for Linux:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-53793>



Additional Resources (cont.)

RSA II and Management Module Documentation (cont.)

- ✓ Obtaining RSA II Firmware and Device Driver Updates:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-54748>

- ✓ RSA II Installation Guide- Servers:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-50316>

- ✓ Connecting to ASM Interconnect network – x335:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-54747>

- ✓ Management Module User's Guide:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-45153>

- ✓ Management Module Command Line Interface Reference Guide:

<http://www-307.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-54667>



Thank You ! ! !



Backup Slides



LDAP Authority Level Attribute

The UserAuthorityLevel attribute is read as a bit-string of 0s and 1s. The bits are numbered from left to right. The first bit is bit position 0. The second bit is bit position 1, and so on.

- Bit position 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 position 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 be individually set the other bits.
- Bit position 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 position 3 - **Networking & 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 position 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 position 5 - **Remote Console Access**. If set, a user can access the remote server console. **For the BladeCenter management module only:** Bit position 5 - **Blade Server Remote Console Access**. If set, a user can access a remote blade server video console with keyboard and mouse control.
- Bit position 6 - **Remote Console and Virtual Media Access**. If set, a user can access the remote server console and the virtual media functions for the remote server. **For the BladeCenter management module only:** Bit position 6 - **Blade Server Remote Console and Virtual Media Access**. If set, a user can access a remote blade server video console with keyboard and mouse control and can also access the virtual media features for that remote blade server.

LDAP Authority Level Attribute (cont.)



- Bit position 7 - **Remote Server Power/Restart Access**. If set, a user can access the power on and restart functions for the remote server. These functions are available in the Power/Restart page in the Web interface. **For the BladeCenter management module only:** Bit position 7 - **Blade Server and I/O Module Power/Restart Access**. If set, a user can access the power on and restart functions for the blade servers and I/O modules. These functions are available on the Blade Tasks Power/Restart page and the I/O Module Tasks Power/Restart page in the Web interface.
- Bit position 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 position 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 position 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 position 11 - **Reserved**. Reserved for future use.

The following list contains examples and their descriptions:

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

[Back](#)



LDAP Binding Methods

Binding Method	Description
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.
Client Authentication	Bind attempt is made with client DN and password specified by this configuration parameter. If the bind is successful, we proceed as above.
User Principal Name (UPN)	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. Note that for Active Directory servers, the userid can have the form <code>someuser@domain</code> or simply <code>someuser</code> .
Strict UPN	This is the same as UPN above, except that the userid must have the form <code>someuser@domain</code> . The string entered by the user will be parsed for the <code>@</code> symbol.



RSA II Command Line Interface (CLI)

- **Each CLI command has the following format:**
 - command [arguments] [-options]
 - Example
 - `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
 - Up to 2 con-current sessions
 - One command per line
 - Primitive editor, no continuation to allow longer syntax lines.
- **Limited set of commands, does not cover fully Web UI commands.**
- **CLI Commands**
 - **Utility Commands**
 - Monitor Commands
 - Server Power Commands
 - Serial Redirection Commands
 - Configuration Commands
 - ASM Control Commands



RSA II CLI continued

- **Utility Commands**

- Help – same as ?, displays the list of commands and their description.
- History – displays a list of the last 8 executed commands.
- Exit – logs off the user, and terminates the CLI session.

- **Monitor Commands**

- Syshealth – Displays the system health, power, system state, restart count, and device driver status.
- Readlog – Displays the ASM event log, displays 5 at a time.
- Clearlog – Clears the ASM event log.
- Temps – Displays all of the temperatures and their thresholds.
- Fans – Displays the fan speeds for all of the fans that are installed in the server.
- Volts – Displays all of the voltages and their thresholds.
- VPD – Vital Product Data of : sys, asm, bios, ismp, and exp

- **Serial Redirection Commands**

- Console – Starts a serial redirection session to the port specified, ie. “Console 1”

