

SUPERMICR[®]

SuperBlade™ Featuring AMD Blades



User's Manual

Revision 1.0

The information in this User's Manual has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

IN NO EVENT WILL SUPERMICRO BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPERMICRO SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA.. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate for further details.



WARNING: HANDLING OF LEAD SOLDER MATERIALS USED IN THIS PRODUCT MAY EXPOSE YOU TO LEAD, A CHEMICAL KNOWN TO THE STATE OF CALIFORNIA TO CAUSE BIRTH DEFECTS AND OTHER REPRODUCTIVE HARM.

Manual Revision 1.0

Release Date: March 21, 2008

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2008 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About this Manual

This manual is written for professional system integrators, Information Technology professionals and technicians. It provides information for the installation and use of Supermicro's SuperBlade system. Installation and maintenance should be performed by experienced professionals only.

Manual Organization

Chapter 1: Introduction

The first chapter provides a checklist of the main components included with the blade system and describes the main features of the mainboard and enclosure. Also included is a section that describes how to perform common tasks on the system.

Chapter 2: System Safety

You should familiarize yourself with this chapter for a general overview of safety precautions that should be followed when installing and servicing the SuperBlade.

Chapter 3: Setup and Installation

Refer here for details on the installing the SuperBlade system into a rack.

Chapter 4: Blade System Modules

This chapter covers the various modules that install into the blade enclosure.

Chapter 5: Blade Unit

This chapter covers the blade module and its components (such as the mainboard, processors, memory and hard drives).

Chapter 6: Power Supply

This chapter covers the system power supplies and their installation.

Chapter 7: Software and RAID

This chapter covers the operating system installation options and the blade management software packages that are included with the system. Also refer to this chapter for the procedure on setting up a RAID array.

Chapter 8: Web-based Management Utility

This chapter covers the Web-based Management Utility and how to use it.

Chapter 9: BIOS

This chapter covers the system BIOS and how to setup, configure and use it.

Appendix A: BIOS POST Codes and Messages

This appendix contains reference information about BIOS POST Codes and Messages.

Appendix B: HCA Mezzanine Card

This appendix covers the HCA Mezzanine card and its installation.

Appendix C: Gigabit Switch Features

This appendix covers the Gigabit Switch and its features.

Appendix D: System Specifications

This appendix provides a summary of system specifications.

Appendix E: iSCSI Setup Procedure

This appendix provides a setup procedure for the iSCSI system use.

Table of Contents

Chapter 1 Introduction	1-1
1-1 Overview.....	1-1
1-2 Product Checklist	1-1
1-3 Blade Module Features	1-2
Processors	1-2
Memory	1-2
Storage.....	1-3
Density	1-3
1-4 Blade Enclosure Features	1-4
Power.....	1-4
Middle Plane	1-4
LEDs	1-4
Enclosure Cooling.....	1-5
1-5 Power Supply Features.....	1-5
Power Supply Modules	1-5
Power Cord	1-5
Power Supply Failure	1-6
1-6 Special Design Features	1-6
Operating System Support.....	1-6
Computing Density/Power	1-6
High-Efficiency Power Supplies	1-6
1-7 Contacting Supermicro.....	1-7
Chapter 2 System Safety	2-1
2-1 Electrical Safety Precautions.....	2-1
2-2 General Safety Precautions.....	2-2
2-3 Electrostatic Discharge Precautions	2-2
2-4 Operating Precautions.....	2-3
Chapter 3 Setup and Installation	3-1
3-1 Overview.....	3-1
3-2 Unpacking the System	3-1
Choosing a Setup Location.....	3-1
Rack Precautions.....	3-2
Server Precautions	3-2

Rack Mounting Considerations 3-2
 Ambient Operating Temperature 3-2
 Reduced Airflow 3-2
 Mechanical Loading 3-2
 Circuit Overloading 3-3
 Reliable Ground 3-3
Installing the System Into a Rack 3-3
Rack Mounting Hardware 3-3
Installation 3-4

Chapter 4 Blade System Modules 4-1

4-1 Chassis Management Module 4-2
 Module Redundancy 4-3
 Master/Slave Modules 4-3
 Module Installation 4-3
 CMM Functions 4-4
 Local KVM 4-4
 Remote KVM over IP 4-4
 Remote Storage (Virtual Media) 4-4
 Serial Over LAN (SOL) 4-4
 Monitoring Functions 4-5
 CMM Switches and Buttons 4-5
 USB Switch 4-5
 Reset Button 4-6
 Firmware 4-6
4-2 InfiniBand Module 4-7
 Installing/Removing the InfiniBand Module 4-8
 InfiniBand Switch LEDs 4-9
4-3 GbE (Ethernet) Modules 4-10
 GEM-001 GbE Ethernet Switch Module 4-10
 GEM-002 GbE Ethernet Pass-through Module 4-11
 Installing/Removing a GbE Module 4-13
 GbE Module LEDs 4-14
 Configuring the GEM-001 GbE Switch Module 4-15
 Web-based Management Utility/IPMI 4-16
 Network Connection/Login 4-16
 Address Defaults 4-17
 Command Line 4-17
 Firmware 4-17
4-4 Blade Modules 4-18

Powering up a Blade Unit	4-18
Powering down a Blade Unit	4-18
Removing a Blade Unit from the Enclosure	4-18
Removing/Replacing the Blade Cover	4-18
Installing a Blade Unit into the Enclosure	4-18
4-5 Double-Wide Modules	4-20
Chapter 5 Blade Unit	5-1
5-1 Control Panel	5-2
Power Button	5-3
KVM Button	5-3
KVM LED Indicators	5-3
KVM Connector	5-3
5-2 Removing or Replacing the Blade Cover	5-4
5-3 Processor Installation	5-4
5-4 Onboard Battery	5-6
5-5 Memory	5-6
Populating Memory Slots	5-6
DIMM Installation	5-8
5-6 SBA-7141M-T Blade Unit Features	5-10
Mainboard	5-11
Jumpers	5-12
CMOS Clear	5-12
Blade Unit Components	5-13
Memory Support	5-14
Hard Disk Drive	5-14
5-7 SBA-7121M-T1 Blade Unit Features	5-15
Mainboard	5-16
Jumpers	5-17
CMOS Clear	5-17
Blade Unit Components	5-18
Memory Support	5-19
Hard Disk Drive	5-19
Chapter 6 Power Supply	6-1
6-1 Power Supply Modules	6-1
Power Supply Failure	6-3
Installing a Power Supply	6-3
Removing a Power Supply	6-3

- 6-2 Power Supply Fans 6-4
- 6-3 Power Components 6-5
 - Power Cord 6-5
 - Power Cable Tie and Clamp 6-6
- Chapter 7 Software and RAID 7-1**
 - 7-1 Installing the Operating System 7-1
 - Installing with an External USB CD-ROM Drive 7-1
 - Installing via PXE Boot 7-1
 - Installing via Virtual Media (Drive Redirection) 7-2
 - 7-2 Management Software 7-2
 - 7-3 Configuring and Setting up RAID 7-2
- Chapter 8 Web-based Management Utility 8-1**
 - 8-1 Network Connection/Login 8-2
 - Address Defaults 8-2
 - 8-2 Home Page 8-3
 - 8-3 Main Menu Icons 8-4
 - Blade System 8-4
 - Blade Screen 8-5
 - Power Supply 8-6
 - Gigabit Switch 8-7
 - CMM 8-8
 - KVM Console 8-9
 - SOL Console 8-11
 - Virtual Media 8-12
 - Floppy Disk 8-12
 - CD-ROM 8-13
 - Drive Redirection 8-14
 - Options 8-15
 - System Health 8-16
 - System Event Log 8-16
 - Alert Settings 8-17
 - User Management 8-18
 - Change Password 8-18
 - Users & Groups 8-19
 - Permissions 8-21
 - KVM Settings 8-22
 - User Console 8-22
 - Keyboard/Mouse 8-25

Device Settings	8-26
Network	8-26
Dynamic DNS	8-28
Security	8-29
Date/Time	8-31
Event Log	8-32
SNMP Settings	8-34
Maintenance	8-35
Device Information	8-35
Event Log	8-36
Update Firmware	8-37
Unit Reset	8-38
8-4 Remote Console	8-39
Remote Console Options	8-39
Monitor Only	8-40
Exclusive Access	8-40
Readability Filter	8-40
Scaling	8-40
Local Cursor	8-40
Chat Window	8-40
Video Settings	8-41
Soft Keyboard	8-42
Local Keyboard	8-42
Hotkeys	8-43
Remote Console Interface Window	8-43
8-5 Log Out	8-45
Chapter 9 BIOS	9-1
9-1 Introduction	9-1
System BIOS	9-1
How To Change the Configuration Data	9-1
Starting the Setup Utility	9-1
9-2 BIOS Updates	9-2
Flashing BIOS	9-2
9-3 Running Setup	9-3
Appendix A BIOS POST Codes and Messages	A-1
A-1 Uncompressed Initialization Codes	A-1
A-2 Bootblock Recovery Codes	A-1
A-3 Uncompressed Initialization Codes	A-2

A-4 BIOS Error Beep CodesA-7

Appendix B HCA Mezzanine CardsB-1

 B-1 Safety Guidelines.....B-1

 ESD Safety GuidelinesB-1

 General Safety GuidelinesB-1

 B-2 Mezzanine HCA CardsB-2

 B-3 Installation.....B-3

 Installation LocationB-4

 Card InstallationB-4

Appendix C Gigabit Switch Features C-1

 C-1 Port Status C-2

 Port VLAN ID (PVID)..... C-2

 Port Configuration C-3

 C-2 Statistics C-4

 Port Statistics C-4

 C-3 VLAN C-7

 C-4 Configuring a Static VLAN..... C-8

 C-5 Trunking C-9

 C-6 Mirroring..... C-11

 C-7 Quality of Service C-12

 Priority Queues C-12

 C-8 Rate Control C-14

 C-9 L2 Management..... C-15

 C-10 Spanning Tree..... C-17

 Bridge Protocol Data Unit (BPDU) C-17

 Port Transition State..... C-18

 RSTP Port Roles..... C-18

 Root Status..... C-19

 Bridge Setting..... C-19

 RSTP Port Settings..... C-20

 C-11 IEEE 802.1x..... C-21

 Wiring for 802.1x..... C-21

 802.1x Configuration..... C-22

 C-12 IGMP Snooping C-23

 C-13 SNMP C-25

 C-14 UpLink Failure Tracking (ULFT) C-26

Appendix D System Specifications D-1

 D-1 Blade Specifications D-1

 D-2 Enclosure Specifications D-2

 D-3 Environmental Specifications D-2

 D-4 Address Defaults D-3

 D-5 Power Supply Power Calculations D-3

Appendix E iSCSI Setup Procedure E-1

Notes

List of Figures

Figure 1-1. Full Rack of Blade Enclosures and Blade Servers	1-3
Figure 2-1. Installing the Onboard Battery	2-2
Figure 3-1. Positioning the Enclosure Template	3-4
Figure 3-2. Securing the Rails to the Rack	3-4
Figure 3-3. Attaching the Optional Handles	3-5
Figure 3-4. Enclosure Installed into Rack	3-6
Figure 4-1. Typical Blade System Module Configuration: Rear View	4-1
Figure 4-2. Chassis Management Module	4-2
Figure 4-3. USB Switch on Rear of CMM	4-5
Figure 4-4. InfiniBand Module	4-7
Figure 4-5. GEM-001 GbE (Ethernet) Switch Module	4-10
Figure 4-6. GEM-002 GbE (Ethernet) Pass-through Module	4-12
Figure 4-7. Configuring the GbE Switch Module	4-15
Figure 4-8. Configuring the GEM-001 GbE Switch Module	4-16
Figure 4-9. Inserting a Blade into the Enclosure	4-19
Figure 4-10. Locking the Blade into Position	4-20
Figure 4-11. Horizontal Spacers for Single Bays	4-21
Figure 4-12. Modifying for a Double-Wide Module Bay (Steps 1 & 2)	4-22
Figure 4-13. Modifying for a Double-Wide Module Bay (Steps 3 & 4)	4-23
Figure 5-1. Blade Control Panel	5-2
Figure 5-2. Installing a Processor in a Socket	5-5
Figure 5-3. Installing the Onboard Battery	5-6
Figure 5-4. 16-slot DIMM Numbering	5-7
Figure 5-5. 8-slot DIMM Numbering	5-8
Figure 5-6. Installing a DIMM into a Memory Slot	5-9
Figure 5-7. SBA-7141M-T Blade Unit Front View	5-10
Figure 5-8. BHDME Mainboard	5-11
Figure 5-9. NVidia MCP55 Pro Chipset: Block Diagram for SBA-7141M-T	5-12
Figure 5-10. Exploded View of the SBA-7141M-T Blade Unit	5-13
Figure 5-11. SBA-7121M-T1 Blade Unit Front View	5-15
Figure 5-12. BHDME Mainboard	5-16
Figure 5-13. NVidia MCP55 Pro Chipset: Block Diagram for SBA-7121M-T1	5-17
Figure 5-14. Exploded View of the SBA-7121M-T1 Blade Unit	5-18
Figure 5-15. Installing a Hard Drive in a Carrier	5-20
Figure 6-1. PWS-1K41-BR Power Supply	6-1
Figure 6-2. PWS-2K01-BR Power Supply	6-2
Figure 6-3. Power Supply Module	6-4

Figure 6-4. Power Components	6-5
Figure 6-5. Power Cable Tie and Clamp Parts	6-6
Figure 6-6. Power Cable Tie and Clamp Assembly	6-7
Figure 8-1. Home Page.....	8-3
Figure 8-2. Blade Status Screen.....	8-5
Figure 8-3. Power Supply Status Screen	8-6
Figure 8-4. Gibabit Switch Status Screen	8-7
Figure 8-5. CMM Status Screen.....	8-8
Figure 8-6. Remote Console Interface Screen.....	8-9
Figure 8-7. SOL Console Screen	8-11
Figure 8-8. Floppy Disk Status Screen	8-12
Figure 8-9. CD-ROM Image Screen.....	8-13
Figure 8-10. Drive Redirections Screen.....	8-14
Figure 8-11. Options Screen.....	8-15
Figure 8-12. System Event Log Screen	8-16
Figure 8-13. IPMI Alert Configuration Screen	8-17
Figure 8-14. Change Passwords Screen	8-18
Figure 8-15. Users and Groups Screen	8-19
Figure 8-16. Permissions Screen.....	8-21
Figure 8-17. KVM Settings Screen.....	8-23
Figure 8-18. Keyboard/Mouse Screen	8-25
Figure 8-19. Network Screen	8-26
Figure 8-20. Dynamic DNS Settings Screen.....	8-28
Figure 8-21. Security Screen	8-29
Figure 8-22. Date/Time Screen.....	8-31
Figure 8-23. Device Settings Event Log Screen	8-32
Figure 8-24. SNMP Settings Screen	8-34
Figure 8-25. Device Information Screen	8-35
Figure 8-26. Maintenance Event Log List Screen	8-36
Figure 8-27. Update Firmware Screen.....	8-37
Figure 8-28. Unit Reset Screen.....	8-38
Figure 8-29. Remote Console Options.....	8-39
Figure 8-30. Chat Window	8-41
Figure 8-31. Video Settings.....	8-41
Figure 8-32. Keys in English Soft Keyboard	8-42
Figure 8-33. Soft Keyboard Language Selection	8-42
Figure 8-34. Hotkeys.....	8-43
Figure 8-35. Console Icon.....	8-44
Figure 8-36. Remote Console Interface Window	8-44
Figure B-1. AOC-IBH-001 Mezzanine HCA Card	B-2

Figure B-2. AOC-IBH-002 Mezzanine HCA Card	B-2
Figure B-3. Installation Location.....	B-3
Figure B-4. Card Installation	B-4
Figure B-5. Installation Complete.....	B-5
Figure C-1. Port Status Screen.....	C-2
Figure C-2. Port Configuration Screen.....	C-3
Figure C-3. Statistics Screen	C-4
Figure C-4. Port Statistics Screen.....	C-5
Figure C-5. VLAN Screen	C-7
Figure C-6. Creating a New VLAN.....	C-8
Figure C-7. New VLAN Screen	C-9
Figure C-8. Trunking Screen.....	C-10
Figure C-9. Port Mirroring Screen.....	C-11
Figure C-10. QoS Setting Screen	C-13
Figure C-11. Rate Limit and Storm Control Screen	C-14
Figure C-12. Storm Control Screen.....	C-15
Figure C-13. L2 Management Screen.....	C-16
Figure C-14. L2 Management: Current Entries Screen.....	C-16
Figure C-15. Rapid Spanning Tree Port Settings.....	C-20
Figure C-16. 802.1x Configuration Screen.....	C-22
Figure C-17. IGMP Snooping Screen	C-24
Figure C-18. Uplink Failure Tracking Configuration Screen.....	C-27
Figure E-1. Microsoft MPIO Multipathing Support for iSCSI Check Box.....	E-2
Figure E-2. Configure iSCSI Network Boot Support Check Box.....	E-3

Notes

List of Tables

Table 1-1. Summary of Blade Module Features	1-2
Table 1-2. Blade Enclosure: LED Descriptions	1-5
Table 4-1. Blade System: Module View	4-1
Table 4-2. CMM Module Interface.....	4-2
Table 4-3. CMM Module Features	4-3
Table 4-4. CMM Reset Settings.....	4-6
Table 4-5. InfiniBand Module Interface	4-7
Table 4-6. InfiniBand Module Features.....	4-8
Table 4-7. InfiniBand Switch LEDs.....	4-9
Table 4-8. GEM-001 GbE Switch Module Interface.....	4-10
Table 4-9. GEM-001 GbE Switch Module Features.....	4-11
Table 4-10. GEM-002 GbE Pass-through Module Interface	4-12
Table 4-11. GEM-002 GbE Pass-through Module Features	4-12
Table 4-12. GbE Switch LEDs	4-14
Table 4-13. GEM-001 GbE Switch Module Address Default Settings	4-17
Table 5-1. SuperBlade Blade Units.....	5-1
Table 5-2. Blade Control Panel.....	5-2
Table 5-3. KVM LED Indicators.....	5-3
Table 5-4. Populating Memory Slots for Interleaved Operation	5-7
Table 5-5. SBA-7141M-T Blade Unit Features	5-10
Table 5-6. BHQME Mainboard Layout.....	5-12
Table 5-7. Main Components of SBA-7141M-T Blade Unit	5-14
Table 5-8. SBA-7121M-T1 Blade Unit Features	5-15
Table 5-9. BHQME Mainboard Layout.....	5-17
Table 5-10. Main Components of SBA-7121M-T1 Blade Unit	5-19
Table 6-1. PWS-1K41-BR Power Supply Features.....	6-1
Table 6-2. PWS-2K01-BR Power Supply Features.....	6-2
Table 6-3. Power Components	6-5
Table 8-1. Address Defaults.....	8-2
Table 8-2. Home Page Controls.....	8-3
Table 8-3. Main Menu Icons.....	8-4
Table 8-4. Blade Status Screen Controls.....	8-5
Table 8-5. Power Supply Status Screen Controls.....	8-6
Table 8-6. Gigabit Switch Status Screen Controls	8-7
Table 8-7. CMM Status Screen Controls	8-8
Table 8-8. Remote Console Interface Screen Controls	8-10
Table 8-9. Floppy Disk Status Screen Controls	8-12

Table 8-10. CD-ROM Image Screen Controls	8-13
Table 8-11. Drive Redirection Screen Controls.....	8-14
Table 8-12. Options Screen Controls.....	8-15
Table 8-13. System Event Log Screen Controls.....	8-16
Table 8-14. Change Password Screen Controls.....	8-18
Table 8-15. Users and Groups Screen Controls	8-19
Table 8-16. Permissions Screen Controls.....	8-21
Table 8-17. KVM Settings Screen Controls	8-23
Table 8-18. Keyboard/Mouse Screen Controls.....	8-25
Table 8-19. Network Screen Controls.....	8-27
Table 8-20. Dynamic DNS Settings Screen Controls.....	8-28
Table 8-21. Security Screen Controls	8-29
Table 8-22. Date/Time Screen Controls.....	8-31
Table 8-23. Device Settings Event Log Screen Controls	8-32
Table 8-24. SNMP Settings Screen Controls.....	8-34
Table 8-25. Device Information Screen Controls	8-35
Table 8-26. Update Firmware Screen Controls.....	8-37
Table 8-27. Unit Reset Screen Controls	8-38
Table 8-28. Items in the Chat Window	8-41
Table 8-29. Remote Console Interface Window	8-45
Table A-1. Uncompressed Initialization Codes	A-1
Table A-2. Bootblock Recovery Codes	A-1
Table A-3. Uncompressed Initialization Codes	A-2
Table A-4. AMIBIOS Error Beep Codes.....	A-7
Table C-1. Gigabit Switch Features and Functions.....	C-1
Table C-2. Port Configuration Screen Controls.....	C-3
Table C-3. Port Statistics Screen Controls.....	C-5
Table C-4. Port Mirroring Screen Controls.....	C-11
Table C-5. QoS Setting Screen Controls	C-13
Table C-6. Storm Control Screen Controls	C-15
Table C-7. Comparison of Port States	C-18
Table C-8. IGMP Snooping Screen Controls	C-25
Table C-9. Uplink Failure Tracking Configuration Screen Controls	C-27
Table D-1. SBA-7141M-T Blade Specification Features.....	D-1
Table D-2. SBA-7121M-T1 Blade Specification Features.....	D-1
Table D-3. Enclosure Specification Features.....	D-2
Table D-4. Environmental Specification Features.....	D-2
Table D-5. Address Default Features.....	D-3
Table D-6. Power Supply: Power Calculations (PWS-2K01-BR)	D-3
Table D-7. Power Supply: Power Calculations (PWS-1K41-BR)	D-4

Notes

Chapter 1

Introduction

1-1 Overview

The SuperBlade is a compact self-contained server that connects to a pre-cabled enclosure which provides power, cooling, management and networking functions. One enclosure can hold up to either ten or fourteen blade units, depending upon the blade enclosure used.

In this manual, "blade system" refers to the entire system (including the enclosure and blades units), "blade" or "blade unit" refers to a single blade module and "blade enclosure" is the unit that the blades, power supplies and modules are housed in.

Each Blade unit is optimized to fit into either a specific ten blade or fourteen blade enclosure.

Please refer to our web site for information on operating systems that have been certified for use with the SuperBlade (www.supermicro.com/products/superblade/).

1-2 Product Checklist

- Blade Enclosure (x1): SBE-710E (10-blade) or SBE-714D (14-blade) Series
- Blade Unit (x1 or more): SBA-7141M-T or SBA-7121M-T1
- Power Supplies (x2 or x4): PWS-1K41-BR, PWS-2K01-BR or PWS-2K51-BR
- CMM Module (x1): SBM-CMM-001
- KVM Cable (x1): CBL-0204L
- Dummy Blade Units (x8): MCP-650-00004-0N
- Dummy Power Supplies (x2): MCP-650-00001-0N
- Dummy CMM Modules (x3): MCP-650-00002-0N
- Dummy GbE Switches (x2): MCP-650-00003-0N

Optional components include:

- InfiniBand® Switch (x1): SBM-IBS-001
- Mezzanine Cards (with Infiniband Switch): AOC-IBH-001 or AOC-IBH-002
- GbE Switches (x1 or x2): SBM-GEM-001
- GbE Pass Through Modules (x1 or x2): SBM-GEM-002
- Extra CMM Module for redundancy (x1): (SBM-CMM-01)

Additional modules will periodically become available. Please refer to <http://www.supermicro.com/products/superblade> for the most current list of modules available for the SuperBlade.

Blade systems install into standard racks. Up to six 7U blade systems may be installed into a 19" industry standard 42U rack.

1-3 Blade Module Features

Table 1-1 lists the main features of a Supermicro blade module. See the preceding section for components typically included in a blade system and other optional components. Specific details on each of the AMD SuperBlades is found in Chapter 5.

Table 1-1. Summary of Blade Module Features

Processors
AMD® Opteron™ 2000 or 8300/8200 series processors, depending upon blade server model
Memory
Eight or sixteen 240-pin DIMM sockets that can support up to 64 GB of ECC FBD (Fully Buffered DIMM) DDR2-667 or DDR2-533 SDRAM, depending upon blade server model
Storage
Configurations include either One/two 3.5-inch SATA (Serial ATA) or one internal 2.5-inch SATA (Serial ATA) hard disk drives, depending upon blade server model
Blades per Enclosure
A maximum of either 10 or 14 blade modules into a single blade enclosure, depending on enclosure model
Blades per Rack
A standard rack may accommodate up to 60 or 84 blade modules in a 42U rack, depending upon blade enclosure model used

Processors

Each AMD blade module supports either single, dual or quad AMD Opteron 2000 or 8300/8200 series processors.

Refer to the Supermicro web site for a complete listing of supported processors (<http://www.supermicro.com/products/superblade>). Please note that you will need to check the detailed specifications of a particular blade module for a list of the CPUs it supports.

Memory

Each blade module has eight or sixteen 240-pin DIMM sockets that can support up anywhere from 32 to 128 GB of ECC FBD (Fully Buffered DIMM) DDR2-667 or DDR2-533 SDRAM, depending upon the chip set of the Blade Server model. Memory is interleaved, which requires modules of the same size and speed to be installed in pairs.

Please refer to the Supermicro web site for a list of supported memory (www.supermicro.com/products/superblade). The detailed specifications for a blade module will contain a link to a list of recommended memory sizes and manufacturers.

Storage

A blade module can support either 2.5-inch or 3.5-inch SATA (Serial ATA) hard disk drives in combinations of a single drive (for 2.5-inch), or one or two (for 3.5-inch) drives on each Blader Server.

Density

A maximum of 10 or 14 blade modules may be installed into a single blade enclosure, depending upon the model of enclosure you are using. Each blade enclosure is a 7U form factor, so a standard 42U rack may accommodate up to 6 enclosures with between 60-84 blade modules, or the equivalent of up to 84 1U servers. With the inclusion of 6 CMM modules, 6 Gigabit Ethernet switches and 6 InfiniBand switches, this would occupy up 72U space in a conventional 1U server configuration.

Figure 1-1 displays a view of a full rack with six blade enclosures in it, each with ten blades to an enclosure.

Figure 1-1. Full Rack of Blade Enclosures and Blade Servers



1-4 Blade Enclosure Features

Supermicro's SBE-710E blade enclosure is designed to house up to 10 blade units, while the SBE-714D blade enclosure houses up to 14 blade units. Both accommodate either two or four power supplies. The enclosure backplane allows the blade units to share certain functions such as power, cooling and networking.

The following is a general outline of the main features for both blade server enclosures.

Power

The typical blade enclosure features a 2000W power system composed of two active power supply modules. An alternate configuration (and required for a full 10 or 14-blade system) features a total of four power supply modules for three active and one backup. This power redundancy feature allows you to replace a failed power module while the backup module takes over to keep the system running. You must have either two or four power supply modules installed in the blade enclosure (four is recommended in a full system).

Logic on a blade motherboard calculates the amount of power it will require based on the number of processors and memory installed. If the power supplies cannot supply enough power for any blade unit, that unit will not power up.

Middle Plane

The middle plane integrates the various functions of the blades, the Gigabit (GbE) switch(es), the Chassis Management Module (CMM) and the InfiniBand switch. These devices all connect to the middle plane through high density connectors that provide both signals and power. This type of configuration reduces the amount of system cabling and simplifies the task of setting up the system. To increase system reliability, the middle plane contains no active components.

LEDs

Two LEDs are located at the right top of the enclosure above blade bay #10. The left LED provides Power Status information and the right LED is the Fault LED, as described in [Table 1-2](#).

For overheat problems, check that there are no obstructions (such as poorly routed cables), check that all fans are operating normally and make sure the ambient room temperature is not too warm (refer to [Section D-3: Environmental Specifications on page D-2](#) for the maximum operating temperature). You can also use either of the blade management software utilities to increase the fan speed and maximize system cooling.

In the event of a power overload, you will have to add additional power supply modules to take up the load. Otherwise, you will not be able to power up all the blade modules. (EEPROMs on each blade motherboard calculate the load to determine if the power supplies can adequately handle the total system configuration.)

Enclosure Cooling

The cooling for the entire blade system is provided by the fans in the power supply modules. The 2000W power supply modules have four fans per module. If a power supply fails, its fans will continue to operate to provide continuous cooling. For this reason, a failed power supply should remain installed in the enclosure until a replacement unit is ready.

Table 1-2. Blade Enclosure: LED Descriptions

LED	State	Indication
Power Status LED (left LED)	NA (off)	Standby state
	Green	Power On
	Green (flashing)	Power Overload
	Red	Power supply failure
Fault LED (right LED)	Yellow	Over temperature state in switch module (GbE, IB)
	Flashing Yellow	Fan failure
	Off	Normal

1-5 Power Supply Features

The SuperBlade enclosure comes standard with one CMM module and either two or four power supplies. Information on the power supplies is summarized below. See [Section 4-1: Chassis Management Module on page 4-2](#) for details on the CMM module and [Chapter 6](#) for details on the power supplies.

If you install only two power supplies in the enclosure, they should be installed in the lower rather than the upper power bays. The reason for this counter-intuitive installation is that the power supplies in the lower bays provide increased airflow across the memory modules within each blade module.

Power Supply Modules

Each power supply module has its own power cord. Four modules are required when the full complement of blade units are installed into an enclosure. An LED on the back of a power supply will be red when AC power is present and green when the power is on.

Supermicro's high-efficiency blade system power supplies deliver continuous redundant power at 90%+ peak efficiency. Each power supply module includes a management module that monitors the power supplies and the power enclosure.

Power Cord

Each power supply module has a C-20 type socket (IEC-60320-C20) for AC power and the power cord must have a C-19 type connector (IEC-60320-C19) to connect to the power supply. A plastic locking clip partially covering the socket was designed to prevent

the power supply module from being removed with the power cord still connected. Refer to [Appendix D](#) for power/amperage calculation tables.

Power Supply Failure

If a power supply or a fan in a power supply fails, the system management software will notify you of the situation. In either case, you will need to replace the power supply module with another identical one. Please note that if a power supply fails, its fans will continue to operate to provide system cooling. For this reason, a failed power supply should remain installed in the enclosure until a replacement unit is ready.

See [Chapter 6](#) for the procedure on replacing power supplies.

1-6 Special Design Features

Supermicro's SuperBlades offer special design features, some of which no other blade server can duplicate. These features give you extraordinary flexibility in configuring a blade system for your own particular needs.

Operating System Support

Both Microsoft Windows and Linux operating systems are supported by SuperBlades. Furthermore, you may have different operating systems running on different blade units within the same blade enclosure.

Computing Density/Power

Each SuperBlade mainboard supports two or four quad-core processors and 32 to 64 GB of main memory. This translates to a maximum potential of 224 processors (cores) and 896 GB of memory per 14-blade enclosure or 1344 processors (cores) and 5.376 TB of memory for a full rack.

High-Efficiency Power Supplies

A reliable source of power is critical in server systems and even more so in a blade system, where up to ten systems (blades) share the same power source. SuperBlade power supplies have been designed to operate at a 90%+ peak efficiency and provide redundancy with a backup unit that activates automatically when any other power supply fails. Using high-efficiency power supplies results in a measurable reduction in energy consumption and generated heat.

1-7 Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)

Web Site: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)

Asia-Pacific

Address: Super Micro Computer, Inc.
4F, No. 232-1, Liancheng Rd.
Chung-Ho 235, Taipei County
Taiwan, R.O.C.

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3991

Web Site: www.supermicro.com.tw

Technical Support:

Email: support@supermicro.com.tw

Tel: +886-2-8228-1366, ext. 132 or 139

Notes

Chapter 2

System Safety

2-1 Electrical Safety Precautions

Basic electrical safety precautions should be followed to protect yourself from harm and the SuperBlade from damage:

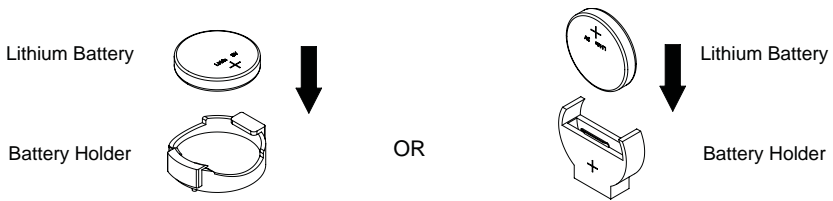
- Be aware of how to power on/off the enclosure power supplies and the individual blades as well as the room's emergency power-off switch, disconnection switch or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the system.
- Do not work alone when working with high voltage components.
- Power should always be disconnected from the blade module when removing or installing such system components as the mainboard, memory modules and processors.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power if necessary.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- The power supply power cords must include a grounding plug and must be plugged into grounded electrical outlets. Power input requires 200-240 VAC only. See the "Power Supply Modules" section in [Chapter 6](#) for details.
- Mainboard Battery: This battery must be replaced only with the same or an equivalent type recommended by the manufacturer (CR2032 Lithium 3V battery). Dispose of used batteries according to the manufacturer's instructions.



WARNING: There is a danger of explosion if the onboard battery is installed upside down, which will reverse its polarities (see [Figure 2-1](#)).

- Mainboard replaceable soldered-in fuses: Self-resetting PTC (Positive Temperature Coefficient) fuses on the mainboard must be replaced by trained service technicians only. The new fuse must be the same or equivalent as the one replaced. Contact technical support for details and support.

Figure 2-1. Installing the Onboard Battery



2-2 General Safety Precautions

Follow these rules to ensure general safety:

- Keep the area around the SuperBlade clean and free of clutter.
- Place the blade module cover and any system components that have been removed away from the system or on a table so that they won't accidentally be stepped on.
- While working on the system, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.
- After accessing the inside of the system, replace the blade module's cover before installing it back into the blade enclosure.

2-3 Electrostatic Discharge Precautions

Electrostatic discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards.

The following measures are generally sufficient to neutralize this difference **before** contact is made to protect your equipment from ESD:

- Use a grounded wrist strap designed to prevent static discharge.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Do not let components or PCBs come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only; do not touch its components, peripheral chips, memory modules or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the mainboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure the blade enclosure provides excellent conductivity between the power supplies, the blade modules and the mainboard.

2-4 Operating Precautions

Care must be taken to assure that the cover of the blade unit is in place when the blade is operating to assure proper cooling. Out of warranty damage to the blade can occur if this practice is not strictly followed.

Any drive carrier without a hard drive installed must remain fully installed in the drive bay when the blade module is operating to ensure proper airflow.

Notes

Chapter 3

Setup and Installation

3-1 Overview

This chapter provides a quick setup procedure for your SuperBlade. Following these steps in the order given should enable you to have the system operational within a minimum amount of time. This quick setup assumes that the processor(s) and memory have already been installed. If not, please turn to [Chapter 4](#) for details on installing specific components

3-2 Unpacking the System

You should inspect the box the SuperBlade was shipped in and note if it was damaged in any way. If the server itself shows damage you should file a damage claim with the carrier who delivered it.

Decide on a suitable location for the rack unit that will hold the SuperBlade. It should be situated in a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise and electromagnetic fields are generated. You will also need it placed near a grounded power outlet. Read the "[Rack Precautions](#)" and "[Server Precautions](#)" in the next section.

The box the SuperBlade was shipped in should include two sets of rail assemblies, two handles and the mounting screws you will need to install the system into the rack. Follow the steps in the order given to complete the installation process in a minimum amount of time. **Please read this section in its entirety before you begin the installation procedure outlined in the sections that follow.**

Choosing a Setup Location

The following are important considerations for choosing a setup location:

- Leave enough clearance in front of the rack to enable you to remove the blade units (~25 inches).
- Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.
- This product is for installation only in a *Restricted Access Location* (dedicated equipment rooms, service closets and the like).
- This product is not suitable for use with visual display work place devices according to §2 of the the *German Ordinance for Work with Visual Display Units*.



WARNING: Please read the following Important Warnings and Precautions!

Rack Precautions

The following are important precautions concerning rack setup:

- The enclosure unit is heavy and requires at least two people to lift it.
- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In single rack installation, stabilizers should be attached to the rack.
- In multiple rack installations, the racks should be coupled together.

Server Precautions

The following are important precautions concerning server setup:

- Review the electrical and general safety precautions in [Chapter 2](#).
- Determine the placement of each component in the rack *before* you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep your system operating in case of a power failure.
- Allow the hot plug hard drives and power supply units to cool before touching them.
- Always keep the rack's front door and all panels and components on the servers closed when not servicing to maintain proper cooling.

Rack Mounting Considerations

Below are listed important considerations for rack mounting.

Ambient Operating Temperature

If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature. Refer to Appendix E for operating temperature specifications.

Reduced Airflow

Equipment should be mounted into a rack so that the amount of airflow required for safe operation is not compromised.

Mechanical Loading

Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Circuit Overloading

Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern. See the power calculation tables in [Appendix D](#).

Reliable Ground

A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (such as the use of power strips and so on).



NOTE: It is recommended that you seek the advice and assistance of a licensed electrician that can advise you on best practices for insuring that the electrical supply and the rack are joined to a *Common Bonding Network*.

Professional documents on grounding techniques include:

- *ANSI/TIA-942 – Telecommunications Infrastructure Standard for Data Centers*
- *J-STD-607-A-2002 – Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications*
- *IEEE Std 1100™-2005 (IEEE Emerald Book) – IEEE Recommended Practice for Powering and Grounding Electronic Equipment*

Installing the System Into a Rack

This section provides information on installing the SuperBlade into a rack. There are a variety of rack units on the market, meaning the procedure may differ slightly. Refer to the Enclosure Template that was included with the system for help.

Rack Mounting Hardware

The following is a list of rack mounting hardware you will need for rack setup and installation:

- Two rail assemblies (one for each side of the enclosure)
- Two handles
- Four roundhead screws for fastening the server ears to the rack
- Eight flathead screws and washers for mounting the rails to the rack

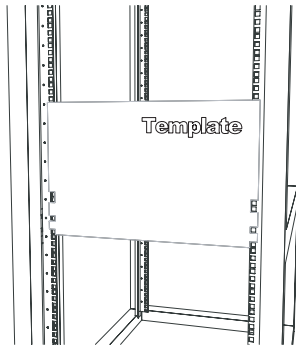
Installation

Use the procedure below for installing an enclosure in a rack.

Installing an enclosure:

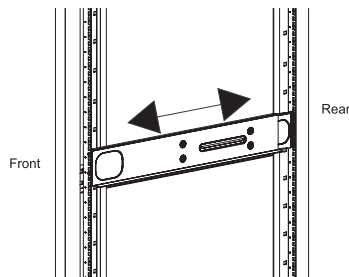
1. Decide where you want to place the blade enclosure into the rack (see ["Rack Mounting Considerations"](#) in the previous section).
2. Position the Enclosure Template at the front of the enclosure to determine the locations of the screws for the enclosure rails (see [Figure 3-1](#)).

Figure 3-1. Positioning the Enclosure Template



3. The two enclosure rail sections are screwed together to keep them immobile during shipping. Release these screws just enough to allow the rails to slide apart. Note the arrow on the rail, which indicates the end that attaches to the front of the rack.
4. Slide the rails apart far enough to match the depth of the rack. Position the rails with the template and secure the front of each to the front of the rack with two flathead screws, then secure the back of each rail to the rear of the rack with two flathead screws (see [Figure 3-2](#)). Note that the rails are left/right specific and very heavy.

Figure 3-2. Securing the Rails to the Rack



5. (Optional step) Add the front left and right handles to the enclosure using five screws to secure each handle. Install a thumbscrew through the bottom hole of each handle (see [Figure 3-3](#)).



NOTE: These handles are optional and need only be installed when mounting the system into a short rack. When mounting into a deep rack, they are unnecessary and regular screws should be used instead of thumbscrews.

Be aware that these handles are not to be used for lifting the system, they are only to be used to slide the system within the rack.

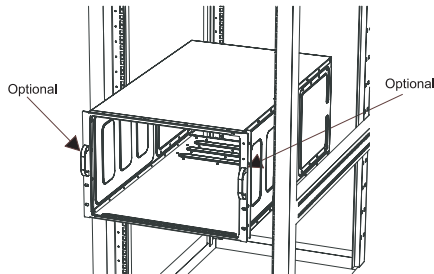
6. With one person on either side (see the descriptive label on the side of the enclosure), lift the enclosure and slide it into the installed rails.



WARNING: Be sure that the enclosure is empty of all blades, power supplies, switches and management modules **BEFORE** lifting. These should be installed **AFTER** the enclosure is mounted in the rack. Injury and damage may occur if components are not removed from the rack prior to installation.

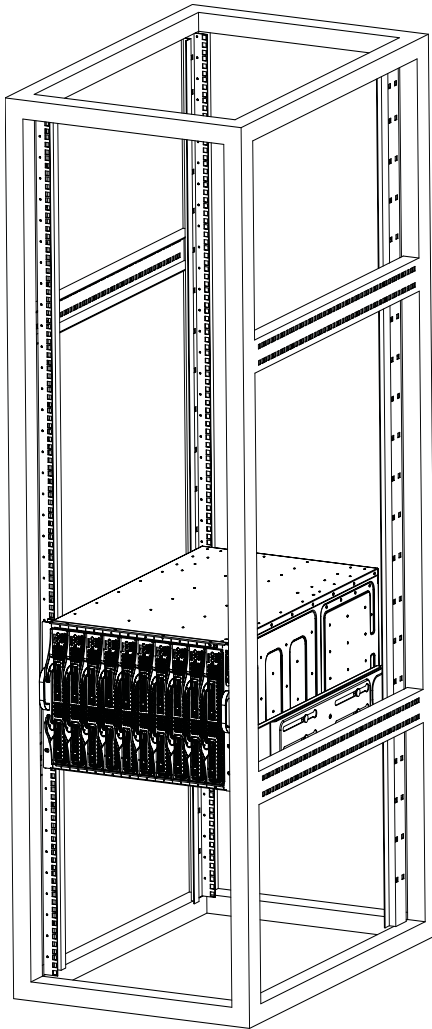
7. After pushing the enclosure all the way into the rack, use two roundhead screws on each side of the server to lock it into place.

Figure 3-3. Attaching the Optional Handles



8. The enclosure is now securely installed in the rack (see [Figure 3-4](#)).

Figure 3-4. Enclosure Installed into Rack



Chapter 4

Blade System Modules

In addition to the blade units, your blade system comes equipped with one or more system modules. The modules fit into the rear of the enclosure into bays above and/or below the power supplies. This chapter describes the various blade modules that may be part of your blade system. Module configurations can be customized; you can install two of the same type module for redundancy purposes or you may omit a module altogether (except for the CMM, which is a required module). [Figure 4-1](#) shows a typical module configuration in a blade system. See [Chapter 6](#) for information on power supply modules.



WARNING: All module bays must be populated either with a module or a dummy module cover to maintain proper airflow.

Figure 4-1. Typical Blade System Module Configuration: Rear View

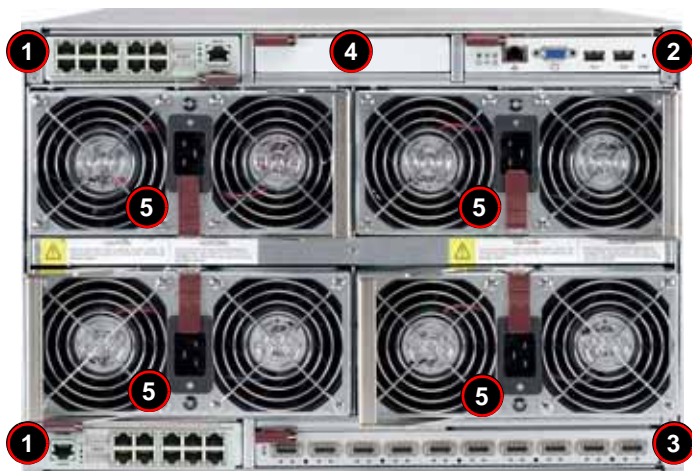


Table 4-1. Blade System: Module View

Item#	Description
1	GbE (Gigabit Ethernet) Switch (Optional)
2	CMM (Chassis Management Module) (x1 standard, x2 optional)
3	InfiniBand Switch (optional)
4	Empty bay with dummy cover (always empty except with InfiniBand switch installed)
5	Power Supply (x2 standard, x4 optional)

4-1 Chassis Management Module

The Chassis Management Module (CMM) (Figure 4-2) is a required module in a blade system. This “command” module communicates with the blade units, the power supplies and the blade switches. Used in conjunction with the Web Interface or IPMI View management software, the CMM provides administrator control over individual blade units, power supplies, cooling fans and networking switches and monitors onboard temperatures, power status, voltage levels and fan speeds.

The CMM provides a dedicated, local and remote KVM (keyboard/video/mouse) connection over an out of band TCP/IP Ethernet network during any server state (functioning, blue-screen, powered down, BIOS and so on). It also supports Virtual Media (VM) redirection for CD, floppy and USB mass storage devices and configures such information as the switch IP addresses. A summary of CMM features is shown in Table 4-3.

Figure 4-2. Chassis Management Module

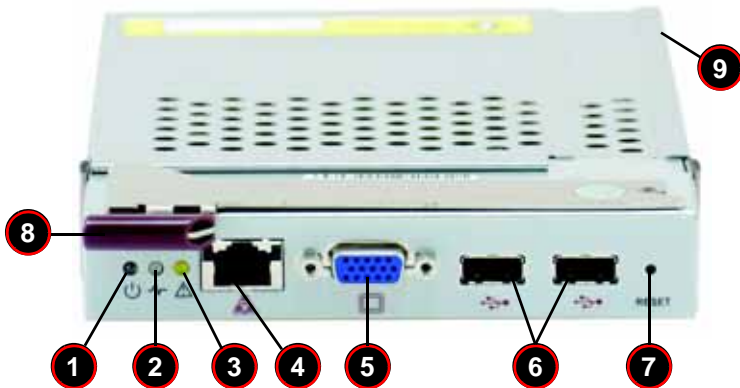


Table 4-2. CMM Module Interface

Item#	Description
1	Power LED
2	Activity LED
3	Fault LED
4	Ethernet Port
5	VGA (Monitor) Port
6	USB Ports
7	Reset Button
8	Module Release Handle
9	USB 2.0/1.1 Switch (accessed at back of module, see Figure 4-3)

Table 4-3. CMM Module Features

Feature	Description
Chipset	Raritan Kira 100
Management Capabilities	Can manage 10 to 14 blade units, two GbE switches, one InfiniBand switch and 4 power supplies
Ports	One Ethernet port, one VGA port and two USB ports
Basic Functions Supported	Local KVM, remote KVM, remote storage, Serial-over-LAN (SOL), blade monitoring and control
System Management	System management interface provided via dedicated LAN
Power Consumption	Approx. 20W
Operating System	Firmware (upgradeable)

Module Redundancy

A blade system must have one CMM and may have two for redundancy (if an InfiniBand module is installed in the enclosure, there will only be room for a single CMM). Since the CMM uses its own processor, all monitoring and control functions are carried out regardless of the operation or power status of the blade units. CMM modules can only be installed in the upper and/or lower right module bays.

The redundancy feature is automatic when two CMM modules have been installed into a blade system.

Master/Slave Modules

When a blade system has two CMM modules, they are assigned a master/slave status. This is done automatically according to the following criteria:

Determining Master/Slave status:

1. The CMM installed in the upper bay will be the master, however...
2. If the master CMM is powered down or removed, the second (slave) CMM module will then immediately be assigned as the master.

Module Installation

Make sure the cover to the module has been installed before proceeding. Follow the anti-static precautions described in [Chapter 2](#).

Installing the Module:

1. Remove the dummy cover from the bay you want to place the module in.
2. Place the module's release handle in the open position.
3. Slide the module into the module bay until it stops.
4. Push the release handle to the closed position.

5. After the module has been installed and the handle locked, it will turn on and a POST test will run to verify it is working properly.

Removing the Module:

1. Pull out the release handle to the open position.
2. Pull the module out of the bay.
3. Replace immediately with another module or with a dummy module cover to maintain airflow integrity.

CMM Functions

The following functions are provided by the CMM module.

Local KVM

KVM stands for Keyboard/Video/Mouse. With KVM, a user can control multiple blades with a single keyboard/video/mouse setup. KVM supports the following video resolutions: 1280 X 1024 @ 60 Hz maximum, 1024 X 768 @ 85 Hz maximum, 800 X 600 @ 85 Hz maximum and 640 X 480 @ 85 Hz maximum.

To Use: Connect your keyboard, mouse and monitor to the USB and VGA connectors on the CMM module, then push the KVM button on the control panel of the blade module you wish to access. The KVM LED on the blade will then illuminate and you can interface directly with that blade. To access a different blade module, simply push the KVM button on that blade's control panel.

Remote KVM over IP

Remote KVM over IP is independent from local KVM (although local KVM can operate in parallel with Remote KVM). Remote KVM encrypts all communication between the remote user and the CMM.

To Use: Remote KVM over IP is initiated with the management software (IPMI View or Web-based utility). Attach the LAN cable to the LAN port on the CMM module then refer to [Chapter 7](#) to login and use either utility.

Remote Storage (Virtual Media)

The Remote Storage function allows the user to connect to a remote storage device (such as a floppy, hard disk, CD-ROM or USB storage device) and access the device as if it were local. This can be used not only to read and write to remote storage devices but to load an operating system from a remote drive.

Serial Over LAN (SOL)

Serial Over LAN allows you to redirect the input and output of a serial port via IPMI in order to manage blade modules from a remote location.

To Use: Serial Over LAN can be activated via the Web-based Management utility. See [Chapter 8](#) for the procedure to initiate SOL.

Monitoring Functions

Used in conjunction with IPMI or the Web-based Management utility, the CMM module can monitor and provide information on the hardware health of the blade modules and the system as a whole. In addition to the monitoring functions, you can remotely power on, power off or reboot a system.

Health information includes:

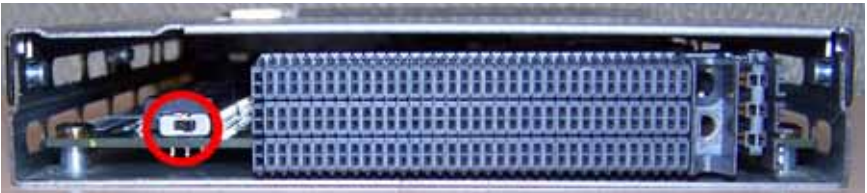
- temperature levels
- fan speeds
- voltage levels
- power status

CMM Switches and Buttons

The various switches and buttons found on the CMM are described below.

USB Switch

Figure 4-3. USB Switch on Rear of CMM



The USB ports on the CMM can function in either 2.0 or 1.1 mode (the default is 1.1). A switch located on the PCB at the back of the CMM module is used to change the USB mode (see [Figure 4-3](#)).

To access the switch, you need to remove the CMM from the enclosure. Pull the CMM out and locate the switch near the large gray connector. The settings are silkscreened on the PCB. After setting the switch, insert the CMM module back into its bay.

Reset Button

The Reset button located on the front of the CMM module is used to reset the following software settings to their defaults:

Table 4-4. CMM Reset Settings

Software Setting	Default
User Name and Password	Reset to ADMIN and ADMIN (case sensitive)
IP Address	Reset to 192.168.100.100
Gateway Address	Reset to 0.0.0.0
Subnet Mask	Reset to 255.255.255.0

To reset these values, press and hold the Reset button for five seconds.

Firmware

The firmware for the CMM switch resides in the SIMCM card in the module. This firmware can be updated with the web-based management utility.

Within the utility, go to the MAINTENANCE > UPDATE FIRMWARE screen. Here you can enter the name of the firmware you want to update or click on BROWSE to select the firmware file. Finish by clicking the UPLOAD button.

4-2 InfiniBand Module



NOTE: This process is not reversible once the firmware is updated, so proceed with caution. It might take a few minutes to complete this procedure. See ["Update Firmware" on page 8-37](#) for further details.

The InfiniBand module is a switch-based, point-to-point bi-directional serial link architecture. The main function of the InfiniBand switch module is to provide high-speed interconnectivity among the blade modules and external peripherals. This is a hot-pluggable module that must be installed in a double-wide bay at the lower right of the enclosure. Because it occupies one of the bays used for the CMM, only one InfiniBand module may be installed in the system.



NOTE: For any blade to access the InfiniBand module, it must first have an InfiniBand card installed on its mainboard. See [Appendix B](#) for details on the Mezzanine HCA cards that available for use with the InfiniBand module.

Figure 4-4. InfiniBand Module

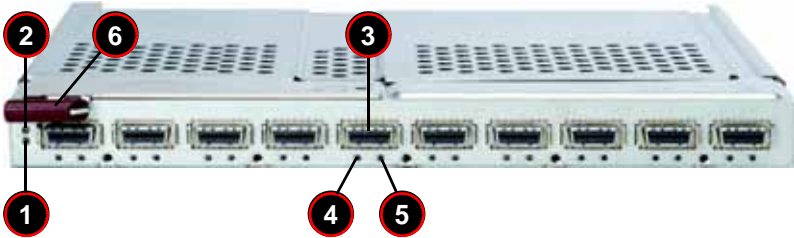


Table 4-5. InfiniBand Module Interface

Item	Description
1	Module Power LED
2	Module Status LED
3	External InfiniBand Port (10 total)
4	Port Physical Link LED (Green)
5	Port Activity LED (Yellow) Module Release Handle
6	Module Release Handle

Table 4-6. InfiniBand Module Features

Feature	Description
Chipset	Mellanox® InfiniScale™ III
Internal/External Ports	Internal: 10 4x DDR copper ports (capable of 14) / External: 10 4x DDR copper ports
Bandwidth	4x DDR (20 Gbps) non-blocking architecture for 960 Gbps total bandwidth (24-port)
Latency	160 ns port-to-port switch latency
Remote Management	In-band InfiniBand IBML (InfiniBand Maintenance Link), Command Line Interface (CLI)
Power Consumption	34 - 40W
Operating System	Firmware (upgradeable)

Installing/Removing the InfiniBand Module

Before installing the InfiniBand module make sure the cover to the module has been installed before proceeding. Refer to the anti-static precautions described in [Chapter 2](#).

The InfiniBand module must be installed into a double-wide bay (as shown in bay #3 in [Figure 4-1](#)). Assuming that you have already created a double-wide bay out of two single-wide bays (detailed in [Section 4-5](#)), continue with the steps below.

Installing the Module

1. Remove the dummy cover from the bay you want to place the module in.
2. Place the module's release handle in the open position.
3. Slide the module into the module bay until it stops.
4. Push the release handle to the closed position.

After the module has been installed and the handle locked, it will power on after a short delay and a POST test will run to verify it is working properly.

Removing the Module

1. Pull out the release handle to the open position.
2. Pull the module out of the bay.
3. Replace immediately with another module or with a dummy module cover to maintain airflow integrity.

InfiniBand Switch LEDs

The following LEDs in [Table 4-7](#) are found on the InfiniBand switch module.

Table 4-7. InfiniBand Switch LEDs

LED	State	Description
Module Status LED	Blink	Switch is booting its firmware
	Steady On	Boot process failed
	Off	Switch is properly booted and operational
Module Power LED (Green)	Steady On	Switch has power and is operational
	Off	There is a problem with the power being supplied to the switch.
Port Physical Link LED (Green)	Steady On	Physical link established
	Blink	Physical link error, poor connection quality
	Off	Port is off or has no physical connection
Port Activity LED (Yellow)	Steady On	Logic link established, no activity
	Blinking	Data transferring to/from the port
	Off	Logical link is down

Configuring the InfiniBand Module

Maintenance and configuration of the InfiniBand module within a Windows OS is performed with Mellanox's® WinIB™ software package. WinIB allows you to upgrade the firmware and monitor temperature, voltages, port utilization and other switch parameters.

In a Linux environment, maintenance and configuration of the InfiniBand module is performed with the OFED (OpenFabrics Enterprise Distribution).

Both software packages are available to download on Mellanox's web site:

WinIB: <https://docs.mellanox.com/dm/WinIB/ReadMe.html>

OFED: <http://www.mellanox.com/products/ofed.php>

4-3 GbE (Ethernet) Modules

Your SuperBlade enclosure can include either of two models of GbE Ethernet Modules installed in it. The GEM-001 GbE Ethernet switch is a configurable switch with ten uplink ports whereas the GEM-002 GbE Ethernet Pass-through Module has fourteen uplink ports and is a non-configurable pass through module.

GbE modules can only be installed in the upper and/or lower left module bays.

GEM-001 GbE Ethernet Switch Module

The GEM-001 GbE Ethernet switch module (part ID SBM-GEM-001) includes 10 (ten) 1-Gb/s uplink (RJ45) ports and 14 1-Gb/s downlink ports for the SuperBlade's LAN interfaces. The Ethernet switch module has two internal Ethernet paths to the CMM(s) and is used to provide a connection between the Ethernet controller integrated on the mainboard and an external Ethernet device. This is a hot-pluggable module.

Figure 4-5. GEM-001 GbE (Ethernet) Switch Module

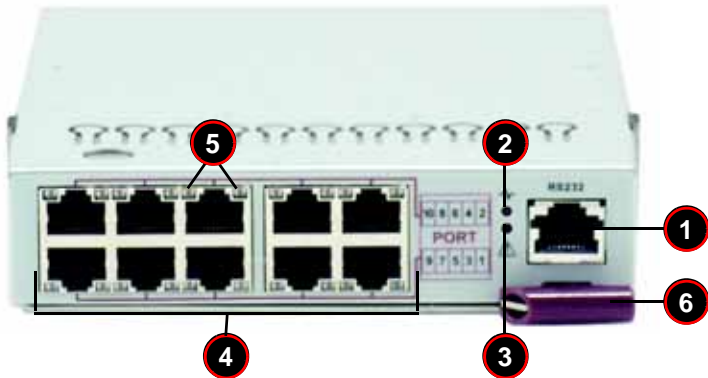


Table 4-8. GEM-001 GbE Switch Module Interface

Item	Description
1	RS232 (COM) Serial Port
2	"Initiation OK" LED
3	Module Fault LED
4	Ethernet Ports
5	Ethernet Port Status LEDs
6	Module Release Handle

Table 4-9. GEM-001 GbE Switch Module Features

Feature	Description
Chipset	Broadcom BCM5345M
Internal/External Ports	Internal: Fourteen 1 Gbps downlink ports / External: Ten 1 Gbps RJ45 uplink ports
Bandwidth	24 Gbps non-blocking
Trunking	Link aggregation support
Jumbo Frame Support	Up to 9 kb
Remote Management	Browser-based management
Protocols	Spanning Tree, Rapid Spanning Tree, Multiple Spanning Tree (802.1d.1w)
Power Consumption	~30.6W
Operating System	Firmware (see "Firmware" on page 4-6 for a procedure)

GEM-002 GbE Ethernet Pass-through Module

The GEM-002 GbE Ethernet Pass-through Module part ID SBM-GEM-001) is a non-configurable pass through module that includes 14 (fourteen) 1-Gb/s uplink (RJ45) ports and 14 1-Gb/s downlink ports for the SuperBlade's LAN interfaces. This Ethernet switch module has two internal Ethernet paths to the CMM(s) and is used to provide a connection between the Ethernet controller integrated on the mainboard and an external Ethernet device.

Unlike the GEM-001 model GbE Ethernet switch, this is a pass-through module and is not configurable. With this module Blade 1 would be connected directly to port 1, Blade 2 to port 2 and so on. If you are only connected to 10 blades then ports 11 through 14 are not connected.

Temperature and voltage of the pass-through module are read through the CMM module. The LED's of the pass-through for a blade are only lit when the blade is on. Like the other GEM-001 switch, this pass-through module is a hot-pluggable module.



NOTE: The GEM-002 pass-through module **must** be connected to another Gigabit Switch in order to operate. If you connect it to a 10/100 switch, it will not work.

Figure 4-6. GEM-002 GbE (Ethernet) Pass-through Module

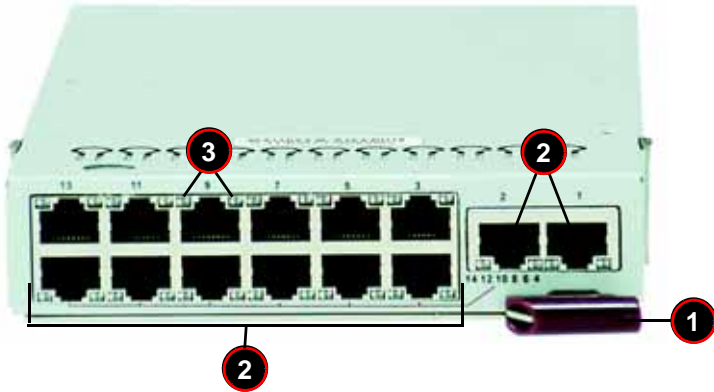


Table 4-10. GEM-002 GbE Pass-through Module Interface

Item	Description
1	Module Release Handle
2	Ethernet Ports
3	Ethernet Port Status LEDs

Table 4-11. GEM-002 GbE Pass-through Module Features

Feature	Description
Chipset	Broadcom 5464
Internal/External Ports	Internal: Fourteen 1 Gbps downlink ports / External: fourteen 1 Gbps RJ45 uplink ports
Remote Management	Browser-based management
Protocols	Spanning Tree, Rapid Spanning Tree, Multiple Spanning Tree (802.1d.1w)
Power Consumption	~30.6W

Installing/Removing a GbE Module

Follow the procedures below for installing or uninstalling a GEM-001 or GEM-002 GbE Module.

Installing a GbE Module

1. Make sure the cover to the module has been installed before proceeding. Follow the anti-static precautions described in [Chapter 2](#).
2. Remove the dummy cover from the bay you want to place the module in.
3. Place the module's release handle in the open position.
4. Slide the module into the module bay until it stops.
5. Push the release handle to the closed position.

After the module has been installed and the handle locked, it will turn on and a POST test will run to verify it is working properly. If there are no problems the blue **Init. OK** LED on the module will illuminate and you will see a **OK** under INITIATED in the GbE SWITCH screen of the management software utility.

Note that if the module is installed in a top bay it will be positioned upside-down.

Removing a GbE Module

1. Pull out the release handle to the open position.
2. Pull the module out of the bay.
3. Replace immediately with another module or with a dummy module cover to maintain airflow integrity.

GbE Module LEDs

Table 4-12 describes the LEDs found on GbE modules. The figure below shows the locations for the Link/Activity LED and the Speed LED next to each Ethernet Port.

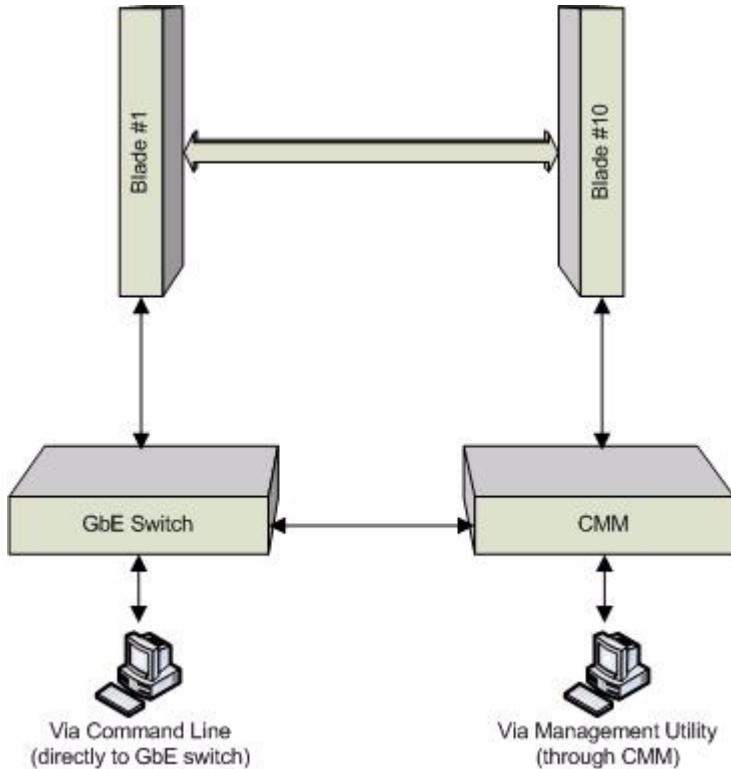


Table 4-12. GbE Switch LEDs

LED	State	Description
Module Initiation OK LED (GEM-001 Module Only)	Steady On	The GEM-001 GbE switch module is operational and has passed the POST (Power-On Self-Test) with no critical faults.
Module Fault LED (Red) (GEM-001 Module Only)	Steady On	When lit, this LED indicates that the GEM-001 GbE switch module has either failed the POST or has detected an operational fault within the module. When this LED is lit, the fault LED on the blade enclosure will also turn on.
Link/Activity Ethernet Port Status LED	Solid Green	This indicates that the link is established, no activity
	Blinking Green	This indicates that data is being transmitted (Tx) or received (Rx)
	Off	This indicates that no link is established
Speed Ethernet Port Status LED	Amber	Connection speed of the port is 1 Gb/sec
	Green	Connection speed of the port is 100 Mb/sec
	Off	Connection speed of the port is 10 Mb/sec

Configuring the GEM-001 GbE Switch Module

Figure 4-7. Configuring the GbE Switch Module



The GEM-001 GbE switch module can be configured using two methods. You may configure it:

- Through the web-based management utility or IPMI (via the CMM module)
- Directly through a command line (using a telnet interface or a serial console)

The management utility and IPMI access the GbE switch module through the CMM module. To access it directly, use the command line (see [Figure 4-7](#)).

Note that any port may be configured as *up* (active) or *down* (inactive). All ports are active by default.

For more detailed information on configuration of the Supermicro Gigabit Ethernet Switch, see [Appendix C](#).

Web-based Management Utility/IPMI

Using the web-based management utility or IPMI is the most user-friendly method of configuring the GbE switch module. These utilities also allow you to reset to the default settings. You can access the configuration menu either through the management utility or by a network connection. See [Chapter 8](#) for details.

Network Connection/Login

Type the IP address of the server that you want to connect in the address bar in your browser and hit <ENTER>. (The default IP address is "192.168.100.102".) Once the connection is made, the LOGIN screen displays.