RSA II CLI continued

• Configuration Commands

- Timeouts – Display or change the timeout values, all values are in minutes
 - § -p <POST_watchdog_option>, values : disable, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
 - § -o <OS_watchdog_option>, values : disabled, 2.5, 3, 3.5, 4
 - § -l <loader_watchdog_option>, values : disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
 - § -f <power_off_delay_option>, values : disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
 - § -n <NMI_reset_delay_option>, values : disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4
- Ifconfig – Configure the ethernet port values
 - § Options : -state <interface_state>, -c <config_method>, -i <static_ip_address>, -g <gateway_address>, -s <subnet_mask>, -n <hostname>, -r <data_rate>, -d <duplex_mode>, -m <max_transmission_unit>, -l <locally_administered_MAC>, -b <burned in MAC address>
- DHCPinfo – Displays the DHCP information for the ethernet port.
 - § Options : -server, -n, -i, -g, -s, -d, -dns1, -dns2, -dns3
- Portcfg – Configure the serial port
 - § Options : -serred <serial_redirect_mode>, -b <baud_rate>, -p <parity>, -s <stop_bits>, -climode <cli_mode>, -cliauth <cli_auth>
 - § Syntax : portcfg com1 -b 57600
- Srcfg – Serial redirection configuration command
 - § Options : -passthru <passthru_mode>, -entercliseq <entercli_keyseq>, -exitcliseq <exitcli_keyseq>
- Users – Configure new/old user ids and passwords
 - § Options : -<user number>, -n <username>, -p <password>, -a <authority level>



RSA II CLI continued

- **Server Power Commands**

- Power : On/Off/State, On, Off, and shows the state of the server, ie. On/off.
 - § Off includes –s parameter to request OS shutdown before server powers off.
- Reset : Reset or restart the server, includes –s parameter mentioned above.

- **ASM Control Commands**

- Resetsp – Resets the RSA II, same as the power reset command.
- Clearcfg – Resets the RSA II to its factory defaults
- Update – Updates the firmware of the RSA
 - § Options : –i <TFTP_server_IP_address> -l <filename>, -v verbose
- Clock – Display or change the clock on the RSA II
 - Options : -d <mm/dd/yyyy>, -t <hh:mm:ss>, -g <gmt offset>, -dst <on/off/special case >



Future Systems Management Enhancements



Plan Change Request - PCR

- **Plan Change Request**

- Customer request for a new feature/function that is not in plan for any product.

- **Status Field**

- RCVD, APPR, PEND, PROG, DEFR, DENY, CLOS

- Weekly SW PLMT to discuss each PCR.
- Provide a link on the Systems Management web page to a table that contains same information
- Once development has completed the code, will track through build process using the defect/feature number.
- Table contains all products, in addition to Build and Release Number for each PCR.
- Separate PCR Notes database used for Management approval process.

Issue Number	PCR Number	Plan Change Request Description	Date Received	Priority	Status	Customer	Development	Test	Defect/Feature Number	Case Number (PE)	Impact
Critical											
1	Submitted	RSA II Linux Client for Remote Disk support (Mozilla Browser) SSH code Support for x335.		1	APPR	HSBC					Same as one above
2				1	CLOS	Morgan Stanley	Completed	In progress			Purchase Dell
3		Change Port Number for VNC on MM I		1	PEND	TX State Bank, Bellsouth					
4	Submitted	Virtual media CLI, along with Linux support SOL over RSA II Slimline LAN	1/06/2004	1	APPR	Verizon, HSBC, Fidelity, Bear Stearns All Linux customers	In Progress				No Linux Client Support for the Remote Media No SOL on RSA II on x236, x336, x346
5		Change Port number for Blaster Virus		1	PROG	BellSouth	Completed	In progress	232196		BellSouth will not buy until fixed
7		Remove BMC Access via IPMI if RSA II Slimline is installed. (Customer configurable)		1	APPR	All customers					Security violation
8		Embedded CLI for RSA II	1/10/2003	1	PROG	ADP, All customers	Completed	In progress	237939		