Logging In to the Network

1. Type in your Username in the USERNAME box.
2. Type in your Password in the PASSWORD box and click on LOGIN.

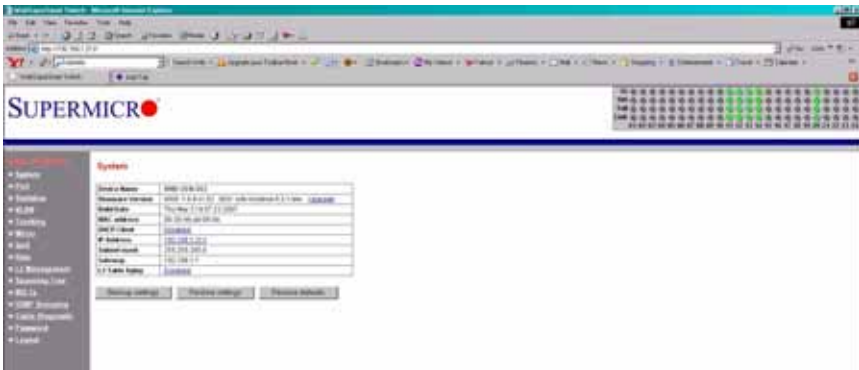


NOTE: The default username and the default password are both **ADMIN**.

3. The screen shown in [Figure 4-8](#) is then displayed.

On the left side of the screen is a clickable list of the various parameters you may change in configuring the GbE switch module to your needs.

Figure 4-8. Configuring the GEM-001 GbE Switch Module



Address Defaults

The following are the default addresses that are initially set. Afterwards, you can change these values within the program (see "[Device Settings](#)" on page 8-26).

Table 4-13. GEM-001 GbE Switch Module Address Default Settings

Address	Default Setting
Default IP Address	192.168.100.102
Default Gateway Address	192.168.100.1
Default Subnet Mask	255.255.255.0



NOTE: If two GbE switches are installed in a SuperBlade system, you will have to change the IP address of one from the default so that both switches have unique addresses.

Command Line

Configuring the GbE switch can be done using a command line via a telnet interface. This is done directly through the Ethernet port of the GbE module using the following procedure.

1. Connect a PC to the Ethernet port on the back of the GbE switch.
2. Type **telnet 192.168.100.102** in the command window then hit the <ENTER> key.
3. Now that you are in the telnet console, provide the username and password to login.
4. The shell prompt **ECOS>** should appear. For help, you may type **help** then hit the <ENTER> key for a list of commands.

Firmware

The firmware for the GEM-001 GbE switch module resides on a chip on the PCB. Use the Web-based Management utility to upgrade the firmware.

Accessing the GbE Switch Firmware

1. Enter the IP address of the switch into the address bar of your browser and hit <ENTER>.
2. On the next screen, click on the **SYSTEM** link on the list on the left. The window to the right shows you the current firmware version and provides an **UPGRADE** link (see [Figure 4-8](#)).
3. Click on the **UPGRADE** link to update your firmware. A Rescue ROM socket is also included on the PCB that allows you to reinstall the firmware with a pluggable chip.

4-4 Blade Modules

Up to ten blade modules may be installed into a single blade enclosure. Blade modules with Windows and Linux operating systems as well as AMD or Intel processors may be mixed together in the same blade enclosure.

Powering up a Blade Unit

Each blade unit may be powered on and off independently from the rest of the blades installed in the same enclosure. A blade unit may be powered up in two ways:

- Press the power button on the blade unit.
- Use IPMI View or the web-browser based management software to apply power.

Powering down a Blade Unit

A blade unit may be powered down in two ways:

- Press the power button on the blade unit.
- Use IPMI View or the web-browser based management software to remove power.

Removing a Blade Unit from the Enclosure

Although the blade system may continue to run, individual blades should always be powered down before removing them from the enclosure.

Removing a Blade Unit from the Enclosure

1. Power down the blade unit (see "[Powering down a Blade Unit](#)" above).
2. Squeeze both handles to depress the red sections then pull out both handles completely and use them to pull the blade unit from the enclosure.

Removing/Replacing the Blade Cover

The blade cover must be removed to access the mainboard when you need to install or remove processors, memory units, the onboard battery and so on.

Removing/Replacing the Blade Cover

1. Remove the blade unit from the enclosure (see "[Removing a Blade Unit from the Enclosure](#)" above).
2. Depress the two buttons on the cover while pushing the cover toward the rear of the blade unit. When it stops, lift the cover off the blade unit.
3. To replace the cover, fit the six grooves in the cover into the studs in the sides of the blade, then slide the cover toward the front of the blade to lock it into place.

Installing a Blade Unit into the Enclosure

Make sure the cover of the blade unit has been replaced first before installing a blade unit in the enclosure.

Installing a Blade Unit into the Enclosure

1. Slowly push the blade unit into its bay with the handles fully pulled out (see [Figure 4-9](#)).
2. When the blade stops, push the handles back in to their locked position, making sure the notches in both handles catch the lip of the enclosure (see [Figure 4-10](#)).



WARNING: Use extreme caution when inserting a blade module into the enclosure. If the blade's power connector becomes damaged, it can damage pins on other blade bays that it is inserted into.

Figure 4-9. Inserting a Blade into the Enclosure

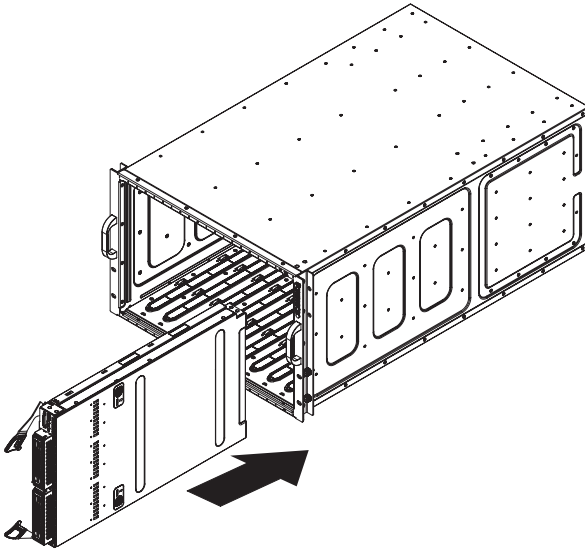
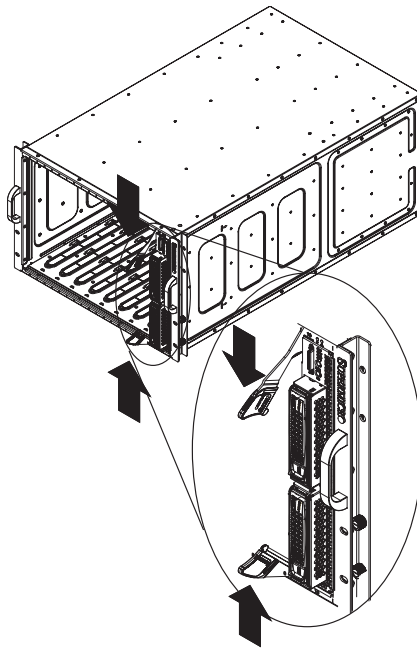


Figure 4-10. Locking the Blade into Position



4-5 Double-Wide Modules

Most modules in the SuperBlade fit into single-wide bays. The InfiniBand module however, requires a double-wide bay. The enclosure's module bays were designed to be easily modified from single to double-wide by following the procedure below.

Modifying an Enclosure's Module Bays for Double-wide Modules

1. Remove the four screws that secure the inner enclosure to the main enclosure. Slide the inner enclosure outward, depressing the locking tabs on both sides to pull it completely out.
2. Remove any single-wide modules that are occupying the bays you wish to modify to a double-wide bay.
3. In the module bay you wish to expand to double wide, remove the two screws that secure the center support to the inner enclosure then take out the center support. See [Figure 4-12, Step 1](#) for details.
4. Remove the two screws from the underside of each of the two horizontal spacers. See [Figure 4-12, Step 2](#) for details.
5. Using four screws, install the long horizontal spacer to the same space where the two short spacers were removed. See [Figure 4-13, Step 3](#) for details.

6. You can now install a double-wide module into the bay. See [Figure 4-13, Step 4](#) for details.



NOTE: This procedure describes modifying two single-wide bays located at the top of the inner enclosure. The same procedure applies to the two single bays located at the bottom of the enclosure, but note that the horizontal spacers in the bottom bays use a guide pin and are not interchangeable with the upper bay spacers (see [Figure 4-5](#) for details).

Modules in the upper bays will have their release handles on the bottom, while modules in the lower bays will have their release handles on the top.

Placing modules in an "upside-down" orientation does not affect their operation.

Figure 4-11. Horizontal Spacers for Single Bays



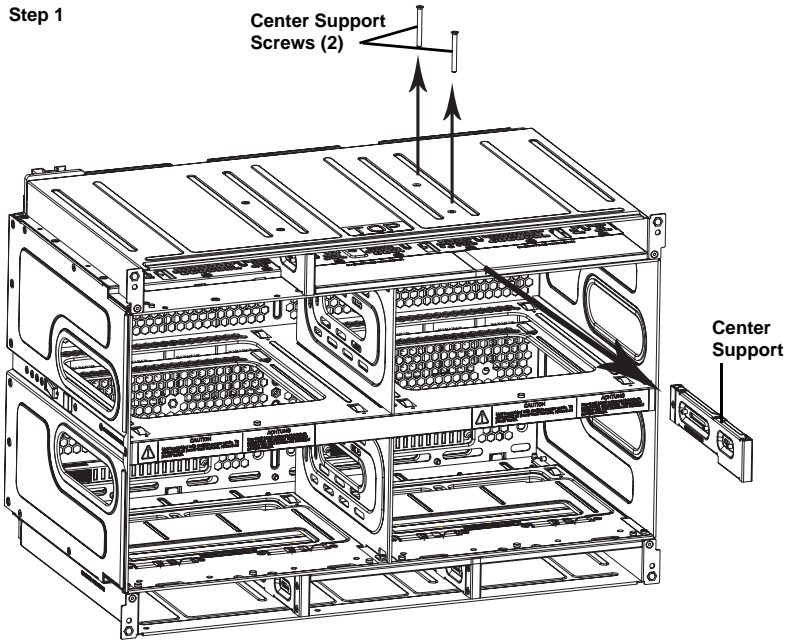
MCP-560-00012-1N
(for top bay)



MCP-560-00009-1N
(for bottom bay)

Figure 4-12. Modifying for a Double-Wide Module Bay (Steps 1 & 2)

Step 1



Step 2

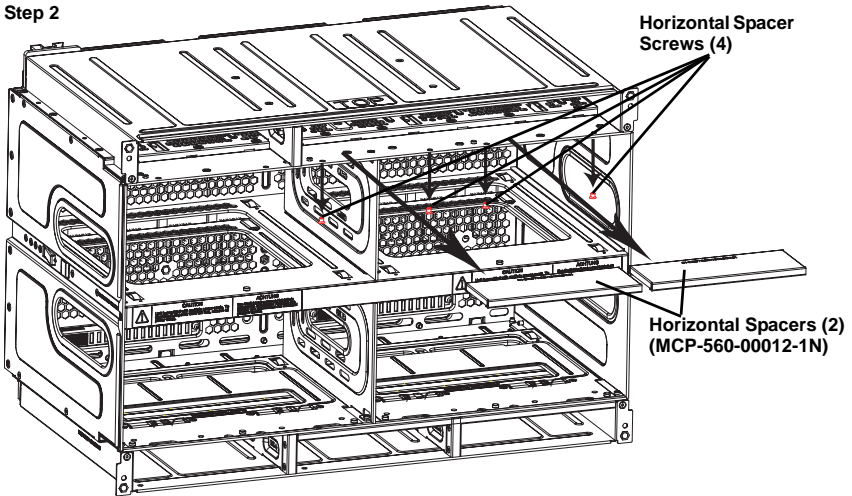
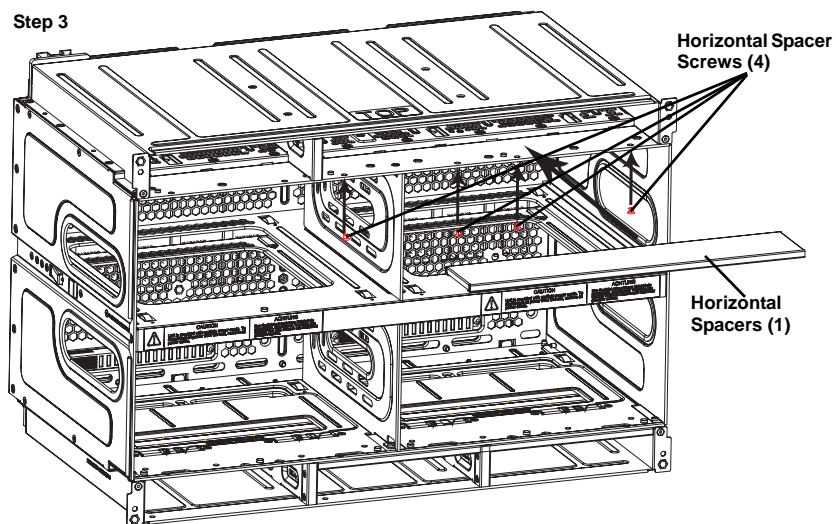
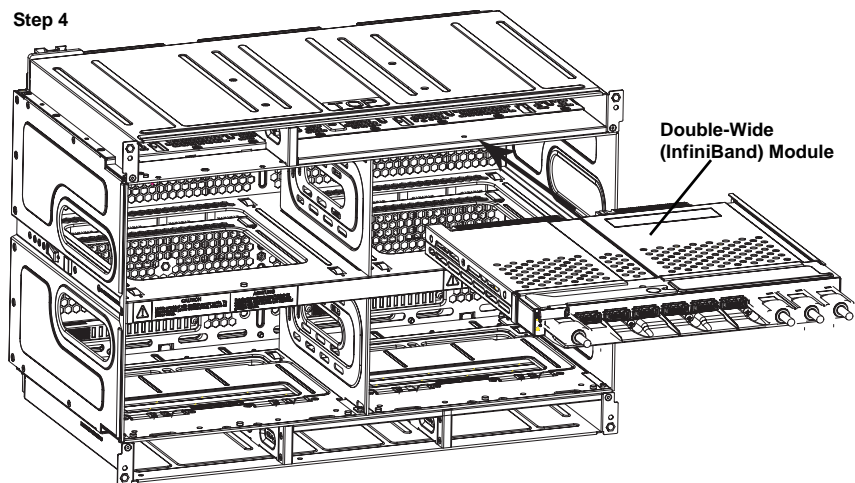


Figure 4-13. Modifying for a Double-Wide Module Bay (Steps 3 & 4)

Step 3



Step 4



Notes

Chapter 5

Blade Unit

This chapter describes the blade units (modules) available for the SuperBlade enclosure. Installation and maintenance should be performed by experienced technicians only.

A summary of available blade units, their mainboards, chipsets and the types of enclosure they can go into is shown in [Table 5-1](#).

Table 5-1. SuperBlade Blade Units

Blade Model	Mainboard	Chipset	Enclosure
SBA-7141M-T	BHQME	NVidia MCP55 Pro	10-bay SBE-710E
SBA-7121M-T1	BHDME	NVidia MCP55 Pro	10-bay SBE-710E

5-1 Control Panel

Each blade has a similar control panel (Figure 5-1) with power on/off button, a KVM connector, a KVM button and four LEDs on the top front of the unit. The numbers mentioned in Figure 5-1 are described in Table 5-2.

Figure 5-1. Blade Control Panel

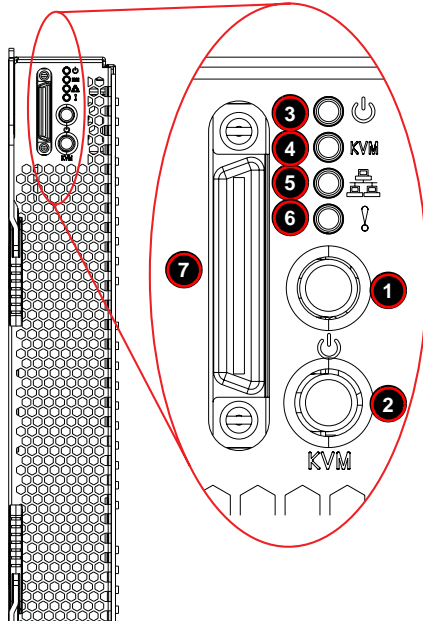


Table 5-2. Blade Control Panel

Item	Function	State	Description
1	Power Button	N/A	Turns blade module on and off
2	KVM Button	N/A	Initiates KVM function (used with remote KVM only)
3	Power LED	Green	Indicates power status "On"
		Orange	Indicates power status "Off" (with power cables plugged in)
4	KVM/UID LED	Blue	Indicates KVM being utilized on blade unit
		Flashing Blue	Indicates UID activated on blade module
5	Network/IB LED	Flashing Green	Indicates network activity over LAN
		Flashing Orange	Indicates network activity over InfiniBand module
6	System Fault LED	Red	Indicates a memory error, VGA error or any error that prevents booting
7	KVM Connector	N/A	Connector for SUV/KVM cable

Power Button

Each blade has its own power button so that individual blade units within the enclosure may be turned on or off independently of the others. Press the power button (#1) to turn on the blade server. The power LED (#3) will turn green. To turn off, press and hold the power button for >4 seconds and the power LED will turn orange.

KVM Button

KVM stands for Keyboard/Video/Mouse. With KVM, a user can control multiple blades with a single keyboard/video/mouse setup. Connect your keyboard, mouse and monitor to the USB and VGA connectors on the CMM module, then push the KVM button on the control panel of the blade module you wish to access.

KVM LED Indicators

The LED indicators for blade modules are shown in [Table 5-3](#).

Table 5-3. KVM LED Indicators

LED	State	Description
Power LED	Green	Power On
	Amber	Standby
	Red	Power Failure (See Note below)
KVM/UID LED (Blue)	Steady On	Indicates that KVM has been initialized on this blade module
	Flashing	Serves as a UID indicator (the UID function is activated with a management program)
Network LED (Green)	Flashing	Flashes on and off to indicate traffic (Tx and Rx data) on the LAN connection to this blade module.
System Fault LED (Red)	Steady On	This LED illuminates red when a fatal error occurs. This may be the result of a memory error, a VGA error or any other fatal error that prevents the operating system from booting up.



NOTE: In the event of a power failure, the N+1 Redundant Power Supply (if included in your system's configuration) automatically turns on and picks up the system load to provide uninterrupted operation. The failed power supply should be replaced with a new one as soon as possible.

KVM Connector

Alternatively, you may connect a KVM cable (CBL-0218L, with a keyboard/video/mouse attached) to the KVM connector (#7) of the blade you wish to access. To switch to another blade, disconnect the cable then reconnect it to the new blade.

See [Section 4-1: Chassis Management Module on page 4-2](#) for details on using the KVM function remotely.

5-2 Removing or Replacing the Blade Cover

The blade cover must be removed to access the mainboard when you need to install or remove processors, memory units, the onboard battery and so on.

Removing/Replacing the Blade Cover

1. Remove the blade unit from the enclosure (see [Section 4-4: Blade Modules on page 4-18](#) for details).
2. Depress the two buttons on the cover while pushing the cover toward the rear of the blade unit. When it stops, lift the cover off the blade unit.
3. To replace the cover, fit the six grooves in the cover into the studs in the sides of the blade, then slide the cover toward the front of the blade to lock it into place.

5-3 Processor Installation

One or two processors may be installed to the mainboard of each blade unit. See [Chapter 1](#) for general information on the features of the blade unit and our web site for further details including processor, memory and operating system support.



WARNING: This action should only be performed by a trained service technician. Allow the processor heatsink to cool before removing it.

Removing a processor

1. Power down and remove the blade unit from the enclosure (see [Section 4-4: Blade Modules on page 4-18](#)).
2. Remove the cover of the blade unit (see [Section 4-4](#)).
3. Loosen the four screws that secure the heatsink to the mainboard.
4. Remove the heatsink by *gently* rotating it back-and-forth sideways with your fingers to release it from the processor. Set the heatsink aside and upside-down so that nothing comes into contact with the thermal grease on its underside.
5. Raise the lever of the processor socket up until the processor is released from the socket, then lift the silver cover plate and remove the processor.



WARNING: This action should only be performed by a trained service technician.

Installing a Processor

1. If present, remove the protective black PnP cap from the processor socket.
2. Raise the lever of the processor socket until it reaches its upper limit.
3. Lift the silver cover plate completely up and out of the way.



NOTE: Be careful not to damage the pins protruding from the CPU socket.

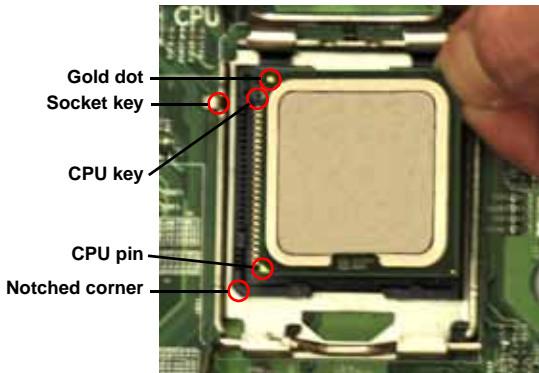
4. Align pin 1 of the processor with pin 1 of the socket (both are marked with a small gold triangle) and gently seat the processor into the socket ([Figure 5-2](#)).
5. Check to make sure the processor is flush to the socket and fully seated.
6. Lower the socket lever until it locks.
7. To install the heatsink, apply thermal grease to the top of the processor. (If reinstalling a heatsink, first clean off the old thermal grease with a clean, lint-free cloth.)
8. Place the heatsink on the processor then tighten two diagonal screws until snug, then the other two screws.
9. When all four screws are snug, tighten them all to secure the heatsink to the mainboard.



NOTE: Do not overtighten the screws as this may damage the processor or the heatsink.

10. Replace the cover on the blade unit and finish by installing the unit back into the blade enclosure.

Figure 5-2. Installing a Processor in a Socket



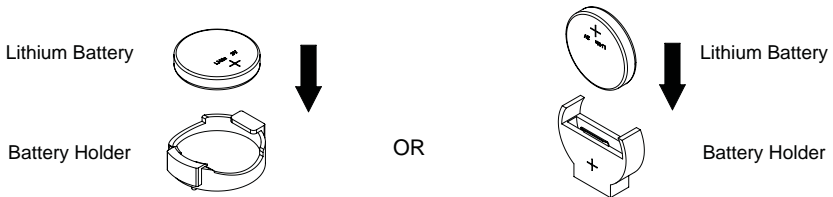
5-4 Onboard Battery

A battery is included on the mainboard to supply certain volatile memory components with power when power has been removed from the blade module. If this battery dies, it must be replaced with an equivalent CR2032 Lithium 3V battery. Dispose of used batteries according to the manufacturer's instructions. See [Figure 5-3](#) for a diagram of installing a new onboard battery.



WARNING: There is a danger of explosion if the onboard battery is installed upside down, which reverses its polarities.

Figure 5-3. Installing the Onboard Battery



5-5 Memory

The mainboard of each blade unit must be populated with DIMMs (Dual In-line Memory Modules) to provide system memory. **The DIMMs should all be of the same size and speed and from the same manufacturer due to compatibility issues.** See details below on supported memory and our web site (www.supermicro.com/products/superblade) for recommended memory.

Populating Memory Slots

The mainboard has eight to sixteen memory slots, depending upon the blade model. Both interleaved and non-interleaved memory are supported, so you may populate any number of DIMM slots.

Populating two slots at a time (DIMM1A + DIMM2A, DIMM3A + DIMM4A, etc.) with memory modules of the same size and of the same type will result in dual-channel, interleaved memory, which is faster than single-channel, non-interleaved memory. See [Table 5-4](#) and [Figure 5-4](#) (16-slots) or [Figure 5-5](#) (8-slots) for details.

For an interleaved configuration, memory modules of the same size and speed must be installed in pairs. You should not mix DIMMs of different sizes and speeds.

Table 5-4. Populating Memory Slots for Interleaved Operation

# of DIMMS	DIMM1A	DIMM1B	DIMM1C	DIMM1D	DIMM2A	DIMM2B	DIMM2C	DIMM2D	DIMM3A	DIMM3B	DIMM3C	DIMM3D	DIMM4A	DIMM4B	DIMM4C	DIMM4D
2	X				X											
4	X				X				X				X			
6	X	X			X	X			X				X			
8	X	X			X	X			X	X			X	X		
10	X	X	X		X	X	X		X	X			X	X		
12	X	X	X		X	X	X		X	X	X		X	X	X	
14	X	X	X	X	X	X	X	X	X	X	X		X	X	X	
16	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Figure 5-4. 16-slot DIMM Numbering

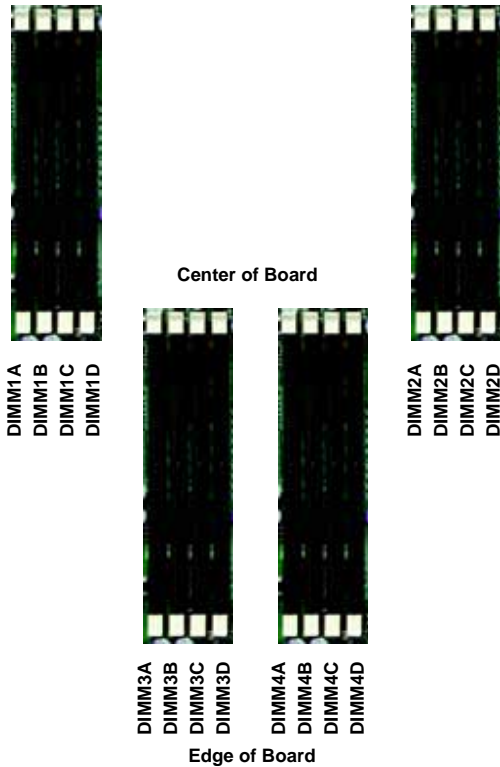
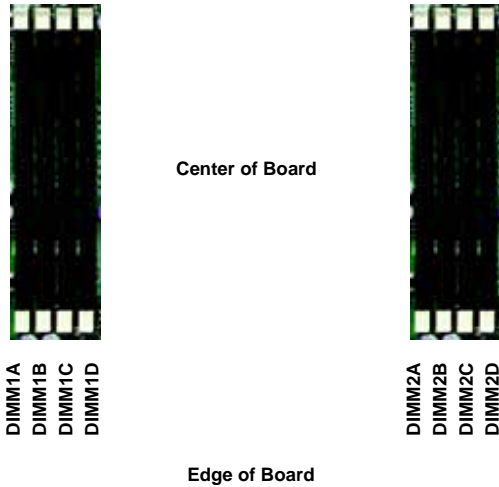


Figure 5-5. 8-slot DIMM Numbering



DIMM Installation



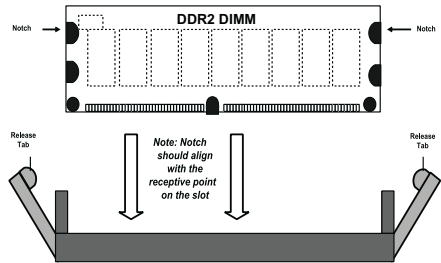
WARNING: Exercise extreme care when installing or removing DIMM modules to prevent any possible damage.

To install DIMM memory modules, use the procedure below.

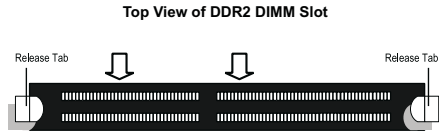
1. Power down the blade module.
2. Remove the blade from the enclosure and the cover from the blade.
3. Remove the air shroud that covers the DIMM slots.
4. Insert each DIMM vertically into its slot, starting with slots 1A and 2A. Pay attention to the notch along the bottom of the module to prevent inserting the DIMM incorrectly (see [Figure 5-6](#)).

Figure 5-6. Installing a DIMM into a Memory Slot

To Install: Insert module vertically and press down until it snaps into place. Pay attention to the bottom notch.



To Remove: Use your thumbs to gently push each release tab outward to free the DIMM from the slot.



5. Gently press down on the DIMM until it snaps into place in the slot. Repeat for all modules (see [Table 5-4](#) for installing DIMMs into the slots in the correct order).
6. Replace the air shroud and the blade cover and install the blade module back into the enclosure.
7. Power up the blade unit.

5-6 SBA-7141M-T Blade Unit Features

Figure 5-7. SBA-7141M-T Blade Unit Front View



This section describes the SBA-7141M-T blade unit. See [Figure 5-7](#) for a front view of the blade unit and [Table 5-5](#) for its features.

Table 5-5. SBA-7141M-T Blade Unit Features

Feature	Description
Processors	Supports four AMD Opteron 8300/8200 series processors
Memory	Supports up to 64 GB of ECC Registered DDR2-667/533/400 DIMMs in four 8-DIMM slot banks
Storage	One Internal 2.5" SATA hard disk drive
Ports	KVM port (1), SATA ports (2)
Features	Onboard ATI ES1000 graphics chip with 16MB of SDRAM, IPMI 2.0, ATA/100, Plug and Play, APM 1.2, DMI 2.3, PCI 2.2, ACPI 1.0/2.0, SMBIOS 2.3, Real Time Clock, Watch Dog,
Power Consumption	Base Power Draw (~35W) / Power per CPU (90W or 130W) / Power per DIMM (typically 14.5W)

Mainboard

The mainboard in the SBA-7141M-T blade unit is a proprietary design, which is based on the NVidia MCP55 Pro chipset. See [Figure 5-9](#) for a block diagram of this chipset, [Figure 5-8](#) for a view of the BHQME Mainboard and [Figure 5-10](#) for an exploded view diagram of the blade unit.

Figure 5-8. BHQME Mainboard

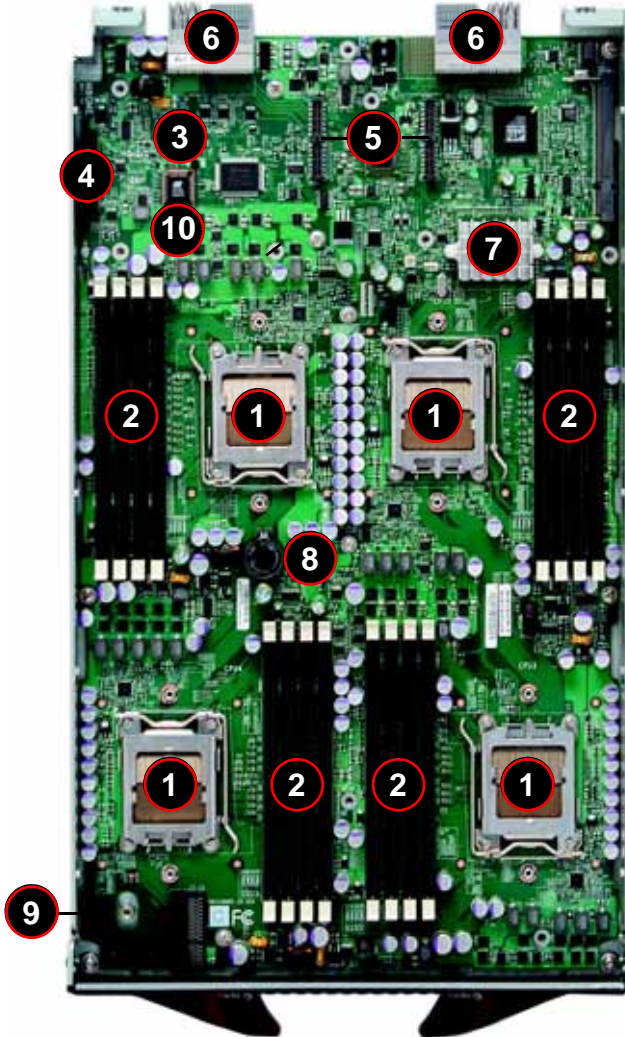
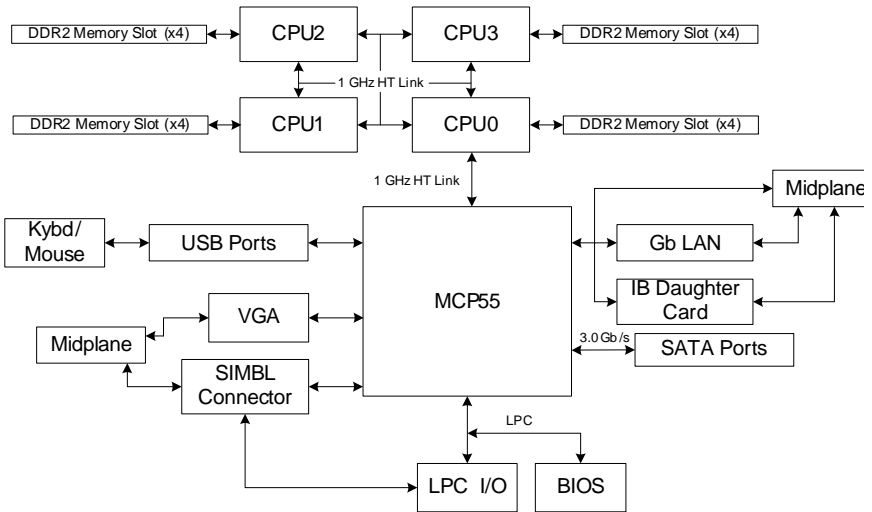


Table 5-6. BQME Mainboard Layout

Item	Description
1	CPU Sockets
2	DIMM Slots
3	Space for 2.5" SAS/SATA Hard Drive
4	SIMBL Slot
5	InfiniBand Connectors (for InfiniBand cards)
6	Gbx Connectors (for power and logic to backplane)
7	MCP55 chip
8	Onboard Battery
10	KVM Module
11	BIOS Chip

Figure 5-9. NVidia MCP55 Pro Chipset: Block Diagram for SBA-7141M-T



Jumpers

The jumpers present on the mainboard are used by the manufacturer only; there are no jumpers used to configure the operation of the mainboard.

CMOS Clear

JBT1 is used to clear CMOS and will also clear any passwords. JBT1 consists of two contact pads located near the BIOS chip (#11 in [Figure 5-8](#)).

Clearing CMOS

1. First power down the blade and remove it from the enclosure.
2. Remove the blade cover to access the mainboard (see ["Removing or Replacing the Blade Cover" on page 5-4](#) for details). Short the CMOS pads with a metal object such as a small screwdriver.
3. Replace the cover, install the blade back into the enclosure and power it on.

Blade Unit Components

Blade components are shown in [Figure 5-10](#) and described in [Table 5-7](#).

Figure 5-10. Exploded View of the SBA-7141M-T Blade Unit

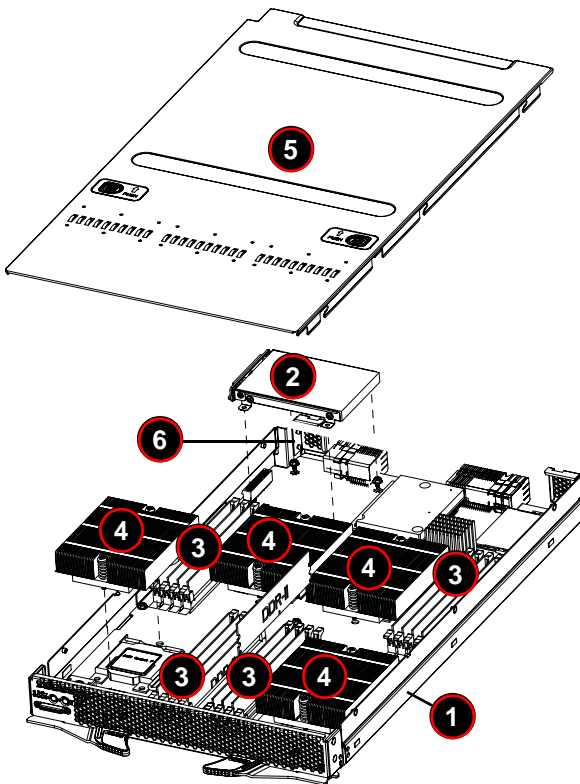


Table 5-7. Main Components of SBA-7141M-T Blade Unit

Item	Description
1	Blade Unit/Module
2	2.5" Hard Drive
3	DIMMs (system memory)
4	CPU Heatsinks (2)
5	Top Cover
6	Backplane



WARNING: Properly ground the server before performing any installation procedures to prevent electrical damage to components. Allow components to cool before handling them.

Memory Support

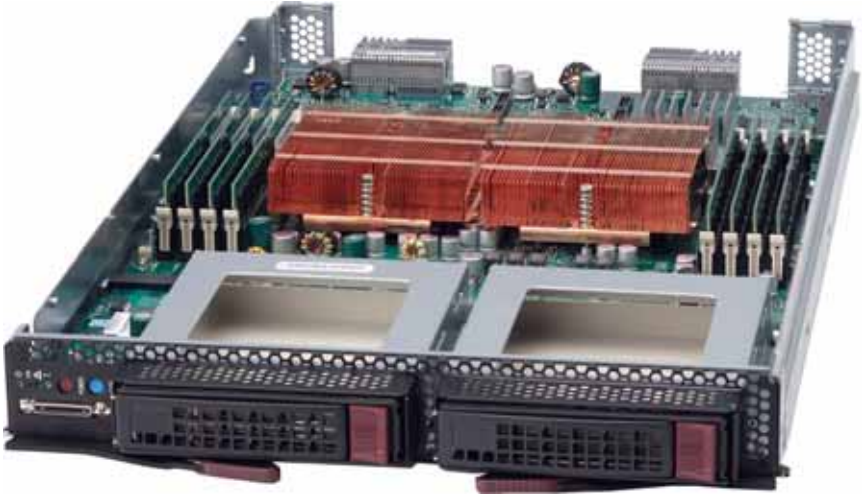
The BHQME mainboard supports up to 64 GB of ECC Registered DDR2-667/533/400 SDRAM in sixteen DIMM sockets. See [Section 5-5](#) for further details on mainboard memory installation.

Hard Disk Drive

The SBA-7141M-T blade unit can accommodate one internal 2.5" SATA hard disk drive, which is mounted directly on the blade's mainboard.

5-7 SBA-7121M-T1 Blade Unit Features

Figure 5-11. SBA-7121M-T1 Blade Unit Front View



This section describes the SBA-7121M-T1 blade unit. See [Figure 5-7](#) for a front view of the blade unit and [Table 5-5](#) for its features.

Table 5-8. SBA-7121M-T1 Blade Unit Features

Feature	Description
Processors	Supports two AMD Quad/Dual-Core Opteron 2000 series processors
Memory	Supports up to 32 GB of ECC Registered DDR2-667/533/400 DIMMs in two 8-DIMM slot banks
Storage	Two hot-plug 3.5" SATA hard disk drives
Ports	KVM port (1), SATA ports (2)
Features	Onboard ATI ES1000 graphics chip with 16MB of SDRAM, IPMI 2.0, ATA/100, Plug and Play, APM 1.2, DMI 2.3, PCI 2.2, ACPI 1.0/2.0, SMBIOS 2.3, Real Time Clock, Watch Dog,
Power Consumption	Base Power Draw (~35W) / Power per CPU (90W or 130W) / Power per DIMM (typically 14.5W)

Mainboard

The mainboard in the SBA-7121M-T1 blade unit is a proprietary design, which is based on the NVidia MCP55 Pro chipset. See [Figure 5-9](#) for a block diagram of this chipset, [Figure 5-8](#) for a view of the BHDME Mainboard and [Figure 5-10](#) for an exploded view diagram of the blade unit.

Figure 5-12. BHDME Mainboard

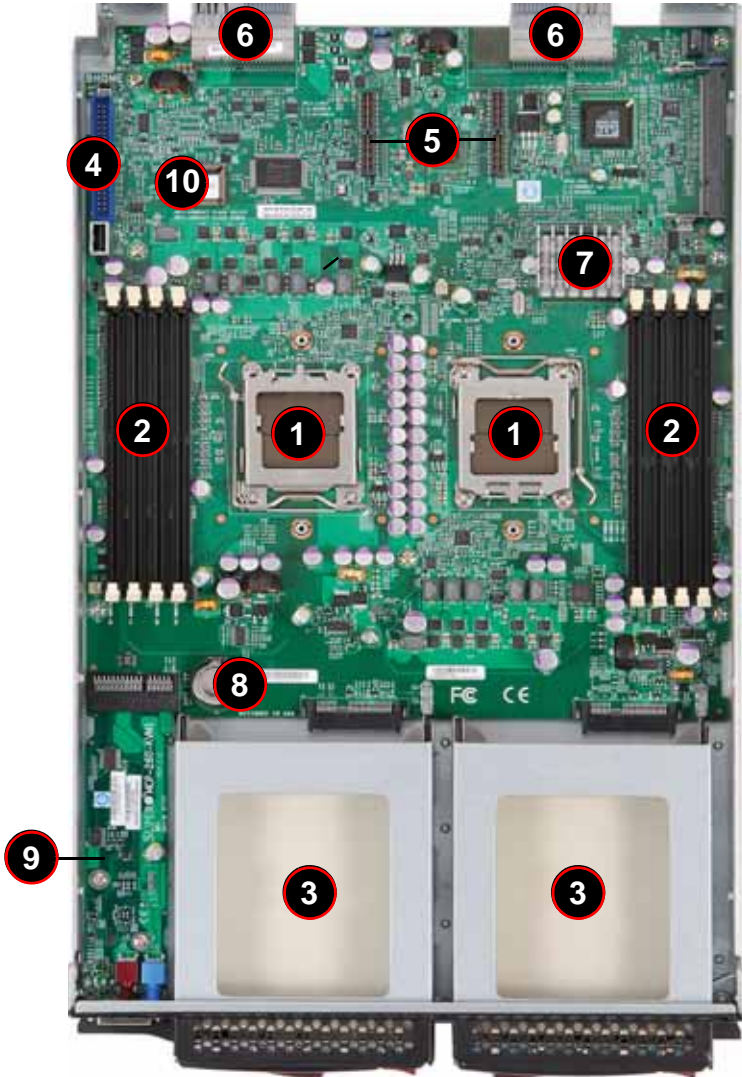
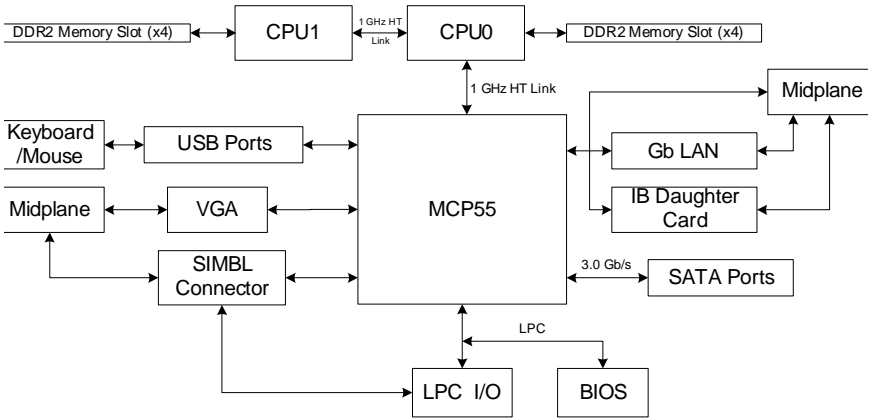


Table 5-9. BHQME Mainboard Layout

Item	Description
1	CPU Sockets
2	DIMM Slots
3	Space for 3.5" SAS/SATA Hard Drive
4	SIMBL Slot
5	InfiniBand Connectors (for InfiniBand cards)
6	Gbx Connectors (for power and logic to backplane)
7	MCP55 chip
8	Onboard Battery
9	KVM Module
10	BIOS Chip

Figure 5-13. Nvidia MCP55 Pro Chipset: Block Diagram for SBA-7121M-T1



Jumpers

The jumpers present on the mainboard are used by the manufacturer only; there are no jumpers used to configure the operation of the mainboard.

CMOS Clear

JBT1 is used to clear CMOS and will also clear any passwords. JBT1 consists of two contact pads located near the BIOS chip (#11 in [Figure 5-8](#)).

Clearing CMOS

1. First power down the blade and remove it from the enclosure.
2. Remove the blade cover to access the mainboard (see ["Removing or Replacing the Blade Cover" on page 5-4](#) for details). Short the CMOS pads with a metal object such as a small screwdriver.
3. Replace the cover, install the blade back into the enclosure and power it on.

Blade Unit Components

Blade components are shown in [Figure 5-10](#) and described in [Table 5-7](#).

Figure 5-14. Exploded View of the SBA-7121M-T1 Blade Unit

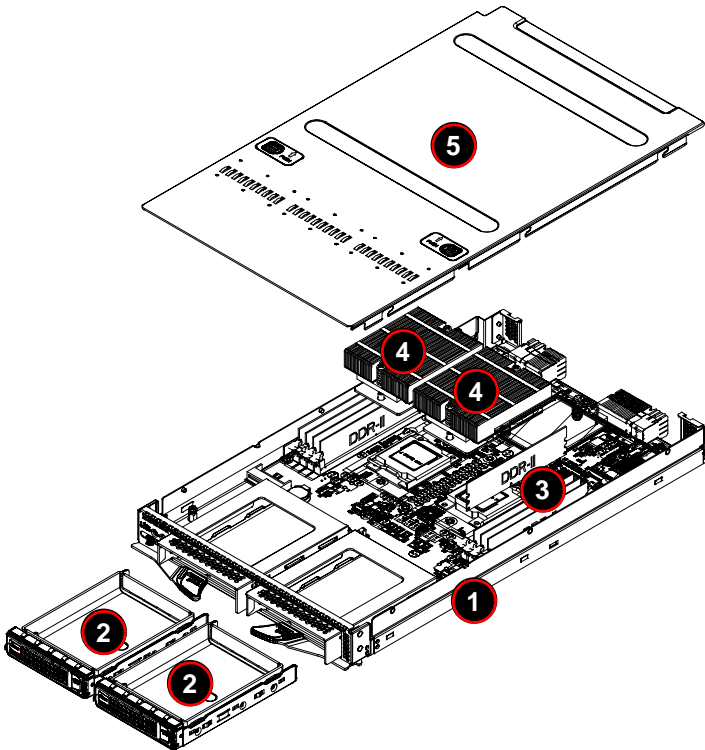


Table 5-10. Main Components of SBA-7121M-T1 Blade Unit

Item	Description
1	Blade Unit/Module
2	SATA Hard Drives (2 per blade module)
3	DIMMs (system memory)
4	CPU Heatsinks
5	Top Cover



WARNING: Properly ground the server before performing any installation procedures to prevent electrical damage to components. Allow components to cool before handling them.

Memory Support

The BHDME mainboard supports up to 32 GB of ECC Registered DDR2-667/533/400 SDRAM in eight DIMM sockets. See [Section 5-5](#) for further details on mainboard memory installation.

Hard Disk Drive

The SBA-7141M-T bladeblade unit can accommodate up to two 3.5" SATA hard disk drives, which are mounted in drive "carriers". The drives are hot-swappable and can be removed or replaced without powering down the blade unit they reside in. The two drives can be used to set up a RAID array (SATA RAID 0 or 1 only) or JBOD. These drives use a blue color for the Blade HDD active LED.



WARNING: To maintain proper airflow, both hard drive bays must have drive carriers inserted during operation whether or not a drive is installed in the carrier.

To remove a hard drive carrier, do the following:

Removing a Hard Drive Carrier

1. Locate the colored "Open" button at the bottom of the drive carrier and press it with your thumb. This action releases the drive carrier from the drive bay.
2. Pull the release handle out about 45-degrees, then use it to pull the drive carrier out.

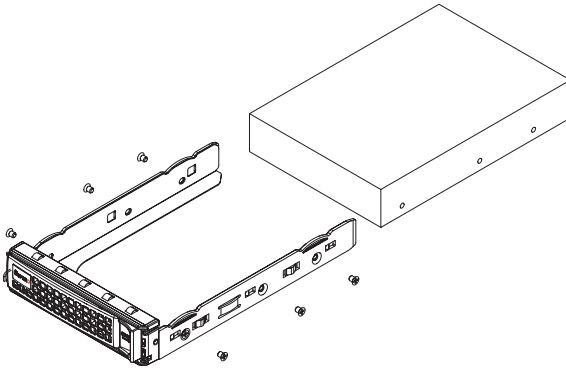
To Install a hard drive, use the following procedure:

Installing a Hard Drive

1. Remove a blank drive carrier from the blade (see removal procedure above).
2. Insert a drive into the carrier with the PCB side facing down and the connector end toward the rear of the carrier.

3. Align the drive in the carrier so that the screw holes of both line up. Note that there are holes in the carrier marked "SATA" to aid in correct installation.
4. Secure the drive to the carrier with six screws as shown in [Figure 5-15](#).
5. Insert the drive carrier into its slot keeping the Open button at the bottom. When the carrier reaches the rear of the bay the release handle will retract.
6. Push the handle in until you hear the carrier click into its locked position.

Figure 5-15. Installing a Hard Drive in a Carrier



Chapter 6

Power Supply

The SuperBlade enclosure comes standard with one CMM module (see the [Chapter 4](#) for details on the CMM module) and either two or four power supplies. See [Appendix D](#) for summary specification details on the power supplies available to the SuperBlade enclosure.

6-1 Power Supply Modules

The SuperBlade enclosure has two models of power supply modules available: the PWS-1K41-BR 1400W module ([Figure 6-1](#)) and the PWS-2K01-BR 2000W module ([Figure 6-2](#)). The features of these power supplies are shown in [Table 6-1](#) and [Table 6-2](#) below.

Figure 6-1. PWS-1K41-BR Power Supply



Table 6-1. PWS-1K41-BR Power Supply Features

Feature	Description
Output	1400W
Type	Redundant Module (N+1)
+12V	116A (200-240VAC input) 100A (100-140VAC input)
5VSB	16A
PFC	Yes
Peak Efficiency	93%
Input AC Range	100-240VAC

Table 6-1. PWS-1K41-BR Power Supply Features (Continued)

Feature	Description
Operating Conditions	Temp: -5 to 50 C Humidity: 5 to 95% RH
Fan Type	2x 90mm fans - PFC0912DE-6L38 (8000 RPM with PWM)

Figure 6-2. PWS-2K01-BR Power Supply



Table 6-2. PWS-2K01-BR Power Supply Features

Feature	Description
Output	2000W
Type	Redundant Module (N+1)
+12V	167A
5VSB	16A
PFC	Yes
Peak Efficiency	90%
Input AC Range	200-240VAC
Operating Conditions	Temp: -5 to 50 C Humidity: 5 to 95% RH
Fan Type	4x 90mm fans - PFB0912DHE-6X39 (8000 RPM) - QFR0912UHE-6F78 (8300 RPM)

Four modules are required when the full complement of 10 blade units are installed into an enclosure. An LED on the back of a power supply will be amber when AC power is present and green when the power is on.

When installing only two power supplies in the enclosure, they should be installed in the lower rather than the upper power bays. This is to provide increased airflow across the memory modules within each blade module.

Both the 1400W and 2000W power supply modules require a 200-240V AC input and a C20 socket, which requires a power cord with a C19 connector (see "[Power Cord](#)" below for details).

Supermicro's high-efficiency blade system power supplies deliver continuous redundant power at 90%+ peak efficiency. Each power supply module includes a management module that monitors the power supplies and the power enclosure

Power Supply Failure

If a power supply or a fan in a power supply fails, the system management software will notify you of the situation. In either case, you will need to replace the power supply module with another identical one (part number: PWS-2K01-BR).



NOTE: Refer to www.supermicro/products/superblade for possible updates on part numbers.

Installing a Power Supply

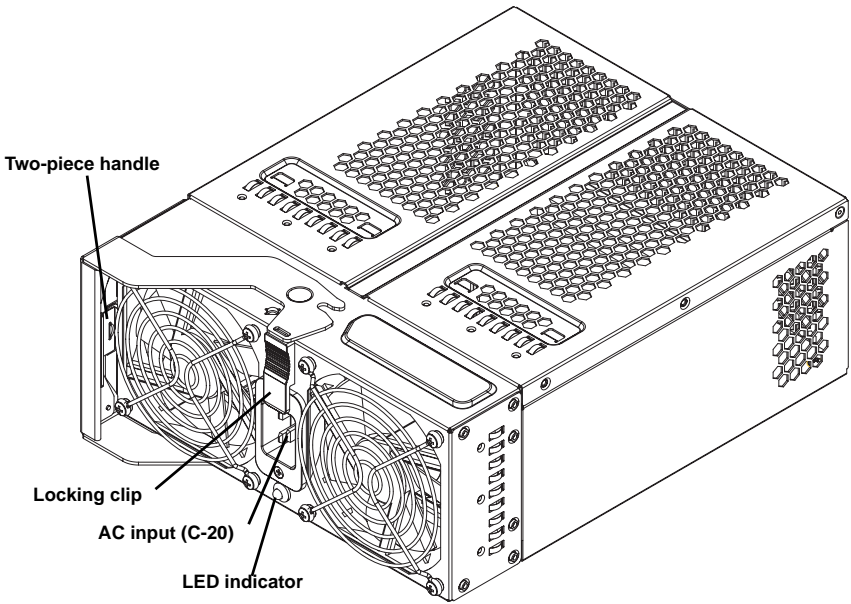
1. Insert a replacement unit into the empty power bay with the handle to the left.
2. Push unit all the way in until it is firmly seated.
3. Push the handle back into the closed position until it clicks into the locked position.
4. Move the locking clip away from the socket and reconnect the power cord.

Removing a Power Supply

First, make sure the power supply has been shut down. You can remove power from a power unit via your system management software.

1. Remove the power cord from the power supply unit.
2. Release the locking clip to unlock the power supply module (see [Figure 6-3](#)).

Figure 6-3. Power Supply Module



3. Pull out the handle and remove the unit: the two-piece handle locks into the closed position. To release the handle, squeeze together the two metal plates of the handle with your thumb and fingers and then pull out.

6-2 Power Supply Fans

Each power supply unit has four rear fans. These fans are not hot-swappable. If one fails, the power supply will continue to operate but you should replace the power supply unit at the earliest opportunity. If two or more fans fail, the power supply unit will shut down and the LED on the back will turn amber.

6-3 Power Components

Power components for your system's power supplies are shown below in [Figure 6-4](#) and described in [Table 6-3](#).

Figure 6-4. Power Components



Table 6-3. Power Components

Item	Name	Description
1	PDU	Power Distribution Unit (MCP-520-00036-0N)
2	Power Cable	Extension Cord (CBL-0223L)
3	AC Power Cord	See " Power Cord " below for details.

Power Cord

Each power supply module has its own power cord with a C19 type connector (IEC-60320-C19) to connect to the power supply (see [Figure 6-4](#) for a view of the power cord). The power cord connects to a C20 type socket (IEC-60320-C20) for AC power on the power supply module. The plastic locking clip that partially covers the socket was designed to prevent the power supply module from being removed with the power cord still connected.

For details on the required power cord for your country, see

<http://www.supermicro.com/products/superblade/powersupply/powercord.cfm>

Power Cable Tie and Clamp

A cable tie and clamp are available for both models of the blade power supplies. Using the cable tie (MCP-140-00015-0N), in conjunction with the cable clamp (MCP-140-00017-0N or MCP-140-00016-0N) and a small screw, allows you to secure the power cord to the power supply unit. This avoids it loosening and falling off the power supply due to any system vibration during its operation.



NOTE: There are two clamps available for use. Use the MCP-140-00017-0N clamp for all power cords that are **at or under** 9mm in diameter. Use the MCP-140-00016-0N clamp for all power cords **over** 9mm in diameter.

Figure 6-5 below provides an illustration of the tie and clamps with a power supply cord and power supply.

Figure 6-5. Power Cable Tie and Clamp Parts

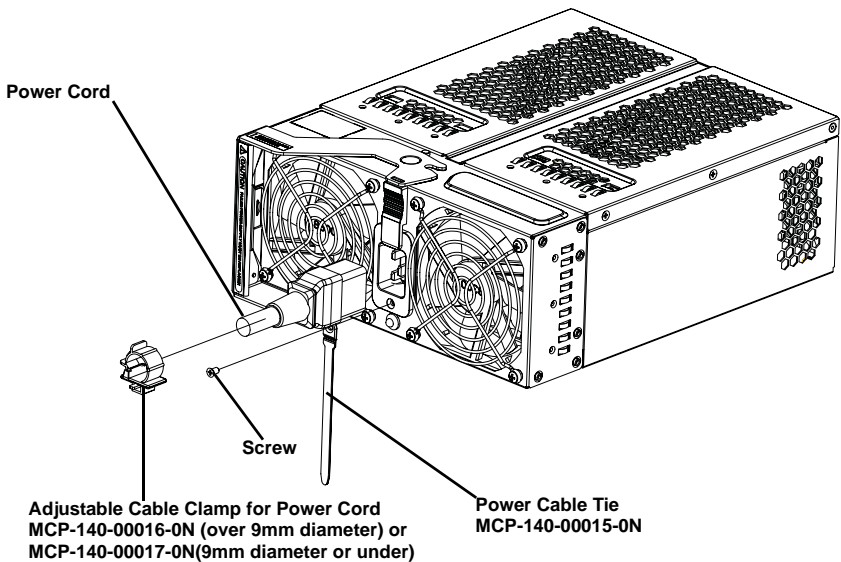
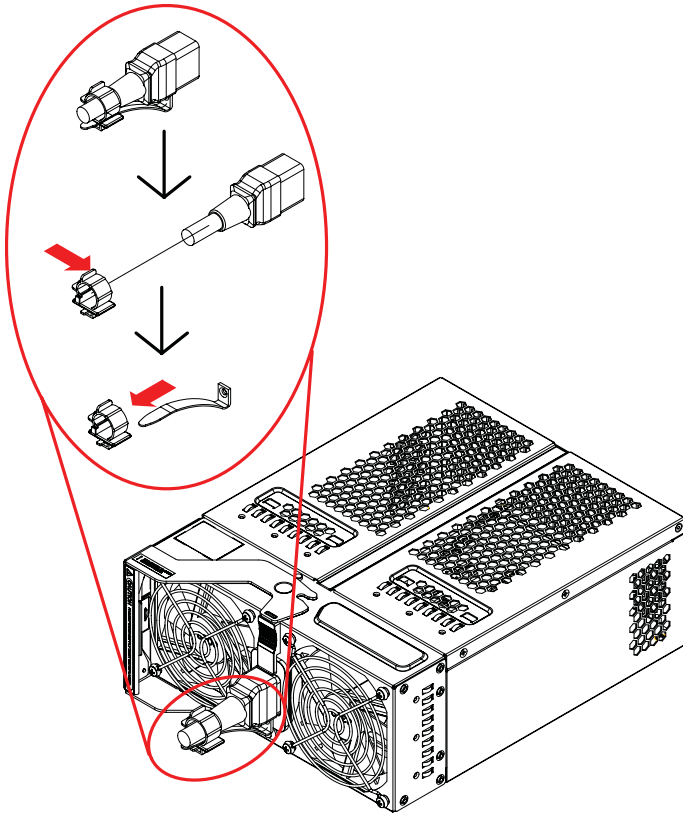


Figure 6-6 shows how to assemble the cable tie and clamp on the power cord. Simply place the clamp around the power cord and attach the cable tie to both the clamp and the power supply using a screw. This will secure the power cord to the power supply and keep it from dislodging during operation.

Figure 6-6. Power Cable Tie and Clamp Assembly



Notes

Chapter 7

Software and RAID

7-1 Installing the Operating System

An operating system (OS) must be installed on each blade module. Unlike most blade systems, blades with Microsoft Windows OS and blades with Linux OS can both occupy and operate within the same blade enclosure. Refer to the Supermicro web site for a complete list of supported operating systems.

There are several methods of installing an OS to the blade modules.

Installing with an External USB CD-ROM Drive

The most common method of installing the OS is with an external USB CD-ROM drive. Take the following steps to install the OS to a blade module:



WARNING: Installing the OS from an external CD-ROM drive may take several hours to complete.

1. Connect an SUV cable (Serial port/USB port/Video port cable) to the KVM connector on the front of the blade module. You will then need to attach a USB hub to the USB port on this cable to provide multiple USB ports.
2. Connect the external CD-ROM drive, a USB keyboard and a mouse to the USB hub. You will also need to connect a monitor to the video connector on the SUV cable. Turn on the blade module.
3. Insert the CD containing the OS into the CD-ROM drive.
4. Follow the prompts to begin the installation.

Installing via PXE Boot

PXE (Preboot Execution Environment) is used to boot a computer over a network. To install the OS via PXE, the following conditions must be met:

1. The PXE BOOT option in BIOS must be enabled.
2. A PXE server has been configured (this can be another blade in the system).
3. The PXE server must be connected over a network to the blade to be booted.
4. The blade has only non-partitioned/unformatted hard drives installed and no bootable devices attached to it.

Once these conditions are met, make sure the PXE server is running then turn on the blade you wish to boot and/or install the OS to. The BIOS in the blade will look at all

bootable devices and finding none will connect to the PXE server to begin the boot/install.

Installing via Virtual Media (Drive Redirection)

You can install the OS via Virtual Media through either the *IPMI* or the *Web-based Management utility*. With this method, the OS is installed from an ISO image that resides on another system/blade. Refer to [Chapter 8](#) for further details on the Virtual Media (CD-ROM or Drive Redirection) sections of these two utility programs.

7-2 Management Software

System management may be performed with either of two software packages: *IPMI* or a *Web-based Management utility*. Both are designed to provide an administrator with a comprehensive set of functions and monitored data to keep tabs on the system and perform management activities.

Refer to the [Chapter 8](#) for details on the various functions provided by these management programs.

7-3 Configuring and Setting up RAID

Each blade module that supports two or more hard drives may be used to create a RAID array. The procedures for doing this vary depending upon the blade model chosen for your SuperBlade system.

Please go to <http://www.supermicro.com/products/superblade/> to see how to configure and set up RAID on your blade module.

Chapter 8

Web-based Management Utility

The Web-based Management Utility is a web-based interface that consolidates and simplifies system management for Supermicro SuperBlade systems. The Web-based Management Utility aggregates and displays data from the SIMCM (the IPMI card designed for Supermicro's Chassis Management Module).

The Web-based Management Utility provides the following key management features:

- Enables IT administrators to view in-depth hardware configuration and status information using a single intuitive interface.
- Provides an OS-independent, remote graphical console.
- Allows remote users to map local media (floppy, CD-ROM, removable disks and hard drives) or ISO images on a shared network drive to a blade server.

Supported Browsers

The following browsers have been tested for use with the Web-based Management Utility. It is recommended that you use the most current revision of the browser you choose.

- Internet Explorer 7
- Firefox 2.0.0.7
- Netscape 9.03b

8-1 Network Connection/Login

To log into the Web-based Management Utility:

1. Launch a web browser.
2. In the address field of the browser, enter the IP address that you assigned to the Chassis Management Module and hit the <ENTER> key.
3. When the browser makes contact with Supermicro's Chassis Management Module, enter your *username* and *password*, then click LOGIN.
4. The WEB-BASED MANAGEMENT UTILITY HOME PAGE will then display as shown in [Figure 8-1](#).

Address Defaults

[Table 8-1](#) shows the default addresses that are initially set for the CMM. Afterwards, you can change these values within the program (see "[Device Settings](#)" on [page 8-26](#)).

Table 8-1. Address Defaults

Default	Description
Default IP Address	192.168.100.100
Default Gateway Address	0.0.0.0
Default Subnet Mask	255.255.255.0
Default username	ADMIN
Default password	ADMIN

8-2 Home Page

Figure 8-1 and Table 8-2 respectively display the WEB-BASED MANAGEMENT UTILITY HOME PAGE and its controls.

Figure 8-1. Home Page

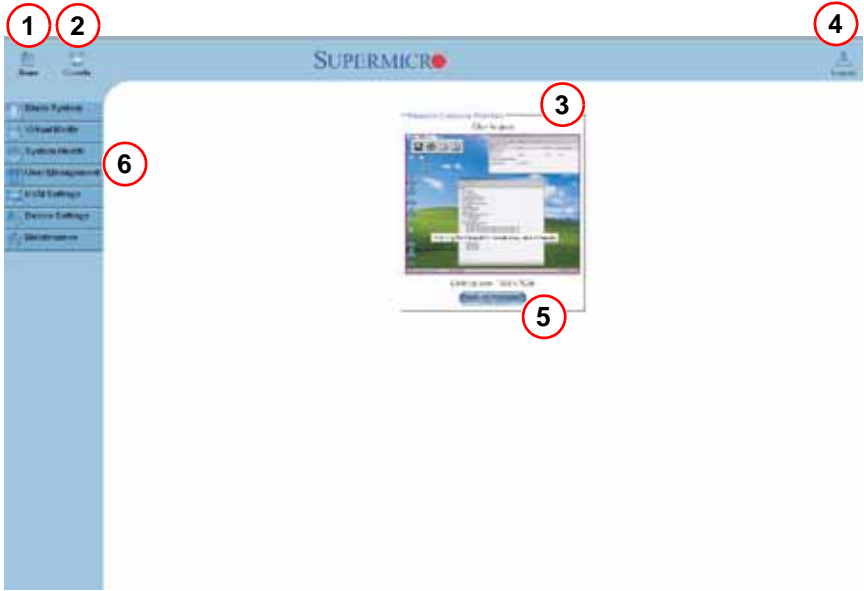


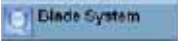






Table 8-2. Home Page Controls

Item	Description
1	Home: Click this icon to return to the Home Page.
2	Console: Click this icon to open the Remote Console Screen. (KVM must first be initialized either with the KVM button or via management software).
3	Remote Console Screen: The active screen from the remote console is displayed here. Clicking on this window also accesses the remote console.
4	Logout: Click on this icon to log out.
5	Refresh: Click on this icon to refresh the remote console preview screen.
6	Main Menu Icons: Used to initiate the various functions in the Web-based Management Utility.

8-3 Main Menu Icons

The icons below in [Table 8-3](#) cover the main functions of IPMI. Clicking on an icon will reveal a submenu of related functions.

Table 8-3. Main Menu Icons

Icon	Description
 Blade System	Click this icon for remote access and management of individual blade modules.
 Virtual Media	Click on this icon to use virtual remote media (storage) devices.
 System Health	Click on this icon to view the system event log and manage the health of remote systems.
 User Management	Click on this icon for User Management.
 KVM Settings	Click on this icon to configure keyboard, video and mouse settings.
 Device Settings	Click on this icon to configure device settings.
 Maintenance	Click on this icon to get information on the SIMCM, update its firmware, check the event log and reset the unit.

Blade System

Clicking the BLADE SYSTEM icon allows you to access the following screens through its sub-menus:

- [Blade Screen](#)
- [Power Supply](#)
- [Gigabit Switch](#)
- [CMM](#)
- [KVM Console](#)
- [SQL Console](#)

Blade Screen

The first BLADE option in the BLADE SYSTEM submenu allows you to check the status of all the blade modules in the system including power status, KVM status, UID status, error status and management. The command icons below the blade status list allows you to perform various functions, as shown in [Figure 8-2](#) and described in [Table 8-4](#)

To perform a function, first click the box(es) next to the blade(s) you wish to issue a command to and then click the command icon. You can also click on the individual blades listed for a remote console.