PCR - Details

RSA II PCR Schedule (Planned Support Date, Subject to Change)																													
Issue Number	PCR Number	Plan Change Request Description	Date Received	Priority	Status	Customer	Development	Test	Defect/Feature Number	Case Number (FE)	Impact	MM1	MM2	Double Edge	Jasper	Juniper	Pearl	Palmetto	Opal	Spruce	Granite	Redwood	Turquoise	Goode	Avatar	Maia	Cruzeador		
Critical																													
1	Submitter	RSA II Linux Client for Remote Disk Support (Maxilla Browser)		1	APPR	HSPC					Some user abuse	1	N/A	4084	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2	N/A	3	N/A	4	N/A	5	N/A
2		SSH needs support for x335.		1	CLOS	Marque Stalder	Completed	In Progress			Parakeet Drill	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Squelch GR 18/04	TZER159A Released in 5.84	Squelch GR 18/04	N/A	Squelch GR 18/04	N/A	Squelch GR 2085	N/A
3		Change Part Number for VNC on MM1		1	PEND	TX State Bank, Drillsack						1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	Submitter	Virtual media CLI, along with Linux support	6/1/2004	1	APPR	Veritas, HSPC, Fidality, Secur Storage	In Progress				No Linux Client Support for the Remote Media No SOL on RSA II on x236, x336, x346	1																	Squelch GR 2085
5		SOL over RSA II Slimline LAN		1	APPR	All Linux customers						N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	3	N/A	2	N/A	1	N/A	2085	N/A
6		Change Part number for Master Vnc		1	PROG	Drillsack	Completed	In Progress	232436		Drillsack will not be nullified Security violation											Squelch GR 18/04	Squelch GR 18/04		Squelch GR 18/04		Squelch GR 2085		
7		Remove BMC Access via IPMI if RSA II Station is installed. [Customer specific] Embedded CLI for RSA II	10/1/2003	1	APPR	All customers	Completed	In Progress	232393							5/28/2004	N/A	5/28/2004	N/A	Squelch GR 22	N/A	Squelch GR 18/04	N/A	Squelch GR 18/04	N/A	Squelch GR 18/04	N/A	Squelch GR 2085	N/A
8				1	PROG	ADP, All customers	Completed	In Progress	232393			2085		N/A	N/A	5/28/2004	N/A	5/28/2004	N/A	Squelch GR 22	N/A	Squelch GR 18/04	N/A	Squelch GR 18/04	N/A	Squelch GR 18/04	N/A	Squelch GR 2085	N/A
LDAP Changes																													
9		Multiple users in LDAP filter field, errors will occur.		1	RCVD	Ford, Dell					Malware examined but																		
10		Multiple group search for LDAP filter field.		2	RCVD	Ford					Malware examined but																		
11		DNS Support for LDAP access.		2	RCVD	Ford					Malware examined but																		
12		LDAP/SSH files for x335		1	RCVD	Multiple customers	In Progress					N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13		Added Keys from Group Name		1	RCVD	Ford	Completed	In Progress	232358		Customer Sol	Squelch GR 4085	N/A	N/A	No Build Yet	UPE859A Released in 5.88	No Build Yet	UPE859A Released in 5.88	No Build Yet	Squelch GR 5/04	No Build Yet	Squelch GR 18/04	No Build Yet	Squelch GR 18/04	CEE859A 7/13	Squelch GR 18/04	No Build Yet	Squelch GR 2085	RUE747A Released in 5.85
14		LDAP installation in managing the LDAP software. In there a method that uses an .ini file, that would be able to change the software for the RSA or MM1 software.	7/9/2004	2	RCVD																								
15		Configure LDAP & SSL software through the Embedded CLI	7/9/2004	2	RCVD	AXA, UBS																							
16		Change software. The user id is not included in the LDAP access, but it user name as local machine and the security on the local machine.		2	RCVD	Ford																							
General																													
17		Turning off alerts for those components that were disabled by customer.	7/9/2004	1	RCVD	Multiple customers																							
18		x335 Work around for RSA II & O2T support.	3/1/2004	2	RCVD	o2q, label					Customer is purchase RSA1 OEM equipment No EHS4T support -L customer																		
19		MM1 & RSA II IPMI/Watchdog support		3																									
20		Device Driver for SLES 9 & RHAL 4 for RSA II & RSA II.		2		Kassal Elvadia, All Linux customers																							
21		RSA II to disable Local KVM ports		3																									
22		Display MAC address, on boot time, or IP address of Service Processor during system POST.	1/1/2004	3	RCVD	Multiple customers																							
23		EM64T Device Driver support for SP & BMC		1		Sting																							
24		RSA II RS485 on the x335, test only		2																									
25		MP CLI for Marqan Stanley (private version)	7/9/2004	2	RCVD	Marque Stalder	Completed	In Progress																					
26		Reliability Security Levels for components with the system. [More security levels, to allow security more access to the Drive Controller Software, on rack Drive, Htd, Drives and on Mail: Travel or Governance]	7/9/2004	2	RCVD	o2q, Fidality, Marque Stalder, WoodSpa	Spec written				Joe Balzo	1	Squelch GR 4085	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
27		MM1 full user who are not necessarily has been disconnected. Today full user only access when MM1 fails, and not the network.	5/1/2004	2	RCVD	Fidality						1	2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
28		Newell Helwan E.S Support Corral drivers have synchronization problem		1		Mercur																							
29		Remove BMC Access via IPMI if RSA II Station is installed.		1		All customers					Security violation																		
30		RSA II installation - how difficult to install		1		Lukman																							
31		Vendor driver driver support for the RSA II H adapter - Device ID number - 1.83-238E-000		2	PROG		In Progress				Vendor 1.5x32.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
32		Post Change for Virtual IPMI		2	PROG	All customers	Completed	In Progress																					
33		Config the serial port used for the adapter	3/1/2004	2	PROG	BPVA	Completed	In Progress			Failure value																		
34		Change the WEB Server port for RSA II web interface		3	DENY	SAP	Desired	Desired			No parameters within SAP																		
35		SHBridge Utility for IPMI support		2	All	UBS	Completed	Used in PVT	N/A																				