Figure 8-2. Blade Status Screen

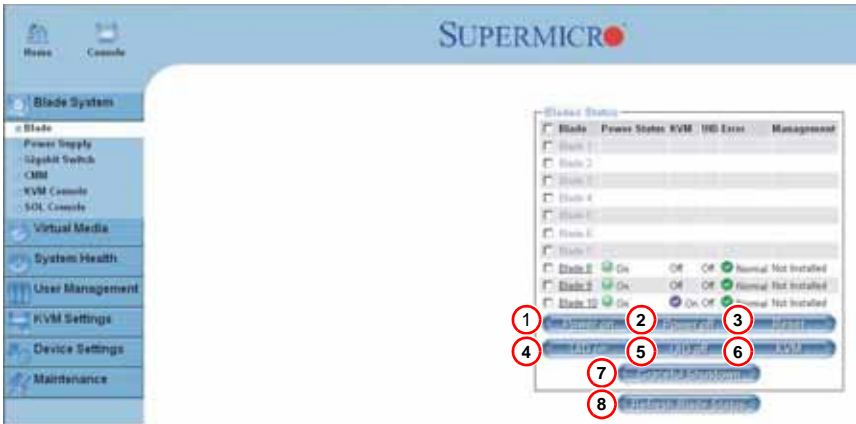


Table 8-4. Blade Status Screen Controls

Item	Name	Description
1	Power On	Click to apply power to (power up) a selected blade module.
2	Power Off	Click to remove power from a selected blade module.
3	Reset	Click this icon to reset a selected blade module.
4	UID On	Click this icon to turn on the UID LED of a selected blade module.
5	UID Off	Click this icon to turn off the UID LED of a selected blade module.
6	KVM	Click on this icon to initiate Remote KVM over IP and remotely operate a selected blade module.
7	Graceful Shutdown	Click to send a selected blade module into an S5 sleep state.
8	Refresh Blade Status	Click to refresh the screen and update the status of the blade modules shown.

Power Supply

Click on POWER SUPPLY to reveal the POWER SUPPLY STATUS screen (Figure 8-3). The POWER SUPPLY option in the BLADE SYSTEM submenu allows you to check the status of all the power supplies in the system you are accessing. Power status (on or off), temperature, fan rpm, wattage, firmware version and FRU version are all shown in the power supply status list. In addition, the commands listed in Table 8-5 may be issued to the power supplies.

To perform a function, first click the box(es) next to the power supply(s) you wish to issue a command to and then click the command icon.

Figure 8-3. Power Supply Status Screen



Table 8-5. Power Supply Status Screen Controls

Item	Name	Description
1	Power On	Click this to power up a selected power supply.
2	Power Off	Click this to shut down a selected power supply.
3	Refresh Power Supply Status	Click to refresh the screen and update the status of the power supplies shown.
4	Power Supply Fan Speed Control	<p>You may alter the speed of the power supply fans by clicking one of these icons. Set to minimum speed by clicking the icon numbered "1" and to maximum speed by clicking the icon numbered "4". The icons numbered "2" and "3" are for incremental increases between the minimum and maximum settings.</p> <p>After changing the fan speed, you should see the fan rpm change in the status screen. Settings affect all fans simultaneously, you cannot control the speed of individual fans.</p>

Gigabit Switch

Click on GIGABIT SWITCH to reveal the GIGABIT SWITCH STATUS screen (Figure 8-4). The GIGABIT SWITCH option in the BLADE SYSTEM submenu allows you to check the status of all the GbE modules in the system you are accessing. Power status (on or off), voltage levels, temperature, error status and initialization status are all shown in the main screen (see Table 8-6). In addition, the commands listed below may be issued to the GbE module.

To perform a function, first click the box(es) next to the GbE module(s) you wish to issue a command to and then click the command icon.

Figure 8-4. Gigabit Switch Status Screen



Table 8-6. Gigabit Switch Status Screen Controls

Item	Name	Description
1	Power On	Click this to power up a selected GbE module.
2	Power Off	Click this to shut down a selected GbE module.
3	Reset	Click this icon to reset a GbE module to its default settings.
4	Refresh Power Supply Status	Click to refresh the screen and update the status of the power supplies shown.
5	Gigabit Switch Links	Click on a switch listed here to open another window that allows you to manage and configure that GbE switch.



NOTE: Initially, you must manually enter the IP address for each GbE switch to gain access to it. Each IP address should be unique when there are multiple GbE switches on the same network segment.

After gaining access to the GbE switch(es), you can use the reset button to reset their configurations to the default settings. The reset button will reset all GbE switch configurations, including IP address and so on.

CMM

Click on CMM to reveal the CMM STATUS screen (Figure 8-5). The CMM option in the BLADE SYSTEM submenu allows you to check the status of all the CMM modules in the system you are accessing. Master/Slave status, operating status, firmware version and firmware tag status are all shown in the main screen.

There are three commands you may give on this screen, as described below in Table 8-7.

Figure 8-5. CMM Status Screen



Table 8-7. CMM Status Screen Controls

Item	Name	Description
1	Refresh CMM Status	Click to refresh the screen and update the status of the CMM modules shown.
2	Get Time	Click this button to get the time as set in the CMM module.
3	Set Time	Click this button to set the time as set in the CMM module. You will first need to enter a time in the window in the window.

KVM Console

Click on KVM CONSOLE to activate the Remote KVM function. The KVM CONSOLE option allows the local host to interact with a remote server through the REMOTE CONSOLE INTERFACE screen (Figure 8-6), where you can share files stored in the local drive with a user connected to the remote server, download data from a local drive to the remote server, issue commands to manage the remote server or allow the remote server be controlled and managed by a local user logged in to the remote server (see Table 8-8 for a list of controls). This function provides a full spectrum of remote console interaction and management.

Figure 8-6. Remote Console Interface Screen

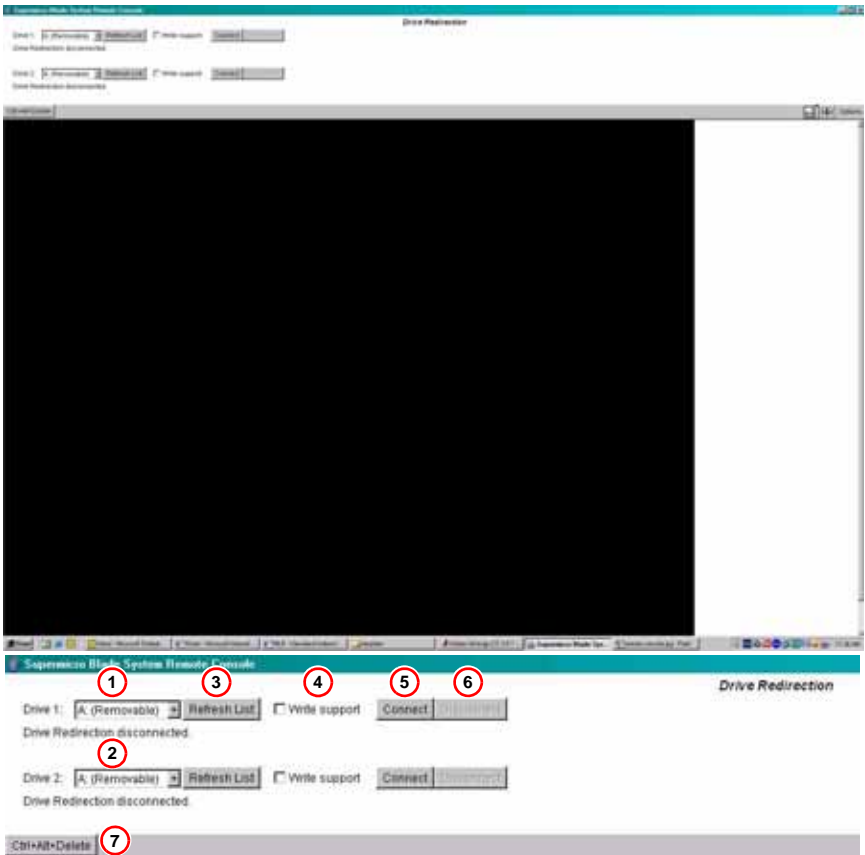


Table 8-8. Remote Console Interface Screen Controls

Item	Name	Description
1	Local Drive List	These two windows display a list of local drives available for remote access. Select from the list a local drive that you want to make accessible for a remote server.
2	Local Drive List	Same as above.
3	Refresh	Click this button to refresh the local drive list.
4	Write Support	Check this button to allow the remote operating system to have write access to the drive that you have selected. This function allows a user to alter, overwrite, erase and destroy data stored in the drive selected and therefore should only be used on drives with non-critical data. When WRITE SUPPORT is checked, a warning message will display. Read the warning message carefully before enabling this function.
5	Connect	Click this button to make the drive you have selected accessible for remote console interaction. Once you have clicked CONNECT, users logged into remote servers will have access to the local drive that you have selected.
6	Disconnect	Click this button to cancel the connection established between a local drive and a remote server. Once you click this button, the drive you have selected will not be accessible for remote console interface.
7	Sending Commands	This functions allows the user to issue a pre-defined command to a remote server for execution.

To use this function, you need to click the hot keys displayed on the upper right corner of the screen.



NOTE: Hot keys are commands that have been pre-defined and pre-stored in a remote consoles.

Click the CTRL+ALT+DELETE button to send the command CTRL+ALT+DELETE to the remote server for execution.

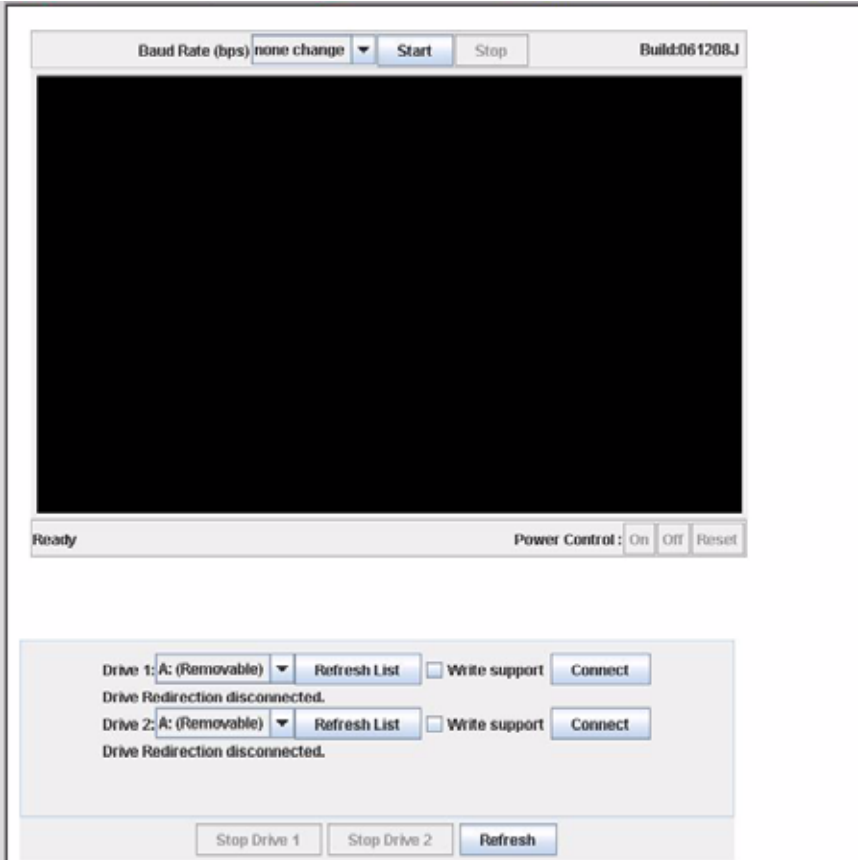
Once you have clicked on the button, it displays a message asking you to confirm if you really want to send CTRL+ALT+DELETE. Click YES to confirm or click CANCEL to cancel sending the command for remote execution.

SOL Console

Click on SOL CONSOLE to activate the SOL (Serial-over-LAN) function. The SOL CONSOLE option functions just like the KVM CONSOLE option, but employs Serial-over-LAN instead of KVM as the interface.

Refer to the "[KVM Console](#)" on page 8-9 functions above for descriptions of the same functions that are also available in the SOL Console.

Figure 8-7. SOL Console Screen



Virtual Media

Clicking the VIRTUAL MEDIA icon allows you to access the following screens through its sub-menus:

- [Floppy Disk](#)
- [CD-ROM](#)
- [Drive Redirection](#)
- [Options](#)

Floppy Disk

The FLOPPY DISK option in the VIRTUAL MEDIA submenu allows you to emulate a floppy drive in the host system to upload images to a remote blade module. The FLOPPY DISK STATUS screen (Figure 8-8) that appears and its controls (Table 8-9) are shown below.

Figure 8-8. Floppy Disk Status Screen

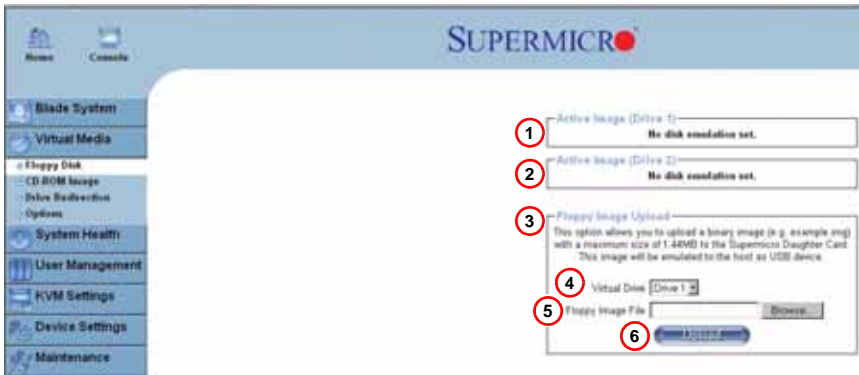


Table 8-9. Floppy Disk Status Screen Controls

Item	Name	Description
1	Active Image (Drive1)	This window displays the data that has been uploaded to drive 1 of the remote host.
2	Active Image (Drive2)	This window displays the data that has been uploaded to drive 2 of the remote host.
3	Floppy Image Upload	This option allows the user to upload the floppy image located in the remote host as "floppy". The floppy image uploaded should be in binary format with a maximum size of 1.44 MB. It will be loaded to the Supermicro SIMCM card and will be emulated to the host as a USB device.
4	Virtual Drive	Select a drive in the remote host as the destination drive to upload your image data to.
5	Floppy Image File	Click "Browse" to preview and select the files that you wish to upload to the selected host drive.
6	Upload	Once the correct file name appears in the box, click here to upload the floppy image to the drive specified in the remote host.

CD-ROM

The CD-ROM IMAGE option allows you to emulate a CD-ROM drive in the host system to upload images to a remote blade module. The CD-ROM IMAGE screen (Figure 8-9) and its controls (Table 8-10) are shown below.

Figure 8-9. CD-ROM Image Screen



Table 8-10. CD-ROM Image Screen Controls

Item	Name	Description
1	Active Image (Drive1)	This window displays the file name of the data currently active in host Drive 1.
2	Active Image (Drive2)	This window displays the file name of the data currently active in host Drive 2.
3	Image on Windows Share	This allows the user to decide how to share the CD-ROM ISO image file with users in the remote host.
4	Virtual Drive	Specify the drive that you want to share your data with in the remote host.
5	Share Host	Key in the IP Address or the name of the system you wish to share data with via Windows Share.
6	Share Name	Key in the name of the shared folder you wish to share data with in the remote host.
7	Path to Image	Key in the location of source files that you wish to share via Windows Share.
8	User/Password (Optional)	Key in the Username and password for the person to access the data that you want to share and click "Set" to enter your selections.

Drive Redirection

The DRIVE REDIRECTION option in the VIRTUAL MEDIA submenu allows you to make local drives accessible to remote users via console redirection. The DRIVE REDIRECTIONS screen (Figure 8-10) and its controls (Table 8-11) are shown below.

Figure 8-10. Drive Redirections Screen

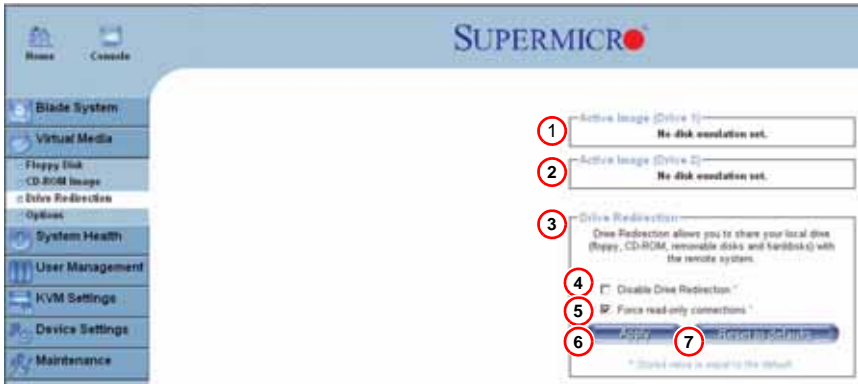


Table 8-11. Drive Redirection Screen Controls

Item	Name	Description
1	Active Image (Drive1)	This window displays the file name of the data currently active in host drive 1.
2	Active Image (Drive2)	This window displays the file name of the data currently active in host drive 2.
3	Drive Redirection	Use this window to configure DRIVE REDIRECTION settings.
4	Disable Drive Redirection	Check the box to disable Drive Redirection. Once this function is disabled, local drives will not be accessible for other remote systems users.
5	Force Read Only	Check this box to allow the data stored in local drives to be read by a remote system, but not overwritten (for data integrity and system security purposes).
6	Apply	After configuring your settings, click "Apply" to initiate drive redirection with the parameters you've set.
7	Reset to Defaults	You can also key in your own setting values and re-set these values as "default" by clicking on this icon to reset the defaults.

Options

The OPTIONS selection in the VIRTUAL MEDIA submenu allows you to configure Virtual Media Options. The OPTIONS screen (Figure 8-11) and its controls (Table 8-12) are shown below.

Figure 8-11. Options Screen



Table 8-12. Options Screen Controls

Item	Name	Description
1	Virtual Media Options	Use this option to disable or enable USB mass storage in the remote host. Checking this box prevents data stored in a local drive from being accessed or uploaded by a remote system. The default setting is enabled (unchecked).
2	Apply	Once you've checked the box, click the APPLY icon to initiate.
3	Reset to Defaults	Click this icon if you want to reset the defaults for the Virtual Media Options.

System Health

Clicking the SYSTEM HEALTH icon allows you to access the following screens through its sub-menus:

- [System Event Log](#)
- [Alert Settings](#)

System Event Log

The SYSTEM EVENT LOG option in the SYSTEM HEALTH submenu allows you to view and clear the contents of the system event log for a remote system. The SYSTEM EVENT LOG screen that appears ([Figure 8-12](#)) and its controls ([Table 8-13](#)) are shown below.

Figure 8-12. System Event Log Screen

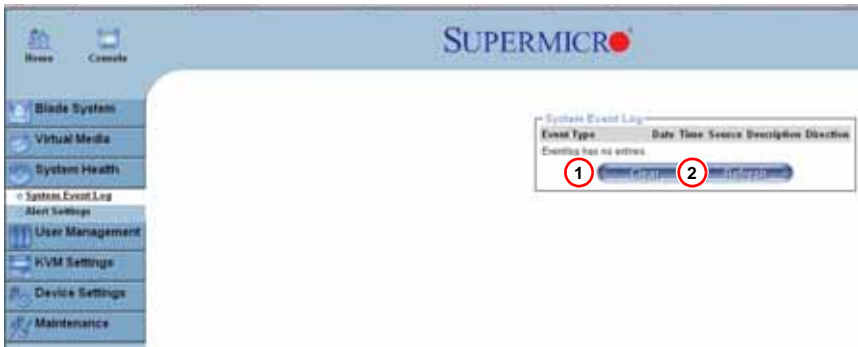


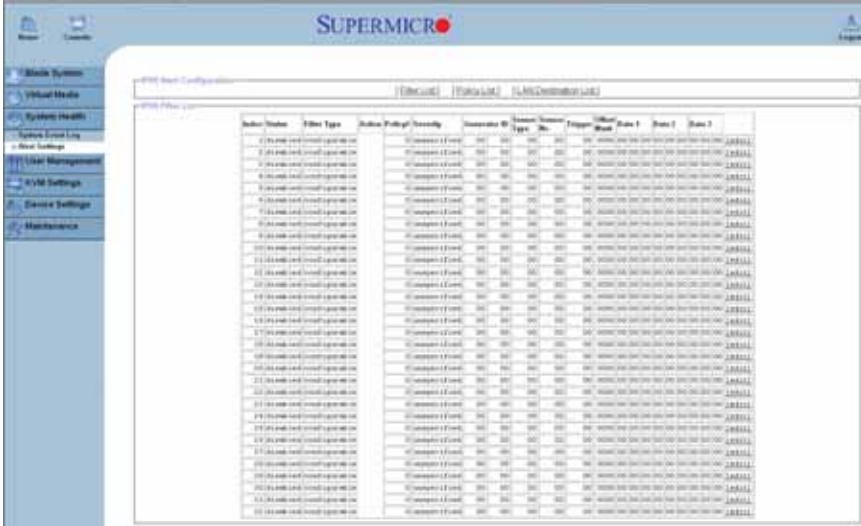
Table 8-13. System Event Log Screen Controls

Item	Name	Description
1	Clear	Click on this icon to clear the event log (delete all entries).
2	Refresh	Click on this icon to refresh the event log.

Alert Settings

The ALERT SETTINGS in the SYSTEM HEALTH submenu allow you to set the parameters to be met for a system to issue an alert. Click on the three headings (filter list, policy list and LAN destination list) at the top of the list in the IPMI ALERT CONFIGURATION screen (Figure 8-13) to sort between the three categories.

Figure 8-13. IPMI Alert Configuration Screen



User Management

Clicking the USER MANAGEMENT icon allows you to access the following screens through its sub-menus:

- [Change Password](#)
- [Users & Groups](#)
- [Permissions](#)

Change Password

The CHANGE PASSWORDS screen ([Figure 8-14](#)) is where you can change the password used to access the Web-based Management Utility. Its controls are shown in [Table 8-14](#).

Figure 8-14. Change Passwords Screen



Table 8-14. Change Password Screen Controls

Item	Name	Description
1	New Password	Type your new password in the window.
2	Confirm New Password	Type your new password in this second window to confirm.
3	Apply	Click this icon to apply the changes you made.

Users & Groups

The USERS & GROUPS screen (Figure 8-15) is where you specify and manage groups and users, which helps you manage the remote systems you are managing. Its controls are shown in Table 8-15.

Figure 8-15. Users and Groups Screen

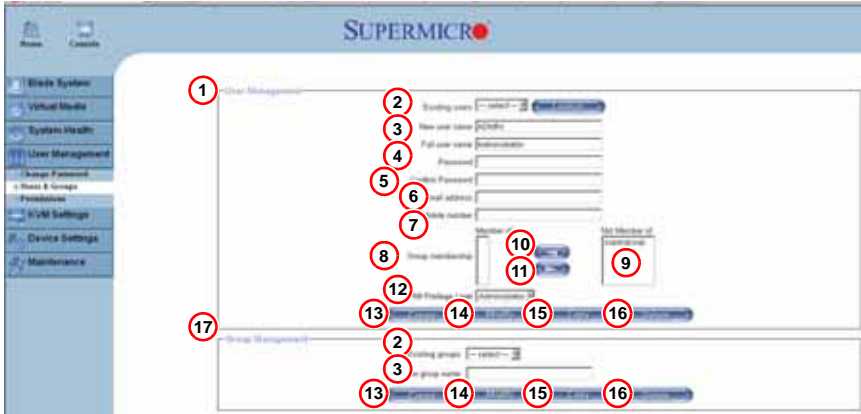


Table 8-15. Users and Groups Screen Controls

Item	Name	Description
1	User Management Section	This window displays the user's information.
2	Existing users	Select an existing user for information updates. Once a user is selected, click on the Lookup icon on the right to view user information.
3	New user name	Type in a new user name in this field.
4	Full user name	Type in the user's full name in this field.
5	Password and Confirm Password	Type the user's password in the window and then retype the password in the next window to confirm. The password must at least four characters in length.
6	Email Address	Type in the user's email address in this window (optional).
7	Mobile Phone	Type in the user's mobile phone number (optional).
8	Group Membership	This field indicates the group that the user belongs to. To select a group, click on the group name in the "Not Member Of" window (9) select it, then click on the backwards arrow (10) to enter the group name in the Group Membership field (8). Reverse the procedure to remove the user from a group.
9	Not Member Of Window	Select a member in this window for assigning to group membership.
10	Backwards Arrow	Use this arrow to add a member to a group membership.
11	Forwards Arrow	Use this arrow to remove a member from group membership.

Table 8-15. Users and Groups Screen Controls (Continued)

Item	Name	Description
12	IPMI Privilege Level	Click on the pull-down arrow to activate the Privilege Selection menu. The IPMI Privilege Level contains five categories: No Access, User, Operator, Administrator and OEM.
13	Create	Click this icon to create a new user or group in the User/Group Management fields.
14	Modify	Click this icon to modify a user's or group information in the User/Group Management fields.
15	Copy	<p>Click on this button to copy a user's or group information in the User/Group Management fields.</p> <p>Copy User: select an existing user from the selection box. Enter a new user name in the "New User Name" window. Click the "Copy" icon and a new user with the name you typed in will be created. The properties of the selected user will be copied to the new user.</p> <p>Copy Group: select an existing group from the selection box. Enter a new group name in the "New Group Name" window. Click the "Copy" icon and a new group with the name you typed in will be created. The properties of the selected group will be copied to the new group.</p>
16	Delete	Click on this button to delete a user's or group information in the User/Group Management fields.
17	Group Management	This window allows you to enter group information for better user management. Create and modify groups they same way you do for users.

Permissions

You can use the PERMISSIONS option to grant and deny access to various IPMI functions in the PERMISSIONS screen (Figure 8-16) using its controls (Table 8-16).

Figure 8-16. Permissions Screen



Table 8-16. Permissions Screen Controls

Item	Name	Description
1	Show Permissions for User/Group	Click on the pull-down arrow to activate the user/group permissions selection menu.
2	Update	Click this icon to update the permissions information.
3	Effective Permissions	This field indicates the actual permissions a user or group has.
4	User Permissions	This field indicates the actual permissions a user has.
5	Inherited Group Permission	This field indicates the permissions a user has due to the fact that they belong to a certain group.

KVM Settings

Clicking the KVM Settings icon allows you to access the following screens through its sub-menus:

- [User Console](#)
- [Keyboard/Mouse](#)

User Console

Selecting the USER CONSOLE option in the KVM SETTINGS submenu brings up the KVM SETTINGS screen ([Figure 8-17](#)). Use this screen to set the remote console settings to specific users. This screen has several sections:

- **Transmission Encoding:** This field allows you to specify how the video data is to be transmitted between the local system and the remote host.
- **Remote Console Type:** This field allows you to decide which remote console viewer to use.
- **Miscellaneous Remote Console Settings:** This field allows you to specify the following Remote Console Settings.
- **Mouse Hotkey:** This option allows you to use a hotkey combination to specify either mouse synchronization mode or the single mouse mode.
- **Remote Console Button Keys:** This field allows you to define button keys for the remote host. The button keys allow simulating keystrokes on a remote host or issuing commands to a remote system. The button keys are needed when you have a missing key or when you want to prevent interference caused to the local system.



NOTE: After a remote console button key is set, it will appear on the right upper corner of the remote monitor screen as shown in [Figure 8-17](#).

For further detailed instructions in creating button keys, please click on the [CLICK HERE FOR HELP](#) link.

The controls found in the above sections are shown and described in detail in [Table 8-17](#).

Figure 8-17. KVM Settings Screen

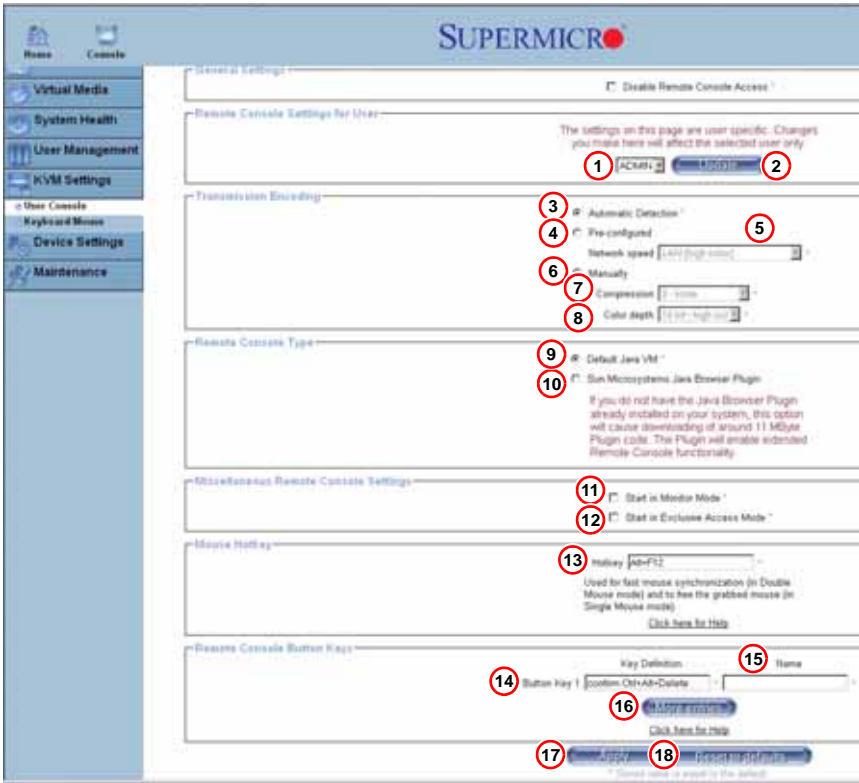


Table 8-17. KVM Settings Screen Controls

Item	Name	Description
1	User Selection	This field allows you to decide which group the user belongs to. Click on the arrow on the right to activate the pull-down menu and highlight the name of the group to select it.
2	Update	Once you've selected the group name, click on UPDATE to save the selections.
3	Automatic Detection	Select this option to allow the OS to automatically detect the networking configuration settings (such as the bandwidth of the connection line) and transmit data accordingly.
4	Pre-configured	This item allows the user to select the data transmission settings from a pre-defined options list. The pre-configured settings will provide the best results because the compression and color depth settings will be adjusted for optimization based on the network speed indicated.
5	Network speed	Once you've selected the PRE-CONFIGURED option above, you then can select a desired network speed setting from the pull-down menu by clicking on the arrow.

Table 8-17. KVM Settings Screen Controls (Continued)

Item	Name	Description
6	Manually	Select a desired network speed setting from the pull-down menu by clicking on the arrow. This item allows the user to adjust both compression and color depth settings individually.
7	Compression	Data signal transmission is compressed to save bandwidth. High compression rates will slow down network interfacing and should not be used when several users are connected to the network.
8	Color Depth	Click on the arrow to select either 16 bit-high color or 8-bit 256 color. The standard color depth is 16-bit high color and is recommended for compression level 0. For typical desktop interfaces, 8-bit 256 color is recommended for faster data transmission.
9	Default Java VM (JVM)	Select this option to use the default Java Virtual Machine of your web browser. This can be the Microsoft JVM for Internet Explorer or the Sun JVM depending on the configuration of your browser.
10	Sun Microsystems Java Browser Plugin	Select this option when the JVM used to run the code for the Remote Console is a Java Applet. If using this function for the first time and the appropriate Java plugin is not yet installed in your system, you may download and install it automatically. To download and install, you need to check YES in the dialog boxes. Downloading Sun's JVM will allow you to use a stable and identical JVM across different platforms. NOTE: If your internet connection is slow, please pre-install JVM on your administration system.
11	Start in Monitor Mode	Check this box to enable Start in Monitor Mode , which allows data to be displayed on the remote monitor as soon as the Remote Console is activated. NOTE: The data displayed in the remote monitor is ready-only.
12	Start in Exclusive Access Mode	Check this box to enable the exclusive access mode immediately upon Remote Console startup, which will force all other users connected to the network to close. No other users can open the Remote Console until you disable this function or log off.
13	Hotkey	Enter a hotkey combination in the box to specify either mouse synchronization mode or the single mouse mode.
14	Button Keys	Enter the syntax of a button key in the box. For detailed instructions on creating button keys, please click on the "Click here for Help" link.
15	Name	Type in the name of a button key in the box. For detailed instructions on creating button keys, please click on the CLICK HERE FOR HELP link.
16	More Entries	Click on this icon to create more button keys.
17	Apply	Click this icon to apply the selections you made.
18	Reset to Defaults	Click this icon if you want to reset the defaults for the Remote Console button keys.

Keyboard/Mouse

Selecting the KEYBOARD/MOUSE option in the KVM SETTINGS submenu allows you to specify the parameters for the keyboard and mouse on the KEYBOARD/MOUSE screen (Figure 8-18). The controls for this screen are shown and explained in Table 8-18.

Figure 8-18. Keyboard/Mouse Screen

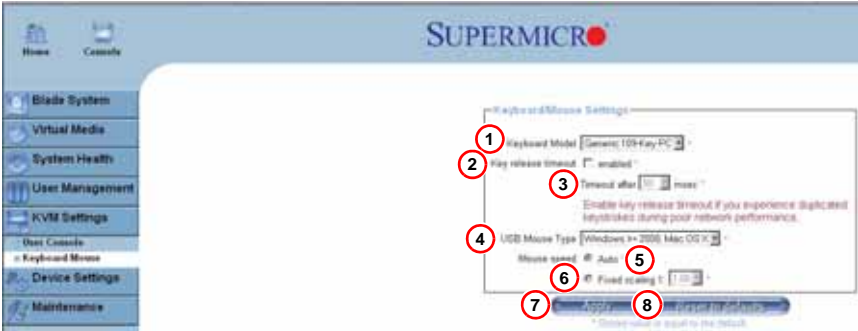


Table 8-18. Keyboard/Mouse Screen Controls

Item	Name	Description
1	Keyboard Model	Click the arrow for the pull-down menu to specify the type of keyboard.
2	Key Release Timeout	Check this box to enable the function of KEY RELEASE TIMEOUT, which sets the time limit for a key to be pressed by the user.
3	Timeout after ___ msec	If the KEY RELEASE TIMEOUT checkbox has been enabled, click on the arrow to select the timeout setting in the pull-down menu.
4	USB Mouse Type	For a USB mouse to function properly, please select the correct operating system for your system from the pull-down menu by clicking on the arrow.
5	Mouse Speed-Auto	Click the checkbox to allow your system to automatically set your mouse speed.
6	Fixed Scaling	You can also check the FIXED SCALING checkbox and manually set the mouse speed with the pull-down menu.
7	Apply	Click on this icon to enter your selections.
8	Reset to defaults	Click this icon to cancel your selections and use the default values that have been pre-set by the manufacturer.

Device Settings

Clicking the DEVICE SETTINGS icon allows you to access the following screens through its sub-menus:

- [Network](#)
- [Dynamic DNS](#)
- [Security](#)
- [Date/Time](#)
- [Event Log](#)
- [SNMP Settings](#)

Network

Clicking the NETWORK option in the DEVICE SETTINGS submenu brings up the NETWORK screen (Figure 8-19). Use the below fields in the screen to specify network parameters.

- **Network Miscellaneous Setting:** This field allows the user to configure miscellaneous network settings.
- **LAN Interface Settings:** This field allows the user to configure LAN Interface settings.

The controls in these fields are shown and detailed in [Table 8-19](#).

Figure 8-19. Network Screen

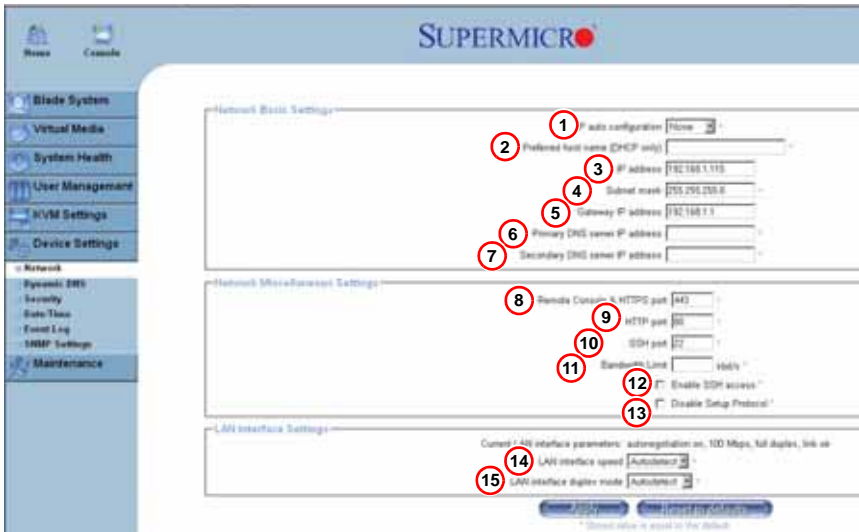


Table 8-19. Network Screen Controls

Item	Name	Description
1	IP Auto Configuration	Click on the pull-down menu to select a desired item from the list. The options are NONE, DHCP, and BOOTP.
2	Preferred Host Name (DHCP only)	Enter a preferred host name here.
3	IP Address	Enter the IP address for the remote host here.
4	Subnet Mask	Enter the subnet mask of the local network here.
5	Gateway IP Address	Enter the local network router's IP address here to provide accessibility for users that are not connected to the local network.
6	Primary DNS Server IP Address	Enter the IP address of the Primary Domain Name Server here.
7	Secondary DNS Server IP Address	Enter the IP address of the Secondary Domain Name Server in the box. It will be used when the Primary DNS Server cannot be contacted.
8	Remote Console & HTTPS Port	Enter the port numbers the remote host and the HTTP server are listening. If a number is not entered in the box, the default value will be used.
9	HTTP Port	Enter the port number the of the HTTP server. If a number is not entered in the box, the default value will be used.
10	SSH Port	Enter the port number of the SSH server. If a number is not entered in the box, the default value will be used.
11	Bandwidth Limit	Enter the maximum bandwidth value for network interfacing. The value should be in Kbits per second.
12	Enable SSH Access	Click this box to enable SSH access.
13	Disable Setup Protocol	Check this box to disable the setup protocol function of the SIMBL card.
14	LAN Interface Speed	Click on the arrow on the right to select a desired LAN interface speed from the pull-down menu. The options are Auto-detect, 10 Mbps or 100 Mbps. If Auto-detect is selected, the optimized speed will be set based on the system configurations detected by the OS.
15	LAN Interface Duplex Mode	Click on the arrow on the right to select a desired LAN interface duplex mode from the pull-down menu. The options are AUTO-DETECT, HALF DUPLEX and FULL DUPLEX. If Auto-detect is selected, the LAN INTERFACE DUPLEX MODE will be set to the optimized setting based on the system configurations detected by the OS.

Dynamic DNS

Selecting the DYNAMIC DNS option from the DEVICE SETTINGS submenu brings up the DYNAMIC DNS SETTINGS screen (Figure 8-20). Use this screen to configure Dynamic DNS settings. Controls for this screen are shown and detailed in Table 8-20.

Figure 8-20. Dynamic DNS Settings Screen



Table 8-20. Dynamic DNS Settings Screen Controls

Item	Name	Description
1	Enable Dynamic DNS	Check this box to enable Dynamic DNS.
2	Dynamic DNS Server Link	Click the www.dyndns.org link to access the DynDNS web site. This is the server name where the DDNS Service is registered.
3	DNS System	If Dynamic DNS is enabled, you can select either CUSTOM or DYNAMIC from the pull-down menu. Select CUSTOM to use your own system as the DNS server. Select DYNAMIC to use the pre-configured Dynamic DNS as your server.
4	Hostname	Enter the name you want to use for the remote host server.
5	Username	Enter the username for the remote host user.
6	Password	Enter the password for the remote host user.
7	Check time (HH:MM)	Enter the time the SIMCM card first registers with the DNS server in the HH:MM format (such as: 07:25 or 19:30).
8	Check Interval	Enter the time interval for the IPMI to report to the Dynamic DNS again.
9	Delete Saved External IP Address	Click this icon to delete the IP address for an external system that has been previously entered and saved.

Security

Selecting the SECURITY option from the DEVICE SETTINGS submenu brings up the SECURITY screen (Figure 8-21). Use this screen to configure the Security settings. Controls for this screen are shown and detailed in Table 8-21.

- **Encryption Settings:** This field allows you to configure encryption settings.
- **IP Access Control:** This section allows you to configure the IP Access Control settings listed below.
- **User Blocking:** This field allows you to set the user blocking conditions.

Figure 8-21. Security Screen

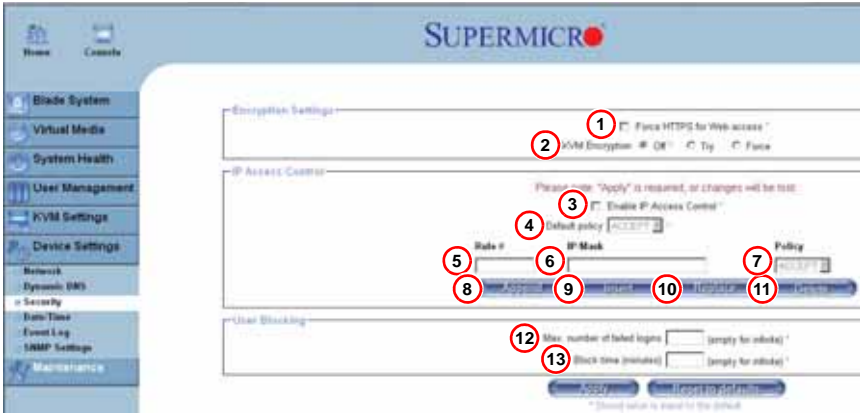


Table 8-21. Security Screen Controls

Item	Name	Description
1	Force HTTPS for Web Access	Check this box to enable Force HTTPS for Web Access. If enabled, you will need to use an HTTPS connection to access the web.
2	KVM Encryption	This option allows you to configure the encryption of the RFB protocol. RFB is used by the remote host to transmit video data displayed in the host monitor to the local administrator machine and to transmit keyboard and mouse data from the local administrator machine back to the remote host. If set to OFF, no encryption will be used. If set to TRY, the applet (JVM of the remote host) will attempt to make an encrypted connection. In this case, when a connection cannot be established, an unencrypted connection will be used. If set to FORCE, the applet will make an encrypted connection. In this case, an error will be reported if no connection is made.
3	Enable IP Access Control	Check this box to enable IP Access Control. This function is used to limit user access to the network by identifying them by their IP address (available to the LAN interface only.)

Table 8-21. Security Screen Controls (Continued)

Item	Name	Description
4	Default Policy	<p>When IP ACCESS CONTROL is enabled, you can select either Accept or Drop from this pull-down menu to either allow or deny access according to pre-defined rules.</p> <p>NOTE: If set to DROP and you do not have a set of rules that will accept the Internet connection, then an Internet connection over the LAN is impossible. In this case, you need to change your security settings via modem or by disabling the IP ACCESS CONTROL.</p>
5	Rule#	<p>Enter a rule number in the box for a command (or commands) that will be used by the IP ACCESS CONTROL.</p>
6	IP/Mask	<p>Enter the IP address or an IP address range for which the command(s) will be applied.</p>
7	Policy	<p>This item instructs the IPMI what to do with the matching packages.</p> <p>NOTE: The sequence or the order of the rules is important; rules are checked in ascending order until one matches. All rules below the matching one will be ignored. The default policy applies if no matching rules are found.</p>
8	Append	<p>Select this option to add IP Address/Mask, rules or commands to the existing ones.</p>
9	Insert	<p>Select this option to insert IP Address/Mask, rules or commands to the existing ones.</p>
10	Replace	<p>Select this option to replace an old IP Address/Mask, rule or command with a new one.</p>
11	Delete	<p>Select this option to delete (a part of) an existing IP Address/Mask, rule or command.</p>
12	Max. Number of Failed Logins	<p>Enter the maximum number of failed attempts or failed logins allowed for a user. If the number of failed logins or attempts exceeds this maximum number allowed, the user will be blocked from the system.</p> <p>NOTE: If this box is left empty, the user is allowed to try to login to the server indefinitely. For network security, this is not recommended.</p>
13	Block Time (Minutes)	<p>Enter the number of minutes allowed for a user to attempt to login. If the user fails to login within this time allowed, the user will be blocked from system.</p> <p>NOTE: If this box is left empty, the user is allowed to try to login to the server indefinitely. For network security, this is not recommended.</p>

Date/Time

Selecting the DATE/TIME option from the DEVICE SETTINGS submenu brings up the DATE/TIME screen (Figure 8-22). Use this screen to set the internal real-time clock for your SIMBL card. Controls for this screen are shown and detailed in Table 8-22.

Figure 8-22. Date/Time Screen

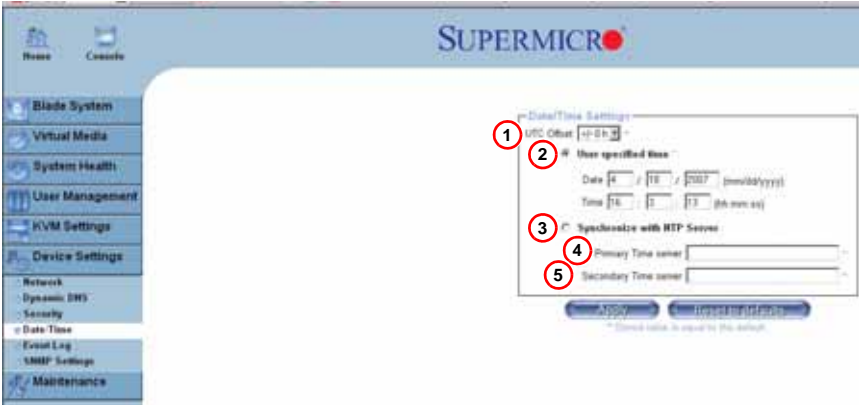


Table 8-22. Date/Time Screen Controls

Item	Name	Description
1	UTC Offset	This pull-down menu allows you to offset the UTC Timer.
2	User Specified Time	This option allows the user to enter the time values for the SIMCM internal real-time clock.
3	Synchronize with NTP Server	Click this to synchronize your SIMBL card's real-time clock with the NTP (Network Time Protocol) server.
4	Primary Time Server	Enter the IP Address for the primary NTP server that you want your SIMBL internal real-time clock to synchronize with. NOTE: Daylight savings time cannot be automatically adjusted. Please manually set up the UTC offset twice a year to compensate for daylight savings time.
5	Secondary Time Server	Enter the IP Address for the secondary NTP server that you want your SIMBL internal real-time clock to synchronize with. NOTE: Daylight savings time cannot be automatically adjusted. Please manually set up the UTC offset twice a year to compensate for daylight savings time.

Event Log

Selecting the EVENT LOG option from the DEVICE SETTINGS submenu brings up the DEVICE SETTINGS EVENT LOG screen (Figure 8-23). Use this screen to set event log targets and assignments. Controls for this screen are shown and detailed in Table 8-23.

- **Event Log Targets:** This section allows you to manually set the event log targets and settings.
- **Event Log Assignments:** This window allows you to specify the types and the destination for the event logging.

Figure 8-23. Device Settings Event Log Screen

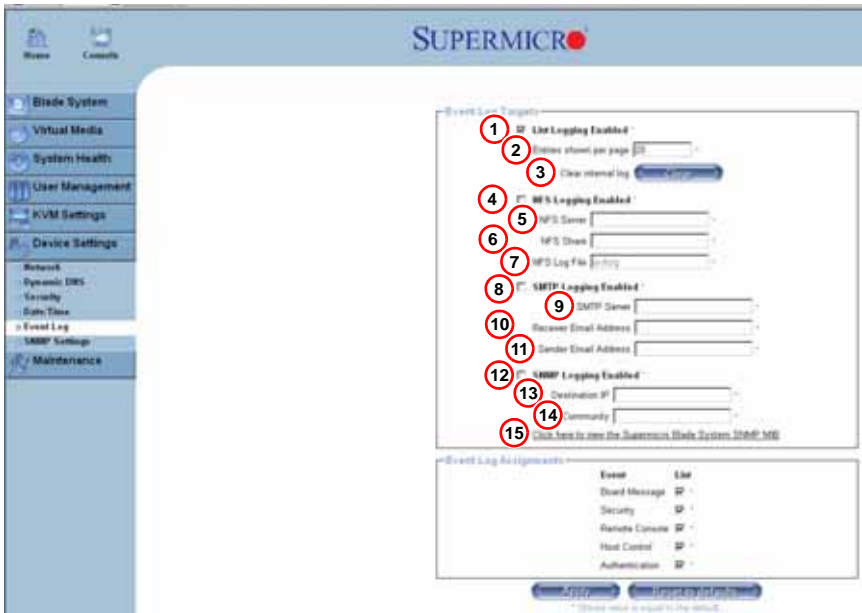


Table 8-23. Device Settings Event Log Screen Controls

Item	Name	Description
1	List Logging Enabled	Check this box to activate the event-logging list. To show the event log list, click on EVENT LOG under SYSTEM HEALTH. NOTE: The maximum number of log list entries is 1,000 events. Every entry that exceeds this limit will automatically override the oldest one in the list. If the reset button is pressed, all logging information will be saved, however, all logging data will be lost if a hard reset is performed or the system loses power.
2	Entries Shown Per Page	Enter the number of entries you want to display on a page.
3	Clear Internal Log	Click this icon to clear the internal event log from memory.

Table 8-23. Device Settings Event Log Screen Controls (Continued)

Item	Name	Description
4	NFS Logging Enabled	Click this box to enable NFS Logging, which will create a Network File System (NFS) for the event logging data to be written into.
5	NFS Server	Enter the IP Address of the NFS server here.
6	NFS Share	Enter the path of the Network File System in which the event logging data is stored.
7	NFS Log File	Enter the filename of the Network File System in which the event logging data is stored.
8	SMTP Logging Enabled	Check this box to enable the SMTP (Simple Mail Transfer Protocol) logging.
9	SMTP Server	Enter the IP Address for the SMTP server.
10	Receiver Email Address	Enter the email address that the SMTP event logging data will be sent to.
11	Sender Email Address	Enter the email address from which the SMTP event logging data is sent.
12	SNMP Logging Enabled	Check this box to enable SNMP (Simple Network Management Protocol) logging.
13	Destination IP	Enter the IP address where the SNMP trap will be sent to.
14	Community	Enter the name of the community if the receiver requires a community string.
15	Click here to view the Supermicro Blade System SNMP MIB	Click this link to see the SMCM card SNMP MIB.

SNMP Settings

Selecting the SNMP SETTINGS option from the DEVICE SETTINGS submenu brings up the SNMP SETTINGS screen (Figure 8-24). Use this screen to configure Simple Network Management Protocol settings. Controls for this screen are shown and detailed in Table 8-24.

Figure 8-24. SNMP Settings Screen

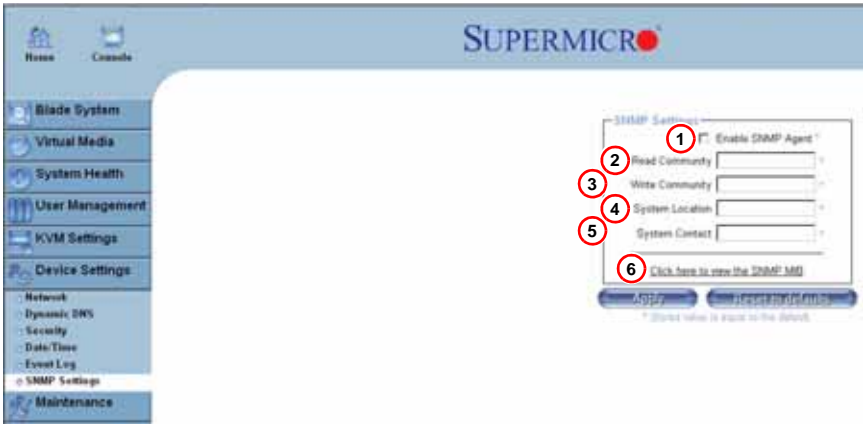


Table 8-24. SNMP Settings Screen Controls

Item	Name	Description
1	Enable SNMP Agent	Check the box to enable the SNMP Agent and allow it to interface with your SIMCM card.
2	Read Community	Enter the name of the SNMP community from which you will retrieve information via SNMP.
3	Write Community	Enter the name of the SNMP community to which you can write information and issue commands via SNMP.
4	System Location	Enter the physical location of the SNMP host server. This location will be used in response to the SNMP request as "sysLocation0".
5	System Contact	Enter the name of the contact person for the SNMP host server. This value will be referred to as "sysContact0".
6	Click here to view the SNMP MIB	Click this link to view the SIMBL card SNMP MIB file. This file may be necessary for an SNMP client to interface with the SIMBL card.

Maintenance

Clicking the MAINTENANCE icon allows you to access the following screens through its sub-menus:

- [Device Information](#)
- [Event Log](#)
- [Update Firmware](#)
- [Unit Reset](#)

Device Information

Clicking the DEVICE INFORMATION option in the MAINTENANCE submenu brings up the DEVICE INFORMATION screen (Figure 8-25), which provides system information. The controls for this screen are detailed in Table 8-25.

Figure 8-25. Device Information Screen



Table 8-25. Device Information Screen Controls

Item	Name	Description
1	Device Information	This field displays information on the SIMBL card and its firmware.
2	View the Data File for Support	Click on this link to view the XML file which contains product information that is needed for technical support.
3	Connected Users	List the name(s), the IP Address(es) and the status of the connect user(s).

Event Log

Clicking the EVENT LOG option in the MAINTENANCE submenu brings up the MAINTENANCE EVENT LOG LIST screen (Figure 8-26). This screen contains information on events that are recorded by the SIMBL in the order of Date/Time, Types and Descriptions including the IP address(es), user(s) and activities involved.

Figure 8-26. Maintenance Event Log List Screen

Date	Event	Description
04/18/2007 16:41:09	Remote Console	Connection to client 192.168.6.86 closed.
04/18/2007 16:33:33	Remote Console	Connection to client 192.168.6.86 established.
04/18/2007 16:32:39	Remote Console	Connection to client 192.168.6.86 closed.
04/18/2007 16:32:35	Remote Console	Connection to client 192.168.6.86 established.
04/18/2007 16:31:52	Remote Console	Connection to client 192.168.6.86 closed.
04/18/2007 16:21:24	Remote Console	Connection to client 192.168.6.86 established.
04/18/2007 16:24:37	Remote Console	Connection to client 192.168.1.132 established.
04/18/2007 16:23:08	Authentication	User 'ADMIN' logged in from IP address 192.168.1.132
04/18/2007 16:23:08	Authentication	User 'ADMIN' logged in from IP address 192.168.6.81
04/18/2007 16:14:40	Authentication	User 'ADMIN' logged in from IP address 192.168.6.81
04/18/2007 14:11:50	Authentication	User 'ADMIN' logged in from IP address 192.168.6.81
01/05/1970 00:00:00	Event Message	Device successfully started.
04/18/2007 12:13:47	Authentication	User 'ADMIN' logged in from IP address 192.168.1.132
04/18/2007 12:13:39	Authentication	User 'ADMIN' failed to log in from IP address 192.168.1.132
04/18/2007 10:50:14	Authentication	User 'ADMIN' logged in from IP address 192.168.6.86
04/17/2007 20:17:59	Remote Console	Connection to client 192.168.6.86 closed.
04/17/2007 20:17:44	Remote Console	Connection to client 192.168.6.86 established.
04/17/2007 20:06:49	Authentication	User 'ADMIN' logged in from IP address 192.168.10.42
04/17/2007 20:02:53	Authentication	User 'ADMIN' logged in from IP address 192.168.6.86
04/17/2007 19:40:42	Remote Console	Connection to client 192.168.1.132 closed.

Update Firmware

Clicking the UPDATE FIRMWARE option in the MAINTENANCE submenu brings up the UPDATE FIRMWARE screen (Figure 8-27). This screen is where you can update the firmware for the SIMCM card in the CMM module. The controls for this screen are detailed in Table 8-26.



NOTE: This process is not reversible once the firmware is updated, so proceed with caution. It might take a few minutes to complete this procedure.

Figure 8-27. Update Firmware Screen

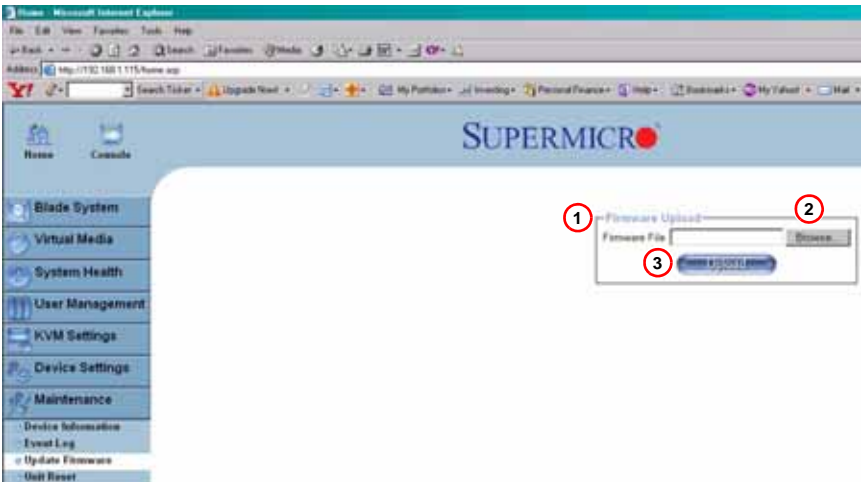


Table 8-26. Update Firmware Screen Controls

Item	Name	Description
1	Firmware File	Enter the name of the firmware you want to update or click BROWSE to select the file.
2	Browse Button	Click the BROWSE button to select the firmware file.
3	Upload	Click on the UPLOAD icon to upload the firmware file to the server for the update.

Unit Reset

Clicking the UNIT RESET option in the MAINTENANCE submenu brings up the UNIT RESET screen (Figure 8-28), which allows you to reset USB and Device components. The controls for this screen are detailed in Table 8-27.

Figure 8-28. Unit Reset Screen

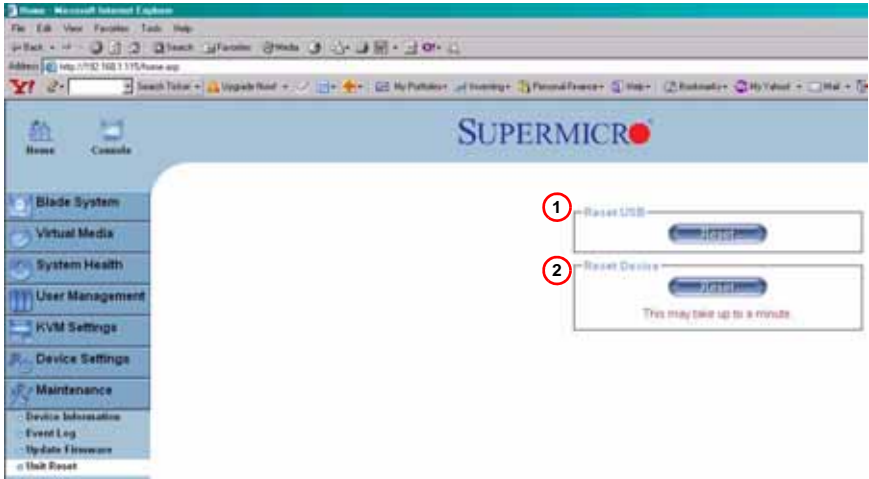


Table 8-27. Unit Reset Screen Controls

Item	Name	Description
1	Reset USB	Click the RESET icon to reset the USB module.
2	Reset Device	Click the RESET icon to cold reset the utility's firmware.

8-4 Remote Console

Activating the remote console may be done in two ways:

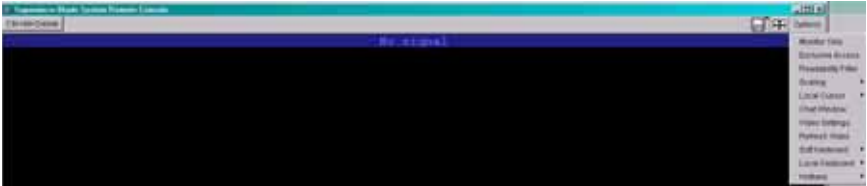
- **Home Page:** On the HOME page, click on the CONSOLE icon in the upper left area of the screen.
- **Blade System Menu:** Click the BLADE SYSTEM icon on the left of the screen, then click BLADE in the submenu. A screen will open with a list of blades.

The blade units listed are hyperlinks - click one of these to open a screen giving details on that blade unit. In each screen you will see a REMOTE CONSOLE PREVIEW pane. At the top is a link that reads CLICK TO OPEN. Click this link to open the remote console.

After the remote console screen appears, click on OPTION in the upper right corner to display the OPTIONS menu as shown below (Figure 8-29).

Remote Console Options

Figure 8-29. Remote Console Options



The following items are included in the OPTIONS Menu and described in more detail in the sections below:

- [Monitor Only](#)
- [Exclusive Access](#)
- [Readability Filter](#)
- [Scaling](#)
- [Local Cursor](#)
- [Chat Window](#)
- [Video Settings](#)
- [Soft Keyboard](#)
- [Local Keyboard](#)
- [Hotkeys](#)

Monitor Only

Click MONITOR ONLY to turn the *Monitor Only* function on or off. If MONITOR ONLY is selected, the KB/MOUSE icon on the lower right corner will be crossed out as shown in [Figure 8-29](#), and the user can only view or monitor remote console activities. Also, any remote console interaction will no longer be available.

Exclusive Access

With the appropriate permission, a user can force other users to quit the remote console and claim the console for their own exclusive use by clicking on EXCLUSIVE ACCESS. When this function is selected, the second user icon on the lower left corner of the screen will be crossed out.

Readability Filter

Click on this to turn the *Readability Filter* on or off. Turn on this function to preserve most of the screen details even when the screen image is substantially scaled down.



NOTE: This item is available for systems with JVM 1.4 or higher.

Scaling

This item allows the user to scale the remote console screen to the desired size. Click on this button to access its submenu and select the desired setting from the options listed in the submenu: 25%, 50%, 100% and SCALE TO FIT.

Local Cursor

This item allows the user to choose the desired shape for the local cursor. Click on this button to access its submenu and select a desired shape from the options listed in the submenu: TRANSPARENT, DEFAULT, BIG, PIXEL and CROSS-HAIR. The availability of the shapes depends on the Java Virtual Machine used.

Chat Window

This item allows the user to communicate with other users logged in to the same remote host. The screen below shows a CHAT WINDOW displayed in a scaled down remote console screen (see [Figure 8-30](#)). The window's controls are shown in [Table 8-28](#).



NOTE: Once you've typed a message in the chat line box and pressed <ENTER>, your message will be sent to remote systems and read by other users. Please review the text displayed in the chat line box before you hit <ENTER>.

Figure 8-30. Chat Window

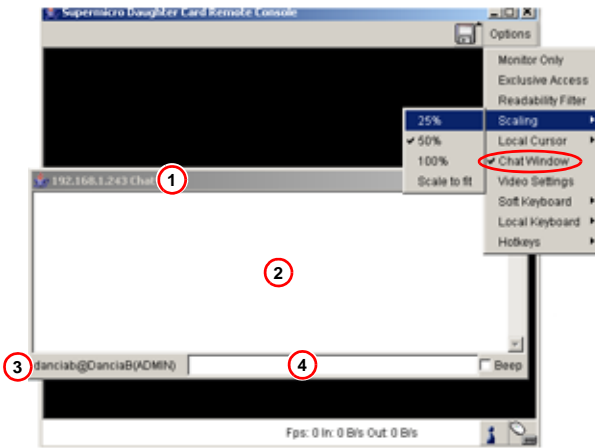


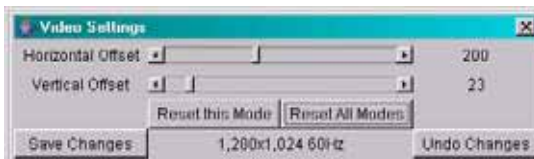
Table 8-28. Items in the Chat Window

Item	Name	Description
1	Title Bar	This shows the IP address of the remote host you are connected to.
2	Chat Window Frame	This frame displays chat messages, including your own messages that have been sent to other users. This is a read-only test display area.
3	User's Identity Label	This line displays your own identity.
4	Chat Line	This is an editable text line where you can enter a new message.

Video Settings

This item allows the user to set the monitor display settings by clicking on the VIDEO SETTINGS button. After you've clicked the VIDEO SETTINGS button, the submenu displays as shown in [Figure 8-31](#).

Figure 8-31. Video Settings



Use your cursor pointer to click on the left and right arrows to adjust the setting for the HORIZONTAL OFFSET and VERTICAL OFFSET.

If you are not happy with the changes you've made, you can click the RESET THIS MODE button to reset a particular item, or click on the RESET ALL MODES button to reset all

items. To save all changes, click on the **SAVE CHANGES** button. You can also click on **UNDO CHANGES** to abandon the changes.

Soft Keyboard

This item allows the user to use the soft keys that have been pre-installed in the *Soft Keyboard* of the particular language selected. Click on **SHOW BUTTON** to show a soft keyboard which contains pre-installed soft keys (see [Figure 8-32](#)). Click on **MAPPING** to display a list of major world languages. When the language list displays, select the language you want to use by clicking on it (see [Figure 8-33](#)).

Figure 8-32. Keys in English Soft Keyboard



Figure 8-33. Soft Keyboard Language Selection



Local Keyboard

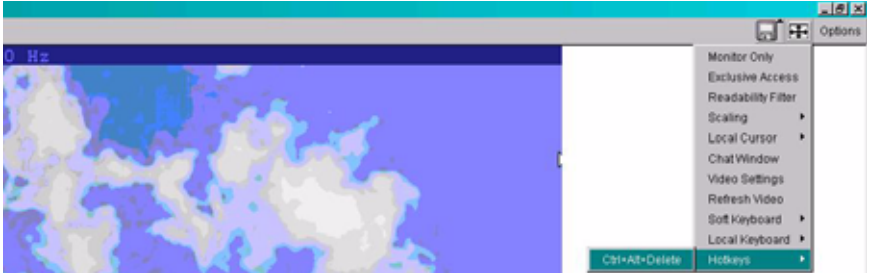
This item allows the user to manually change the local keyboard setting for interaction with a remote host. Use this function to change the language mapping of your browser machine running the remote console host. After you have clicked **LOCAL KEYBOARD** button, a language submenu displays. When this language list displays, select the language you want to use.