MM I New Security Roles

- **Management Roles for Chassis**

- User Account Management
- Log Administration
- Chassis Configuration
- Chassis Administration

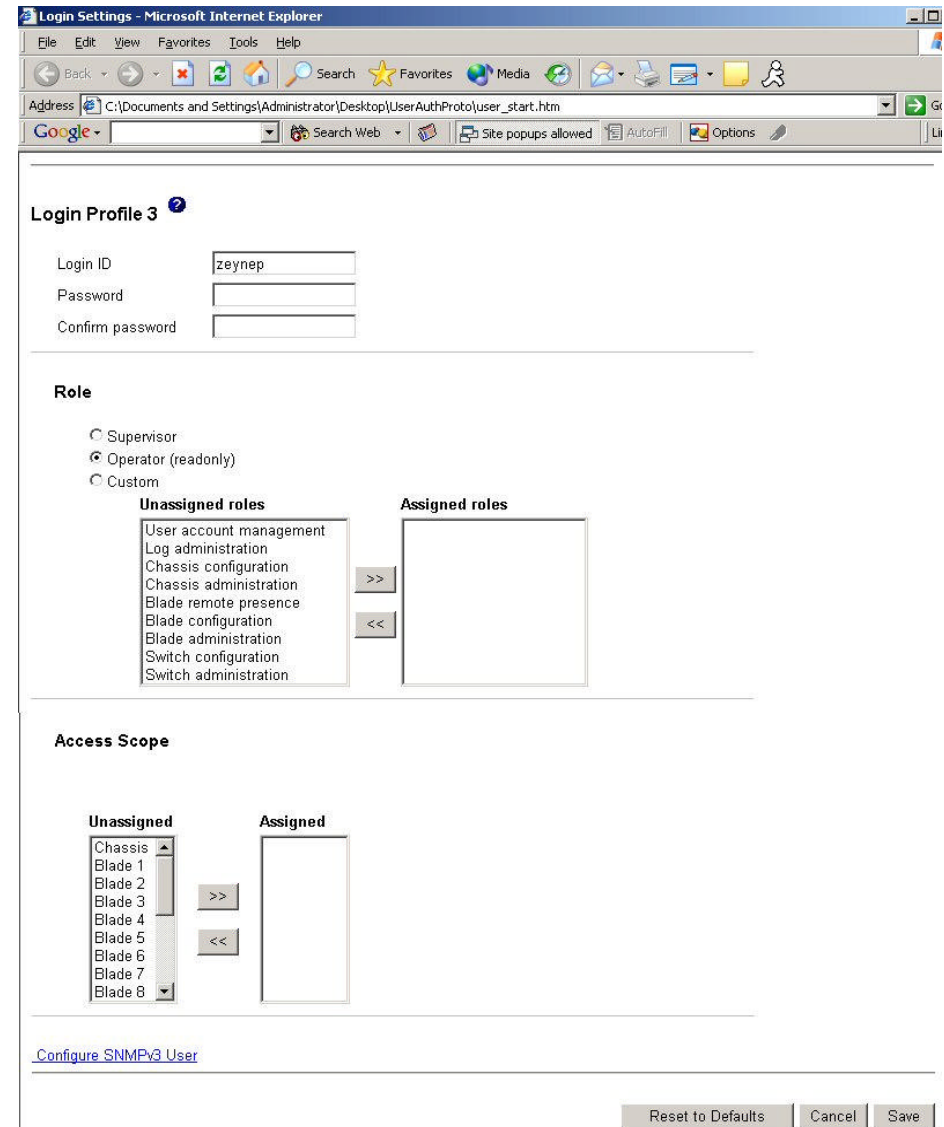
- **Management Roles for Blades**

- Blade Remote Presence
- Blade Configuration
- Blade Administration

- **Management Roles for Switches**

- **Switch Configuration**
- **Switch Administration**

- No ability to create groups
- Security is based up on Resources (Scope) and Management Role
- New MM II Security based on Groups and Higher levels of authentication.



Login Settings - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address C:\Documents and Settings\Administrator\Desktop\UserAuthProto\user_start.htm

Google Search Web Site popups allowed AutoFill Options

Login Profile 3

Login ID

Password

Confirm password

Role

Supervisor

Operator (readonly)

Custom

Unassigned roles

User account management
Log administration
Chassis configuration
Chassis administration
Blade remote presence
Blade configuration
Blade administration
Switch configuration
Switch administration

Assigned roles

Access Scope

Unassigned

Chassis
Blade 1
Blade 2
Blade 3
Blade 4
Blade 5
Blade 6
Blade 7
Blade 8

Assigned

[Configure SNMPv3 User](#)

Reset to Defaults Cancel Save

BladeCenter Management Module 2 HW