Hotkeys

This item allows the user to select a pre-defined hot key from a list. Once a hot key is selected, the command associated with the hot key will be sent to the remote console host for execution.

After you've clicked the HOTKEY button, the submenu displays as shown in [Figure 8-34](#).

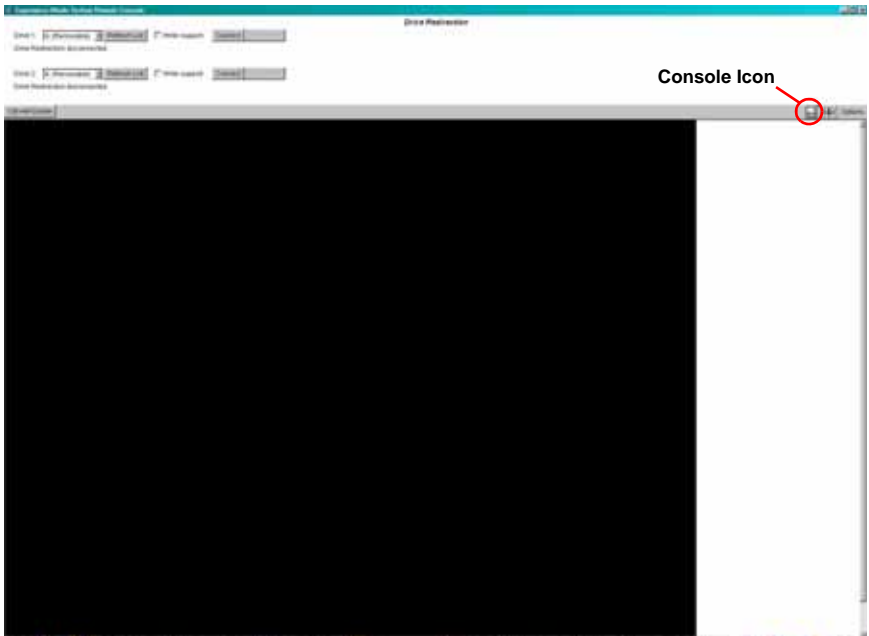
Figure 8-34. Hotkeys



Remote Console Interface Window

To access the REMOTE CONSOLE INTERFACE window, click the CONSOLE icon on the REMOTE CONSOLE window as shown in [Figure 8-35](#).

Figure 8-35. Console Icon



This function allows the local host to interact with a remote server. Through the REMOTE CONSOLE INTERFACE window (Figure 8-36), the user can share files stored in the local drive with a user connected to the remote server, download data from a local drive to the remote server, issue commands to manage the remote server or allow the remote server be controlled and managed by a local user logged in to the remote server. This function provides a full spectrum of remote console interaction and management.

You need to have the *Administrator Privilege* to use this feature.

Table 8-29 details the controls found in the REMOTE CONSOLE INTERFACE window.

Figure 8-36. Remote Console Interface Window

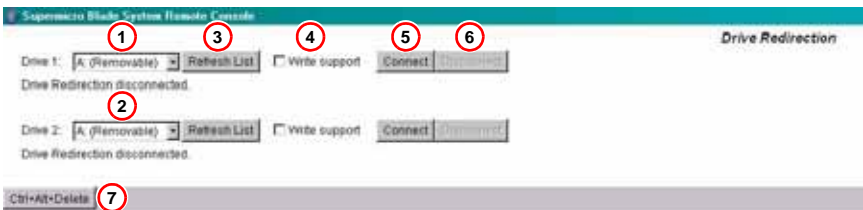


Table 8-29. Remote Console Interface Window

Item	Name	Description
1	Local Drive List (Drive 1)	This window displays a list of local drives available for remote access. Select from the list a local drive that you want to make accessible for a remote server.
2	Local Drive List (Drive 2)	This window displays a list of local drives available for remote access. Select from the list a local drive that you want to make accessible for a remote server.
3	Refresh	Click this button to refresh the local drive list.
4	Write Support	Check this button to allow the remote operating system to have write access to the drive that you have selected. This function allows a user to alter, overwrite, erase and destroy data stored in the drive selected. This feature should only be used with non-critical data. When "Write Support" is checked, a warning message will display. Read the warning message carefully before enabling this function.
5	Connect	Click this button to make the drive you have selected accessible for remote console interaction. Once you have clicked "connect," users logged into remote servers will have access to the local drive that you have selected.
6	Disconnect	Click this button to cancel the connection established between a local drive and a remote server. Once you click this button, the drive you have selected will not be accessible for remote console interface.
7	Sending Commands	This function allows the user to issue a pre-defined command to a remote server for execution. To use this function, you need to click the hot keys displayed on the upper right corner of the screen. Note: Hot keys are commands that have been pre-defined and pre-stored in a remote consoles.

Click the CTRL+ALT+DELETE button to send the command CTRL+ALT+DELETE to the remote server for execution.

Once you have clicked on the button, it displays a message asking you to confirm if you really want to send CTRL+ALT+DELETE. Click YES to confirm or click CANCEL to cancel sending the command for remote execution.

8-5 Log Out

From any page, click on the LOG OUT icon at the top right of the screen to log out of the Web-based Management Utility.

Notes

Chapter 9

BIOS

9-1 Introduction

This chapter describes the BIOS for AMD SuperBlade modules. The AMD Blade modules use a AMI™ ROM BIOS that is stored in a flash chip. This BIOS can be easily upgraded using a floppy disk-based program.



NOTE: Due to periodic changes to the BIOS, some settings may have been added or deleted and might not yet be recorded in this manual. Please refer to the <http://www.supermicro.com/products/superblade/> website for further details on BIOS setup and the BIOS menus for your SuperBlade blade module.

System BIOS

BIOS stands for Basic Input Output System. The AMI BIOS flash chip stores the system parameters, types of disk drives, video displays, etc. in the CMOS. The CMOS memory requires very little electrical power. When the blade unit is turned off, a backup battery provides power to the BIOS flash chip, enabling it to retain system parameters. Each time the blade is powered on it is configured with the values stored in the BIOS ROM by the system BIOS, which gains control at boot up.

How To Change the Configuration Data

The CMOS information that determines the system parameters may be changed by entering the BIOS Setup utility. This Setup utility can be accessed by pressing the <DELETE> key at the appropriate time during system boot. (See "Starting the Setup Utility" below.)

Starting the Setup Utility

Normally, the only visible POST (Power-On Self-Test) routine is the memory test. As the memory is being tested, press the <DELETE> key to enter the main menu of the BIOS Setup utility. From the main menu, you can access the other setup screens, such as the Security and Power menus.



WARNING: To prevent possible boot failure, do not shut down or reset the system while updating the BIOS.

9-2 BIOS Updates

It may be necessary to update the BIOS used in the blade modules on occasion. However, it is recommended that you not update BIOS if you are not experiencing problems with a blade module.

Updated BIOS files are located on our web site(www.supermicro.com/products/superblade/). Please check the current BIOS revision and make sure it is newer than your current BIOS before downloading.

There are several methods you may use to upgrade (flash) your BIOS. After downloading the appropriate BIOS file (in a zip file format), follow one of the methods described below to flash the new BIOS.

Flashing BIOS

Use the procedures below to "Flash" your BIOS with a new update using the KVM dongle, USB ports on the CMM module or by use of a Floppy disk.

Flashing a BIOS using the KVM Dongle:

For this method, you must use a KVM "dongle" cable (CBL-0218L, included with the system).

1. Copy the contents of the zip file to a bootable USB pen drive.
2. Connect the KVM dongle (CBL-0218L) to the KVM connector at the front of the blade you will be flashing the BIOS to.
3. Connect your bootable USB pen drive to one of the two USB slots on the KVM dongle.
4. Boot to the USB pen drive and go to the directory where you saved the contents of the zip file.
5. Type **flash filename.rom** (replace *filename.rom* by the actual ROM file name).

Flashing a BIOS using the USB Ports on the CMM:

1. Copy the contents of the zip file to a bootable USB pen drive.
2. Connect your bootable USB pen drive to one of the two USB slots on the CMM (located on the back side of the enclosure).
3. Boot to the USB pen drive and go to the directory where you saved the contents of the zip file.
4. Type **flash filename.rom** (replace *filename.rom* by the actual ROM file name).

Flashing a BIOS using a Floppy Image File

This method must be performed remotely.

1. Copy the image file from the zip file to your desktop.
2. Use the web browser or IPMIView to access your CMM remotely using its IP Address.

3. Go to the VIRTUAL MEDIA menu and select FLOPPY IMAGE UPLOAD.
4. BROWSE or OPEN to locate the *.img file on your desktop. Select this *.img file.
5. Press the UPLOAD button and wait a few seconds for the image to upload to the CMM.
6. Once the upload finishes, turn on the blade module and press to enter the BIOS setup utility.
7. In the BOOT MENU, bring **USB LS120: PEPPCMM VIRTUAL DISC 1** to the top of the boot priority list.
8. Exit while saving the changes. The blade module will boot to the virtual media (floppy image) **A:\>**.
9. Type **flash filename.rom**.



NOTE: Replace *filename.rom* by the actual ROM file name (such as **B7DBE142.rom** for example) in the command.

9-3 Running Setup

The BIOS setup options described in this section are selected by choosing the appropriate text from the MAIN BIOS SETUP screen.

When you first power on the computer, the BIOS is immediately activated.

While the BIOS is in control, the Setup program can be activated in one of two ways:

1. By pressing <DELETE> immediately after turning the system on, or
2. When the message “Press the <Delete> key to enter Setup” appears briefly at the bottom of the screen during the POST, press the <DELETE> key to activate the main SETUP menu:

See our (www.supermicro.com/products/superblade/) website for details on BIOS setup and the menu options for your blade system’s BIOS.

Notes

Appendix A

BIOS POST Codes and Messages

When AMIBIOS performs the Power On Self Test, it writes checkpoint codes to I/O port 0080h. If the computer cannot complete the boot process, diagnostic equipment can be attached to the computer to read I/O port 0080h.

A-1 Uncompressed Initialization Codes

The uncompressed initialization checkpoint codes are listed in order of execution in [Table A-1](#).

Table A-1. Uncompressed Initialization Codes

Checkpoint	Code Description
D0h	The NMI is disabled. Power on delay is starting. Next, the initialization code checksum will be verified.
D1h	Initializing the DMA controller, performing the keyboard controller BAT test, starting memory refresh and entering 4 GB flat mode next.
D3h	Starting memory sizing next.
D4h	Returning to real mode. Executing any OEM patches and setting the Stack next.
D5h	Passing control to the uncompressed code in shadow RAM at E000:0000h. The initialization code is copied to segment 0 and control will be transferred to segment 0.

A-2 Bootblock Recovery Codes

The bootblock recovery checkpoint codes are listed in order of execution in [Table A-2](#).

Table A-2. Bootblock Recovery Codes

Checkpoint	Code Description
E0h	The onboard floppy controller if available is initialized. Next, beginning the base 512 KB memory test.
E1h	Initializing the interrupt vector table next.
E2h	Initializing the DMA and Interrupt controllers next.
E6h	Enabling the floppy drive controller and Timer IRQs. Enabling internal cache memory.
E6h	Enabling the floppy drive controller and Timer IRQs. Enabling internal cache memory.
Edh	Initializing the floppy drive.
Eeh	Looking for a floppy diskette in drive A:. Reading the first sector of the diskette.
Efh	A read error occurred while reading the floppy drive in drive A:.
F0h	Next, searching for the AMIBOOT.ROM file in the root directory.
F1h	The AMIBOOT.ROM file is not in the root directory.

Table A-2. Bootblock Recovery Codes (Continued)

Checkpoint	Code Description
F2h	Next, reading and analyzing the floppy diskette FAT to find the clusters occupied by the AMIBOOT.ROM file.
F3h	Next, reading the AMIBOOT.ROM file, cluster by cluster.
F4h	The AMIBOOT.ROM file is not the correct size.
F5h	Next, disabling internal cache memory.
FBh	Next, detecting the type of flash ROM.
FCh	Next, erasing the flash ROM.
FDh	Next, programming the flash ROM.
FFh	Flash ROM programming was successful. Next, restarting the system BIOS.

A-3 Uncompressed Initialization Codes

The following runtime checkpoint codes are listed in order of execution in [Table A-3](#). These codes are uncompressed in F0000h shadow RAM.

Table A-3. Uncompressed Initialization Codes

Checkpoint	Code Description
03h	The NMI is disabled. Next, checking for a soft reset or a power on condition.
05h	The BIOS stack has been built. Next, disabling cache memory.
06h	Uncompressing the POST code next.
07h	Next, initializing the CPU and the CPU data area.
08h	The CMOS checksum calculation is done next.
0Ah	The CMOS checksum calculation is done. Initializing the CMOS status register for date and time next.
0Bh	The CMOS status register is initialized. Next, performing any required initialization before the keyboard BAT command is issued.
0Ch	The keyboard controller input buffer is free. Next, issuing the BAT command to the keyboard controller.
0Eh	The keyboard controller BAT command result has been verified. Next, performing any necessary initialization after the keyboard controller BAT command test.
0Fh	The initialization after the keyboard controller BAT command test is done. The keyboard command byte is written next.
10h	The keyboard controller command byte is written. Next, issuing the Pin 23 and 24 blocking and unblocking command.
11h	Next, checking if <END> or <INS> keys were pressed during power on. Initializing CMOS RAM if the Initialize CMOS RAM in every boot AMIBIOS POST option was set in AMIBCP or the <END> key was pressed.
12h	Next, disabling DMA controllers 1 and 2 and interrupt controllers 1 and 2.
13h	The video display has been disabled. Port B has been initialized. Next, initializing the chipset.

Table A-3. Uncompressed Initialization Codes (Continued)

Checkpoint	Code Description
14h	The 8254 timer test will begin next.
19h	Next, programming the flash ROM.
1Ah	The memory refresh line is toggling. Checking the 15 second on/off time next.
2Bh	Passing control to the video ROM to perform any required configuration before the video ROM test.
2Ch	All necessary processing before passing control to the video ROM is done. Looking for the video ROM next and passing control to it.
2Dh	The video ROM has returned control to BIOS POST. Performing any required processing after the video ROM had control
23h	Reading the 8042 input port and disabling the MEGAKEY Green PC feature next. Making the BIOS code segment writable and performing any necessary configuration before initializing the interrupt vectors.
24h	The configuration required before interrupt vector initialization has completed. Interrupt vector initialization is about to begin.
25h	Interrupt vector initialization is done. Clearing the password if the POST DIAG switch is on.
27h	Any initialization before setting video mode will be done next.
28h	Initialization before setting the video mode is complete. Configuring the monochrome mode and color mode settings next.
2Ah	Bus initialization system, static, output devices will be done next, if present. See the last page for additional information.
2Eh	Completed post-video ROM test processing. If the EGA/VGA controller is not found, performing the display memory read/write test next.
2Fh	The EGA/VGA controller was not found. The display memory read/write test is about to begin.
30h	The display memory read/write test passed. Look for retrace checking next.
31h	The display memory read/write test or retrace checking failed. Performing the alternate display memory read/write test next.
32h	The alternate display memory read/write test passed. Looking for alternate display retrace checking next.
34h	Video display checking is over. Setting the display mode next.
37h	The display mode is set. Displaying the power on message next.
38h	Initializing the bus input, IPL, general devices next, if present. See the last page of this chapter for additional information.
39h	Displaying bus initialization error messages. See the last page of this chapter for additional information.
3Ah	The new cursor position has been read and saved. Displaying the Hit message next.
3Bh	The Hit message is displayed. The protected mode memory test is about to start.
40h	Preparing the descriptor tables next.

Table A-3. Uncompressed Initialization Codes (Continued)

Checkpoint	Code Description
42h	The descriptor tables are prepared. Entering protected mode for the memory test next.
43h	Entered protected mode. Enabling interrupts for diagnostics mode next.
44h	Interrupts enabled if the diagnostics switch is on. Initializing data to check memory wraparound at 0:0 next.
45h	Data initialized. Checking for memory wraparound at 0:0 and finding the total system memory size next.
46h	The memory wraparound test is done. Memory size calculation has been done. Writing patterns to test memory next.
47h	The memory pattern has been written to extended memory. Writing patterns to the base 640 KB memory next.
48h	Patterns written in base memory. Determining the amount of memory below 1 MB next.
49h	The amount of memory below 1 MB has been found and verified.
4Bh	The amount of memory above 1 MB has been found and verified. Checking for a soft reset and clearing the memory below 1 MB for the soft reset next. If this is a power on situation, going to checkpoint 4Eh next.
4Ch	The memory below 1 MB has been cleared via a soft reset. Clearing the memory above 1 MB next.
4Dh	The memory above 1 MB has been cleared via a soft reset. Saving the memory size next. Going to checkpoint 52h next.
4Eh	The memory test started, but not as the result of a soft reset. Displaying the first 64 KB memory size next.
4Fh	The memory size display has started. The display is updated during the memory test. Performing the sequential and random memory test next.
50h	The memory below 1 MB has been tested and initialized. Adjusting the displayed memory size for relocation and shadowing next.
51h	The memory size display was adjusted for relocation and shadowing.
52h	The memory above 1 MB has been tested and initialized. Saving the memory size information next.
53h	The memory size information and the CPU registers are saved. Entering real mode next.
54h	Shutdown was successful. The CPU is in real mode. Disabling the Gate A20 line, parity, and the NMI next.
57h	The A20 address line, parity, and the NMI are disabled. Adjusting the memory size depending on relocation and shadowing next.
58h	The memory size was adjusted for relocation and shadowing. Clearing the Hit message next.
59h	The Hit message is cleared. The <WAIT...> message is displayed. Starting the DMA and interrupt controller test next.
60h	The DMA page register test passed. Performing the DMA Controller 1 base register test next.
62h	The DMA controller 1 base register test passed. Performing the DMA controller 2 base register test next.

Table A-3. Uncompressed Initialization Codes (Continued)

Checkpoint	Code Description
65h	The DMA controller 2 base register test passed. Programming DMA controllers 1 and 2 next.
66h	Completed programming DMA controllers 1 and 2. Initializing the 8259 interrupt controller next.
67h	Completed 8259 interrupt controller initialization.
7Fh	Extended NMI source enabling is in progress.
80h	The keyboard test has started. Clearing the output buffer and checking for stuck keys. Issuing the keyboard reset command next.
81h	A keyboard reset error or stuck key was found. Issuing the keyboard controller interface test command next.
82h	The keyboard controller interface test completed. Writing the command byte and initializing the circular buffer next.
83h	The command byte was written and global data initialization has completed. Checking for a locked key next.
84h	Locked key checking is over. Checking for a memory size mismatch with CMOS RAM data next.
85h	The memory size check is done. Displaying a soft error and checking for a password or bypassing WINBIOS Setup next.
86h	The password was checked. Performing any required programming before WINBIOS Setup next.
87h	The programming before WINBIOS Setup has completed. Uncompressing the WINBIOS Setup code and executing the AMIBIOS Setup or WINBIOS Setup utility next.
88h	Returned from WINBIOS Setup and cleared the screen. Performing any necessary programming after WINBIOS Setup next.
89h	The programming after WINBIOS Setup has completed. Displaying the power on screen message next.
8Ch	Programming the WINBIOS Setup options next.
8Dh	The WINBIOS Setup options are programmed. Resetting the hard disk controller next.
8Fh	The hard disk controller has been reset. Configuring the floppy drive controller next.
91h	The floppy drive controller has been configured. Configuring the hard disk drive controller next.
95h	Initializing the bus option ROMs from C800 next. See the last page of this chapter for additional information.
96h	Initializing before passing control to the adaptor ROM at C800.
97h	Initialization before the C800 adaptor ROM gains control has completed. The adaptor ROM check is next.
98h	The adaptor ROM had control and has now returned control to BIOS POST. Performing any required processing after the option ROM returned control.
99h	Any initialization required after the option ROM test has completed. Configuring the timer data area and printer base address next.
9Ah	Set the timer and printer base addresses. Setting the RS-232 base address next.

Table A-3. Uncompressed Initialization Codes (Continued)

Checkpoint	Code Description
9Bh	Returned after setting the RS-232 base address. Performing any required initialization before the Coprocessor test next.
9Ch	Required initialization before the Coprocessor test is over. Initializing the Coprocessor next.
9Dh	Coprocessor initialized. Performing any required initialization after the Coprocessor test next.
9Eh	Initialization after the Coprocessor test is complete. Checking the extended keyboard, keyboard ID, and Num Lock key next. Issuing the keyboard ID command next.
A2h	Displaying any soft errors next.
A3h	The soft error display has completed. Setting the keyboard typematic rate next.
A4h	The keyboard typematic rate is set. Programming the memory wait states next.
A5h	Memory wait state programming is over. Clearing the screen and enabling parity and the NMI next.
A7h	NMI and parity enabled. Performing any initialization required before passing control to the adaptor ROM at E000 next.
A8h	Initialization before passing control to the adaptor ROM at E000h completed. Passing control to the adaptor ROM at E000h next.
A9h	Returned from adaptor ROM at E000h control. Performing any initialization required after the E000 option ROM had control next.
Aah	Initialization after E000 option ROM control has completed. Displaying the system configuration next.
Abh	Uncompressing the DMI data and executing DMI POST initialization next.
B0h	The system configuration is displayed.
B1h	Copying any code to specific areas.
00h	Code copying to specific areas is done. Passing control to INT 19h boot loader next.

A-4 BIOS Error Beep Codes

During the POST (Power-On Self-Test) routines, which are performed each time the system is powered on, errors may occur.

- **Non-fatal errors** are those which, in most cases, allow the system to continue the boot-up process. The error messages normally appear on the screen.
- **Fatal errors** are those which will not allow the system to continue the boot-up procedure. If a fatal error occurs, you should consult with your system manufacturer for possible repairs.

These fatal errors are usually communicated through a series of audible beeps. The numbers on the fatal error list, on the following page, correspond to the number of beeps for the corresponding error. All errors listed, with the exception of Beep Code 8, are fatal errors.

POST codes may be read on the debug LEDs located beside the LAN port on the serverboard backplane.

The AMIBIOS error beep codes are shown in [Table A-4](#).

Table A-4. AMIBIOS Error Beep Codes

Beep Code	Error Message	Description
1 beep	Refresh	Circuits have been reset (ready to power up).
5 short, 1 long	Memory error	No memory detected in system
8 beeps	Display memory read/write error	Video adapter missing or with faulty memory

Notes

Appendix B

HCA Mezzanine Cards

This appendix describes safety guidelines, features and installation of HCA Mezzanine cards used with the InfiniBand module. See [Section 4-2: InfiniBand Module on page 4-7](#) for further details.

B-1 Safety Guidelines

To avoid personal injury and property damage, carefully follow all the safety steps listed below when accessing your system or handling the components.

ESD Safety Guidelines

Electric Static Discharge (ESD) can damage electronic components. To prevent damage to your system, it is important to handle it very carefully. The following measures are generally sufficient to protect your equipment from ESD.

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing a component from the antistatic bag.
- Handle the add-on card by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules, avoid touching their pins.
- Put the card and peripherals back into their antistatic bags when not in use.

General Safety Guidelines

- Always disconnect power cables before installing or removing any components from the computer.
- Disconnect the power cable before installing or removing any cables from the system.
- Make sure that the add-on card is securely and properly installed on the motherboard to prevent damage to the system due to power shortage.

B-2 Mezzanine HCA Cards

Available Mezzanine HCA cards for the InfiniBand switch are shown below. The IBH-001 card has Dual 4x DDR IB ports while the IBH-002 card has a single 4x DDR IB port.



NOTE: All images and layouts shown in this user's guide are based upon the latest PCB Revision available at the time of publishing. The card you have received may or may not look exactly the same as the graphics shown in this manual.

Figure B-1. AOC-IBH-001 Mezzanine HCA Card

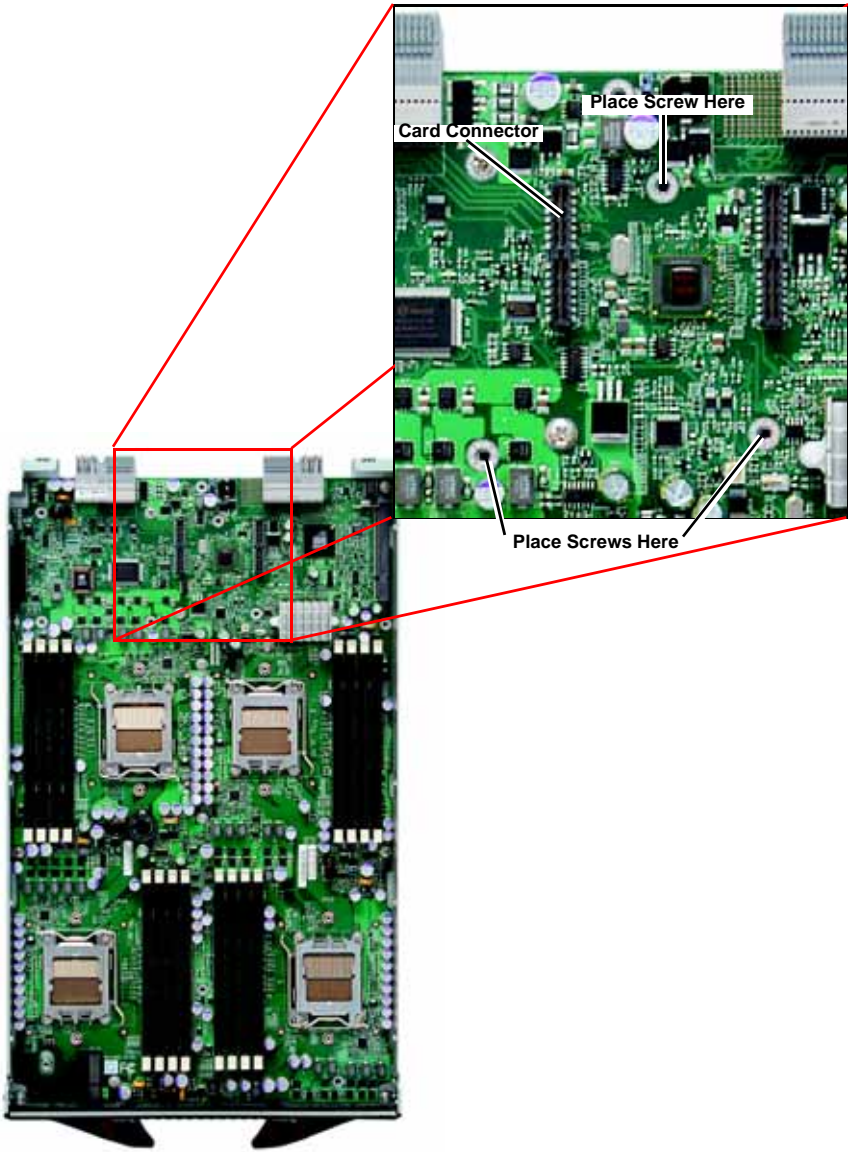


Figure B-2. AOC-IBH-002 Mezzanine HCA Card



B-3 Installation

Figure B-3. Installation Location



Installation Location

Both models of the Mezzanine HCA card are compatible with both SBI and SBA blade modules. For the latest compatibility information, see our website:

<http://www.supernmicro.com/products/superblade/>

Card Installation

To Install an HCA Card:

1. Confirm that you have the correct card and three (3) screws.
2. Following the instructions from the SuperBlade Manual, remove the blade module and open the cover to access the mainboard.
3. In a standard, electro-magnetically protected workstation, secure the card to the serverboard by gently but firmly attaching the card to the two connectors.
4. Using a Phillips screw driver, secure and tighten each screw one at a time. Do not overtighten the screws.

Figure B-4. Card Installation

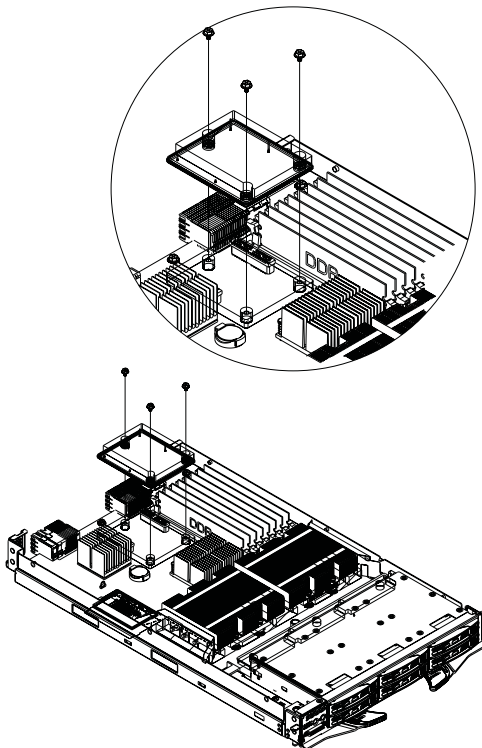
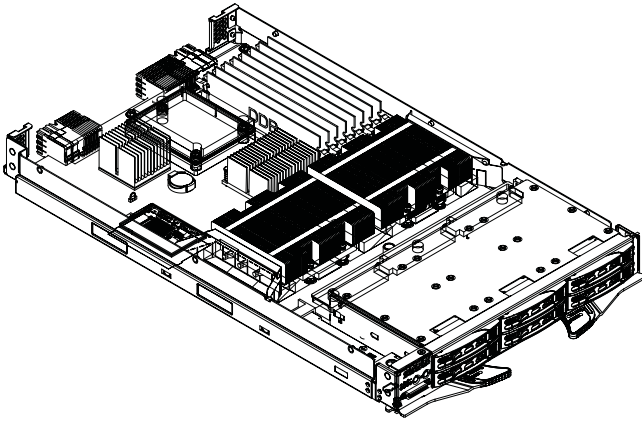


Figure B-5. Installation Complete



Notes

Appendix C

Gigabit Switch Features

Table C-1 provides a summary of features and functions for the Gigabit switch.

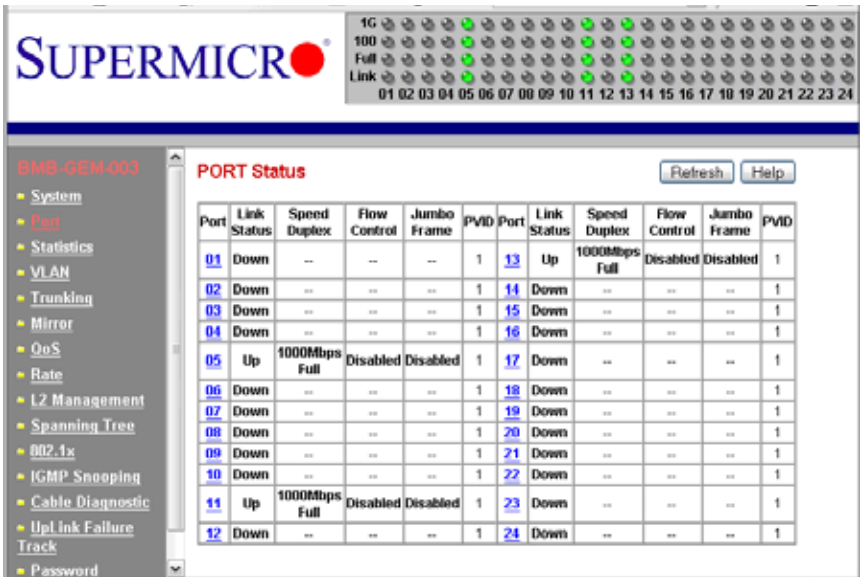
Table C-1. Gigabit Switch Features and Functions

Item	Functions	Features
Basic Functions	Throughput	24Gbps (14 internal 1Gbps + 10 external 1Gbps)
	Latency	Average 2.65usec (frame size 1518 bytes)
	Switching mode	Store-and-forward
	MAC address learning table size	8192 entries
	MAC address learning	IVL (Independent VLAN learning)
	Jumbo frame support	Up to 9216 bytes
	Flow control	802.3x pause frame flow control
	Broadcast Storm Control	Support per-system control types and rates
	Ingress rate control	Support per-port rate control
	Port mirroring	A copy of ingress and egress data of the monitored port is sent to snooping port
Scalability	Trunking (Static Link Aggregation)	Increase bandwidth and redundancy. Up to 8 ports per trunk, 4 trunks per switch.
Redundancy	IEEE802.1D STP IEEE802.1W RSTP	To make a loop-free and redundant network using RSTP. RSTP is upward compatible with legacy STP.
VLAN	IEEE802.1q VLAN	Supports 256 VLAN groups.
QoS	IEEE802.1p QoS	Supports 802.1p priority queuing and 4 priority queues per port.
Multicast	IGMP v1/v2 Snooping	Prevents unnecessary forwarding of multicast packets to reduce multicast traffic.
Management	SNMP agent	Supports SNMP v1 and v2c
	Http server	Forwarding

C-1 Port Status

The PORT STATUS screen provides a status overview of the switch's 24 ports. As shown in Figure C-1, it includes link, speed, duplex, flow control, jumbo frame and PVID. In this screen click on PORT on left menu bar. The port status will show up. To retrieve and update to the latest status, click the REFRESH button.