- **Proposed MM II hardware features**
 - **Processor** : IBM Power 440GP 400Mhz
 - **Memory** : 256MB standard, with 1 SO dimm port, to install a ECC SO Dimm.
 - **Storage** : 128MB standard, with CF connector (Proposed)
 - Real time clock, with 1 yr battery backup
 - Local USB Mouse & Keyboard
 - Local video and FPGA for legacy Blade video compression.
 - Concurrent KVM supported only on new Blades, those with DVI and FPGA onboard
 - (1) 10/100/1000 External Management Ethernet port
 - USB 2.0 Chip to support USB 1.1(Legacy Blades) and 2.0.
- **Compatibility**
 - MM II Support BC1, BC2, BCE
 - High Availability : Only supports like to like device, ie. MM I with MM I in same chassis.



BladeCenter Management Module 2 SW

- **Proposed MM II software features**

- Embedded OS – industry standard OS
- Multi-Tenant Security support.
- Support CIM Model
- OEM SDK
- All Web UI will have a corresponding CLI.
- Services

- Web Server (HTTP/HTTPS)
- Secure Socket Layer (SSL)
- Telnet for CLI support
- DNS Resolver
- SMTP client
- Secure SSH
 - SFTP server

- Service Location Protocol (SLOP) agent
- Secure LDAP client
- SNMP agent
- TFTP client
- DHCP client
- LDAP/LDAPS client

- **Compatibility**

- MM II Support BC1, BC2, BCE
- High Availability : Only supports like to like device, ie. MM I with MM I in same chassis.