Figure C-1. Port Status Screen



The port column indicates the port number of the switch. The LINK STATUS shows the current link status (either up or down) for each port. The SPEED DUPLEX indicates the link speed and duplex status for each port when it is linked up. If the link is down, there is no status shown on SPEED DUPLEX. The FLOW CONTROL indicates that the state of flow control is either disabled or enabled for each port when it is linked up. The PVID shows current default port VLAN ID for each switch port.



NOTE: In the figures BMB-GEM-003 is the number of the Gigabit switch board and not a separate model of switch.

Port VLAN ID (PVID)

The PVID is used in a port-based VLAN to allow assigning a port to belong to a VLAN. A VLAN can then be configured to be a group of member ports. This switch is an 802.1q tag-aware switch. If no VLANs are defined on the switch, every port will be assigned to a default VLAN which has VLAN ID 1. Each port will have PVID equal to 1.

If incoming frames are untagged, they will be tagged with the default PVID of the port on which they are received. The destination MAC address of the frame and the PVID will be used for forwarding decisions. An incoming tagged frame will be kept intact. The switch will use the VID in the frame and the destination MAC address for the forwarding decision. Look for a more detailed description in the VLAN section.

Port Configuration

To modify the configuration of each port, click on the port number in the PORT STATUS screen (see Figure C-2). The PORT CONFIGURATION screen defines speed and duplexing for a port when auto-negotiation is off. When auto-negotiation is on, this data are negotiated with the link partner.

Figure C-2. Port Configuration Screen

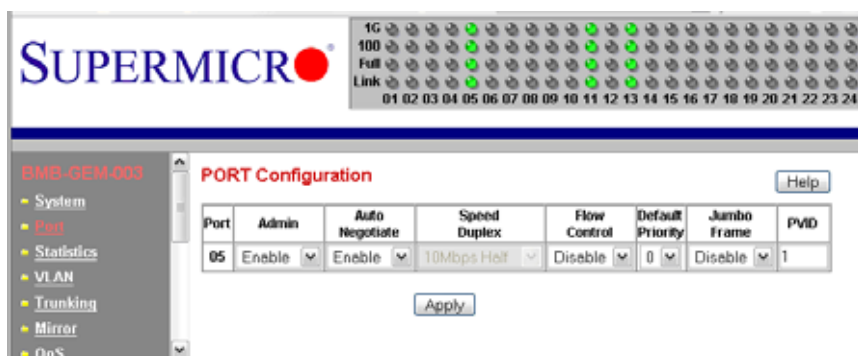


Table C-2. Port Configuration Screen Controls

Control	Description
Port	Specifies the port number to control.
Admin	Enables or disables the port.
Auto Negotiation	Enables or disables auto-negotiation. When auto-negotiation is enabled, the port negotiates with the link partner and works out speed, duplex operation, and flow control. When auto-negotiation is disabled, port speed, duplex operation, and flow control is programmable by the user.
Duplex Speed	Indicates duplex state and speed of the port.
Flow Control	Turns flow control on or off. When flow control of the port is on, it sends out a Pause frame or a Jam Packet if it is over-subscribed. When this port receives a Pause Frame or Jam Signal, it will postpone sending for a certain period to send out a frame by IEEE definition.
Default Priority	Assigns packet priority for packets arriving at the port without tagging. If the packet comes in with tag or priority-tag, the priority is retrieved from the priority field of the tag.

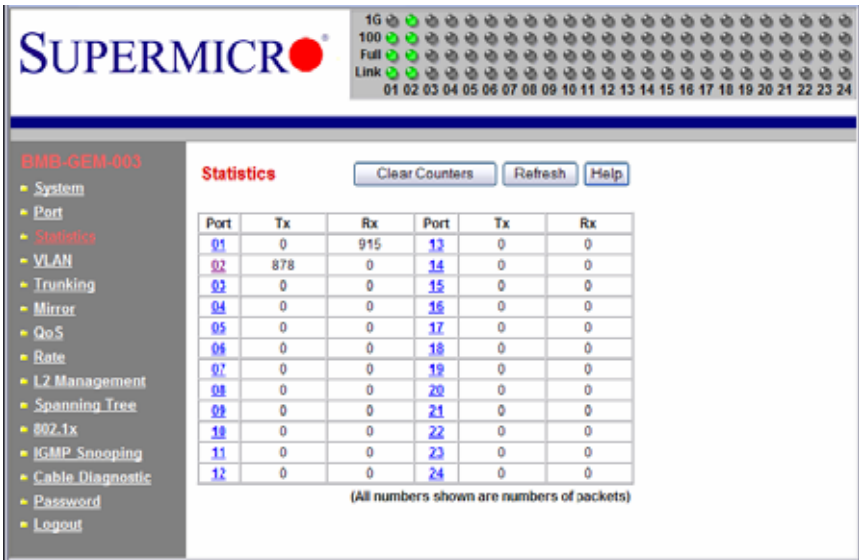
Table C-2. Port Configuration Screen Controls (Continued)

Control	Description
Jumbo Frame	Enable or Disable the jumbo frame. When a jumbo frame is enabled, the maximum length of a frame that can be forwarded by a switch is 9216. When the jumbo frame is disabled, the maximum length of a frame that can be forwarded by a switch is 1518.
PVID	Assigns default port VLAN ID for the port. When the port receives a frame which is untagged or priority tagged (VLAN ID = 0), the PVID will be used for forwarding decision for these two kind of frame.

C-2 Statistics

The STATISTICS screen displays the total number of packets transmitted or received on each port as shown in [Figure C-3](#). Click on the REFRESH button to retrieve the current count and update the screen. Click on the CLEAR COUNTERS button to reset the count to zero for each port. Click on each port number to retrieve detail statistic information for that particular port.

Figure C-3. Statistics Screen



Port Statistics

The PORT STATISTICS screen ([Figure C-4](#)) displays detailed traffic statistics for each port to help a user analyze network operations such as traffic bytes, errors, number of packets, etc. The following traffic statistics are provided for each port.

Figure C-4. Port Statistics Screen

Port Statistics [Refresh] [Help]

Port	05			
TX				
Octets	49394	UnicastPkts	0	
NonUnicastPkts	756	Discards	0	
Errors	0	QLength	0	
RX				
Octets	9170	UnicastPkts	5	
NonUnicastPkts	0	Discards	0	
Errors	0			
Summary				
DropEvents	0	UnknownPkts	0	
TotalRcvMulticastPkts	16	TotalRcvBroadcastPkts	15	
RcvUndersizePkts	0	RcvOversizePkts	0	
RcvFragments	0	RcvJabbers	0	
TxCollisions	0	RcvCRCAlignErr	0	
Total Octets Rcv	9170	Total Pkts Rcv	36	
64 Bytes Rcv Pkts	12	65-127 Bytes Rcv Pkts	7	
128-255 Bytes Rcv Pkts	0	256-511 Bytes Rcv Pkts	17	
512-1023 Bytes Rcv Pkts	0	1024-1518 Bytes Rcv Pkts	0	
1519-9216 Bytes Rcv Pkts	0	1519-9216 Bytes Tx Pkts	0	

Table C-3. Port Statistics Screen Controls

Control	Description
TX	Displays traffic information on outgoing frames.
Octets	Indicates total octets transmitted.
UnicastPkts	This indicates transmitted unicast packets.
NonUnicastPkts	This indicates transmitted nonunicast packets.
Discards	This indicates discarded packets.
Errors	This indicates Excessive Collision packets.
QLength	This indicates count of packets currently buffered.
RX	Displays traffic information on incoming frames.
Octets	Indicates total octets transmitted.
UnicastPkts	Indicates received unicast packets.
NonUnicastPkts	Indicates received non-unicast packets.
Discards	Indicates discarded packets.

Table C-3. Port Statistics Screen Controls (Continued)

Control	Description
Errors	Indicates undersize/fragment/FCS error/oversized errors with good FCS packets.
UnknownProtos	Indicates received packets using unknown protocols, such as packets that are dropped due to reasons other than drop events and storm limits.
Summary	Displays traffic information by packet type, type of error and frame size range.
DropEvents	Indicates events in which packets are dropped due to a lack of resources. This includes events where the receiving shared buffer is full, and events when a transmission failure is due to a late collision.
TotalRxMulticastPkts	Indicates the total received multicast packets.
TotalRxBroadcastPkts	Indicates the total received broadcast packets.
RxUndersizePkts	Indicates received packets with a length that is less than the minimum packet size.
RxOversizePkts	Indicates received packets with length more than maximum packet size.
RxFragments	Indicates received packets (length 10 ~ 63 bytes) with invalid FCS or alignment error.
RxJabbers	Indicates received packets (invalid FCS or code error) that exceed the counter maximum size to the maximum received frame length.
TxCollisions	Indicates the total transmitted collision packets.
RxCRCAlignErr	Indicates received packets (invalid FCS) that have a length between 64 bytes and the counter maximum size.
Total Octets Rx	Indicates total number of octets of data received (excluding framing bits, but including FCS bytes).
Total Pkts Rx	Indicates total received packet count (including all bad packets, unicast, broadcast, multicast and MAC control packets).
64 Bytes Rx Pkts	Indicates received packets with a packet length that is less than or equal to 64 bytes.
65-127 Bytes Rx Pkts	Indicates received packets with a packet length that is between (includes) 65 ~ 127 bytes.
128-255 Bytes Rx Pkts	Indicates received packets with a packet length that is between (includes) 125 ~ 255 bytes.
256-511 Bytes Rx Pkts	Indicates received packets with a packet length that is between (includes) 256 ~ 511 bytes.
512-1023 Bytes Rx Pkts	Indicates received packets with a packet length that is between (includes) 512 ~ 1023 bytes.
1024-1518 Bytes Rx Pkts	indicates received packets with a packet length that is between (includes) 1024 ~ 1518 bytes.
1519-9216 Bytes Rx Pkts	indicates received packets with a packet length that is between (includes) 1519 ~ 9216 bytes.
1519-9216 Bytes Tx Pkts	indicates transmitted packets with a packet length that is between (includes) 1519 ~ 9216 bytes.

C-3 VLAN

Virtual LAN (VLAN) is a technology used to create several independent logical networks in a physical network. Hence, it reduces the size of the broadcast domain in a network. Packets are forwarded within the same VLAN. It can also be used to combine several network segments into a same group of networks that appear as a single LAN to create a flexible and extensible LAN network system. The VLAN screen is shown in [Figure C-5](#).

Figure C-5. VLAN Screen



The switch supports an 802.1Q tagging VLAN. All packets entering the port of a switch only can be forwarded to a port that is a member of same VLAN. The ingress untagged frames are tagged by a per-port default tag (PVID). The forward decision is based on this assigned default PVID. If the ingress frames are 802.1Q tagged, the port won't alter the frames but will keep the frame's VLAN information intact. Tagged frames are forwarded according to a VID contained within the tag.

The switch also supports ingress filtering. The switch will examine the VLAN information in the incoming packets header to determine whether to drop or forward the packets. If the incoming frame has tagged VLAN information, the ingress port will check itself to see if it is a member of the tagged VLAN. If it is not, the frame will be dropped. If it's a member of the tagged VLAN, then it will check the destination port to see if it is a member of the tagged VLAN. If not, the frame is dropped. If the destination is a member of the VLAN, the frame is forwarded to the destination port. If the incoming frame is not tagged with VLAN information, the ingress port will use PVID as the VLAN ID. If the destination port is not in the same VLAN, the frame is dropped.

The switch is initially configured to have one VLAN and its VID is 1. This VLAN is called the default VLAN. By default, all ports are initially assigned to the default VLAN.

Frames can not be forwarded across VLANs. Frames, whether they are unicast, multicast or broadcast, cannot flow from one VLAN to another VLAN unless there is a VLAN routing device to bridge them.

The switch also allows a user to configure the egress packets to either tagging or untagging. The untagging feature of 802.1Q VLAN allows a user to hook up the port to a legacy switch that doesn't recognize 802.1Q tagging header in the packet. Also, the tagging feature allows VLANs to span into multiple 802.1Q compliant switches through physical connections between switches.

C-4 Configuring a Static VLAN

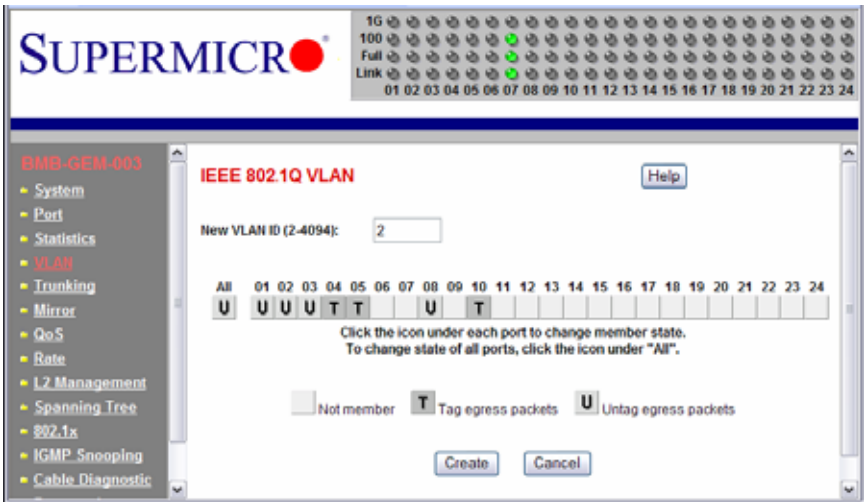
The switch currently supports static VLANs only. To configure the VLAN, click on the VLAN folder at the left-hand side bar. The IEEE802.1Q VLAN screen should appear as shown in [Figure C-5](#). It lists the entire current VLAN configuration and also allows a user to create a new VLAN or modify port membership of a VLAN. The MEMBER PORTS indicates the number of member ports of the VLAN. There are two color symbols for each port to indicate tagging or untagging of packets egress from the port:

- Orange: Indicates a tagged egress packet
- Teal: Indicates an untagged egress packet

Creating a New VLAN

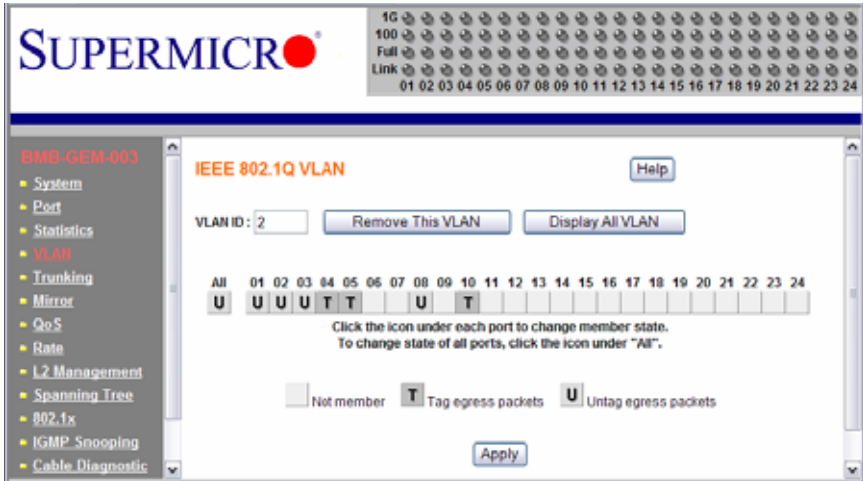
1. Click on the CREATE NEW VLAN button. The screen as shown in [Figure C-6](#) should appear.

Figure C-6. Creating a New VLAN



2. Assign a new VLAN ID, then click on the icon under each port to change the member state. There are three states to choose from: untag egress packets, tag egress packets and not member of a VLAN.
3. Click on the CREATE button to create the new VLAN. A new VLAN is shown in [Figure C-7](#).

Figure C-7. New VLAN Screen



4. If you want to remove this VLAN, click on the REMOVE THIS VLAN button. Click on DISPLAY ALL VLAN to list all of current VLAN configuration.
5. To change the port member state or remove a VLAN, select the VLAN either from the VLAN ID drop down menu or by clicking on the VLAN ID in the table in [Figure C-5](#). This screen shows the current member state of the selected VLAN. Users can modify the port member state, apply a change or remove the VLAN.

C-5 Trunking

Trunking aggregates multiple physical ports link into a single trunk to provide a single logical high-speed pipeline link. This is useful for switch-to-switch, switch-to-server and switch-to-router applications. The switch supports static type link aggregations. It uses a distribution algorithm to balance traffic between trunk members. This aggregates the bandwidth of the trunk. The switch considers a trunk as a single port entity regardless of the trunk composition.

The switch supports up to four port trunks. Each trunk consists of 2 to 8 ports. A port in one trunk cannot simultaneously be in another trunk. Link aggregation is supported only on point-to-point links with the MAC operating in full duplex mode. All links in a trunk must operate at the same data rate.

The links within a trunk should have an equal amount of traffic to achieve maximum efficiency in a multiple-link trunk. Thus, some sort of load balancing among the links in a trunk is employed. One requirement for load balancing is that the frames being transmitted must not be out of order. The switch performs load balancing based on a distribution algorithm that used the following information to assign conversation to ports:

- MAC source address

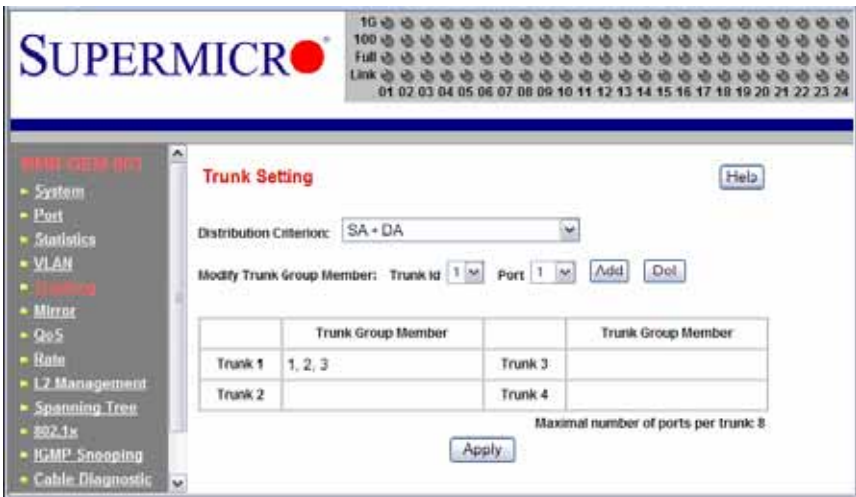
- MAC destination address
- MAC source address + destination address

The user can choose one of the distribution criteria from the configuration screen as shown in [Figure C-8](#).

Configuring the Trunk

1. Click on TRUNKING folder on left-hand side bar to bring up the TRUNK SETTING screen, as shown in [Figure C-8](#).

Figure C-8. Trunking Screen



2. Click on the TRUNK ID drop down list to select the trunk group to which you want to add port member.
3. Click on the PORT drop down list to select the port number which you want to add to the selected trunk.
4. Click on the ADD button to add it in. The port number should show up under the TRUNK GROUP MEMBER in the table. Click the DEL button to delete the port member from the selected trunk.
5. Select one of the distribution criteria for the load balancing algorithm.
6. Then, click APPLY button to update and save to a new setting.

C-6 Mirroring

The switch supports port mirroring. A copy of the egress (transmit) data and the ingress (receive) data of the mirrored (monitored) port is sent to the mirroring (snooping) port. A user can attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe to view the traffic at the mirrored port. This is useful for network monitoring and troubleshooting.

The switch allows for one mirrored port at any given time. Port mirroring is independent from L2 switching. The receive mirrored port still forwards the frame to the mirroring port, even if the frame is eventually dropped.

To configuring port mirroring, click on the MIRROR folder in the left-hand side bar. The MIRROR SETTING screen should appear as in [Figure C-9](#).

Figure C-9. Port Mirroring Screen

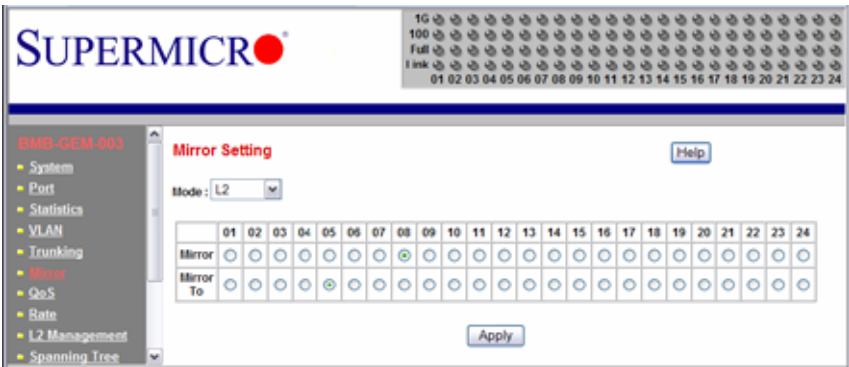


Table C-4. Port Mirroring Screen Controls

Control	Description
Mode	This enables or disables mirroring. Select L2 to enable the mirroring.
Mirror	This specifies a Mirror port to which ingress and egress traffic will be mirrored.
Mirror To	This specifies the mirrored-to port.
Apply	This applies the mirror setting to the system.

C-7 Quality of Service

Quality of Service (QoS) helps a network user to reserve a guaranteed bandwidth for some critical application functions that require a high bandwidth and high priority. Applications such as video, audio streaming, VoIP and video conferencing must have a certain amount of bandwidth to maintain their operation correctly. QoS allows user to prioritize network traffic, thereby providing better services for those applications with a higher priority.

The switch supports 802.1p priority queuing QoS based on the priority bit in a frame's VLAN header. The 802.1p priority bit, if present in the frame, specifies the priority of the frame during forwarding. The 802.1p standard uses eight (0-7) priority levels for network traffic. Priority level 7 is the highest priority. Priority level 0 is the lowest level.

Priority Queues

Four priority queues are provided for each port. The priority queues are labeled from 3 to 0. Priority queue 3 has highest priority while queue 0 has lowest priority. The switch transmits the frames based on the priority of the queue, not the priority tag. Frames in a higher priority queue are served more often than frames in a lower priority queue.

User configurable mapping (priority queue assignment) between the eight 802.1p priority classes and the four priority queues is provided. If the incoming frame is untagged, the switch uses the priority field in the per-port default priority (configurable in the PORT folder) to assign a frame to a priority queue. If the incoming frame is tagged or priority-tagged, the switch uses the priority field in the incoming frame to assign the frame to a priority queue.

The scheduling for transmission among the four priority queues is accomplished by one of the two user-configurable schemes: strict (fixed) priority and weighted round-robin.

For strict priority based scheduling, the packets which were put in the higher priority queue are transmitted first. If there are multiple frames with different priority tags in the same priority queue, the frame with higher priority level is transmitted first. After all frames in the higher priority queue have been transmitted, the frames in the lower priority queue will start transmitting.

For the weighted round-robin based scheduling, the number of packets served in the priority queue is determined by the weight number. After those packets are transmitted, the service moves to transmit the packets in the next queue. Therefore, a higher priority queue should have a higher weight number than a lower priority queue. The weight number is from 1 to 15 for the switch. If each queue has same weight number, then each queue has an equal opportunity to transmit frames just like in round-robin queuing.

To configure the QoS, click the QoS folder on the left-hand side bar. It should display as shown in [Figure C-10](#).

The QoS SETTING sets the priority relationship between the four queues, selects the scheduling method for those queues, associates packets of specific priorities to specific queues, and specifies a "weight" for each queue.

Figure C-10. QoS Setting Screen



Table C-5. QoS Setting Screen Controls

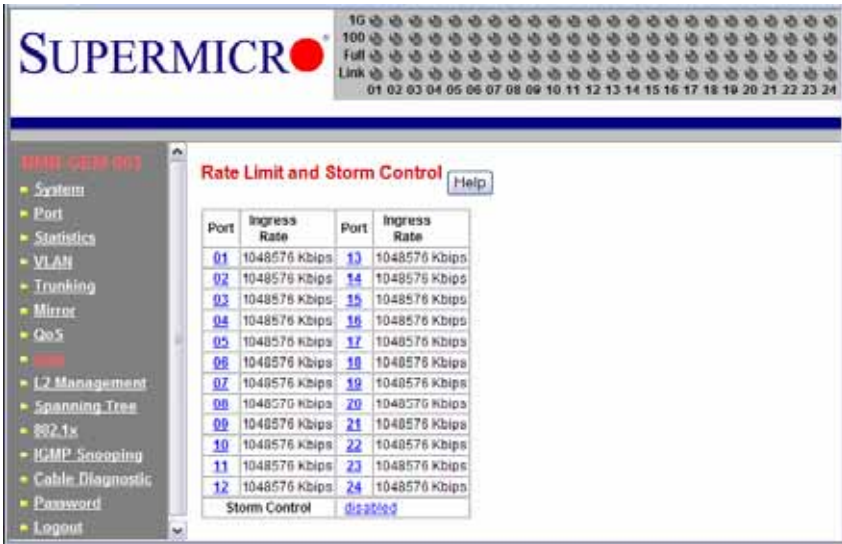
Control	Description
Scheduling Method	This specifies one of the two scheduling methods (Strict and Weighted Round-Robin) for the queues.
Queue [0:3]	Queue [0:3] prioritizes the four queues. Queue 0 is the lowest priority queue and queue 3 is the highest priority queue. Packets in queue 3 are served more often than packets in queue 0.
Priority	This indicates packet priority. This value is retrieved from the priority tag field, with values from 0 to 7. 0 indicates the lowest priority and 7 indicates the highest priority. Click on the radio button to send packets of a specific priority to a particular queue.
Weight	This indicates the weight (number of packets) to be served in the queue before moving to serve the next queue. A high priority queue should have a higher weight than a low-priority queue.

C-8 Rate Control

The switch supports per-port rate control. When the data rate of the incoming frame for a particular port exceeds a selected rate, the excess frame traffic is subject to packet drops or flow control, depending on the per-port flow control configuration in the PORT folder. If the flow control of a particular port is enabled, then the switch uses flow control to inhibit any excess traffic. If the flow control is disabled, the excess frames will be dropped.

To configure the ingress rate limit for a port, click on RATE in the left-hand side bar. The RATE LIMIT AND STORM CONTROL screen appears as [Figure C-11](#).

Figure C-11. Rate Limit and Storm Control Screen



The screen shows the Ingress Rate (in kilobits per sec) for all ports. Click on the port number to control the ingress rates for the port. There are eight different levels to select: *no limit (1Gbps), 256Kbps, 1Mbps, 4Mbps, 16Mbps, 64Mbps, 128Mbps or 512Mbps*. The STORM CONTROL indicates the current status of storm control.

A traffic storm happens when broadcast, multicast or unknown unicast packets flood the network, which will degrade the network performance. The storm control monitors the traffic of an incoming particular type of frame (configured by the user) and limits traffic to a user configurable rate level (threshold). The storm rate threshold is counted in number of packets per second (pps). If the traffic of a particular frame type exceeds the threshold during one second, all the rest of that type of frame will be dropped before the end of that second.

The switch provides configuration to assign storm control type and rate limitations to the entire system.

To configure storm control, click on the link at STORM CONTROL OF RATE LIMIT and STORM CONTROL screen as shown in [Figure C-11](#). The STORM CONTROL screen should appear as shown in [Figure C-12](#).

Figure C-12. Storm Control Screen

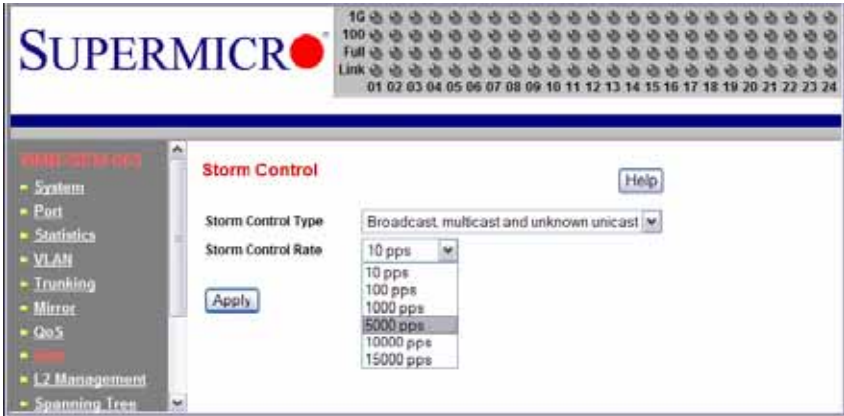


Table C-6. Storm Control Screen Controls

Control	Description
Storm Control Type	This selects the type of the packet storm. The figure below shows all available options: Broadcast only, Broadcast and multicast, Broadcast unknown unicast and Broadcast, multicast, and unknown unicast.
Storm Control Rate	This selects a rate (packets-per-second) for storm control. The figure below shows all available options: 10 pps 100 pps 1000 pps 5000 pps 10000 pps and 15000 pps.

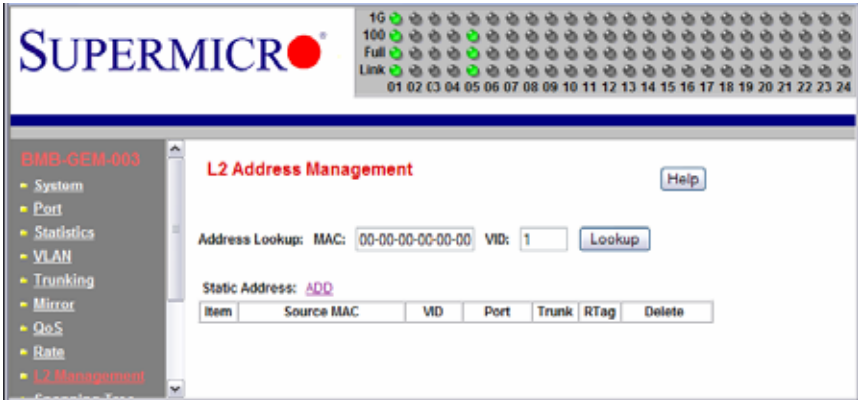
C-9 L2 Management

L2 management provides a way to add, delete, and look up MAC addresses in the L2 address table. The switch supports 8192 L2 address table entries, each specifying a MAC address, VLAN ID, destination port number, trunk ID and Rtag. The switch supports store-and-forward mode switching.

After a frame is received, its source MAC address (MACSA) and destination MAC address (MACDA) are retrieved. Depending on the port state, the MACSA and port number may be used to dynamically update the L2 address table. The MACDA may be used to determine the frame's destination port. User can also statically add a MAC address to the L2 address table.

To add a static entry into the L2 ADDRESS table, click on the ADD link on the L2 ADDRESS MANAGEMENT screen as shown in [Figure C-13](#).

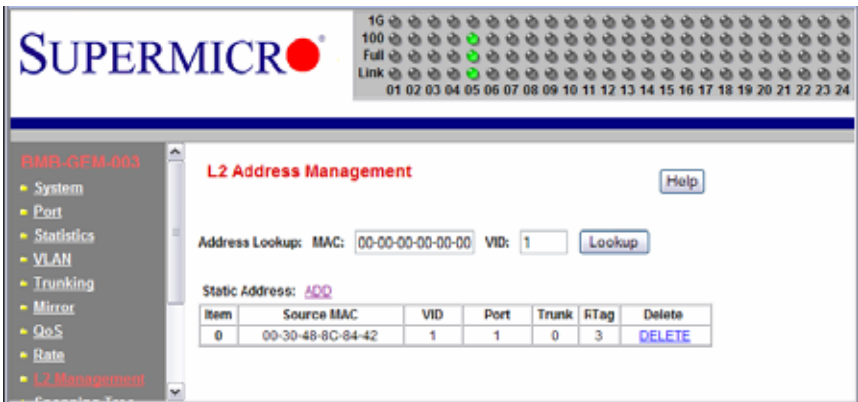
Figure C-13. L2 Management Screen



To remove the specified static MAC address from the table, click the DELETE link for that MAC address as shown in Figure C-14 when there are static entries in the table.

To search for a MAC address to see if it exists in the table or not, enter the MAC ADDRESS and VID, then click on LOOKUP button. If the MAC address is in L2 ADDRESS table, whether it is a static or a dynamic MAC address, the result will be displayed.

Figure C-14. L2 Management: Current Entries Screen



C-10 Spanning Tree

The Spanning Tree Protocol (STP) helps to detect and prevents loops from occurring on a switched or bridged network. When multiple paths exist on a network, STP will configure the network to use the most efficient path between network devices. All other paths are forced into a blocked standby state. If the active path fails, then STP will automatically select another path to become active path on the network to sustain normal network operations. An active path is selected by comparing path costs defined on each path. The path with the lowest cost will be selected.

The switch supports IEEE802.1d Spanning Tree Protocol and IEEE802.1w Rapid Spanning Tree Protocol (RSTP). The Rapid Spanning Tree Protocol significantly reduces the convergence time by assigning port roles and by determining the active topology. A reconfiguration of the spanning tree can occur in less than one second. The RSTP is backward compatible with the legacy device running IEEE802.1d STP and serves as an STP device when an STP device is present in the network.

Bridge Protocol Data Unit (BPDU)

The spanning tree is built by obtaining switch information by exchanging Bridge Protocol Data Unit (BPDU) packets among the participating switches. When RSTP is enabled for a switch, it will generate a BPDU and periodically forward it out through each port on the switch. The interval is configurable through the Hello Time, which is set to a two second default. This enables the switch to keep track of network topology changes and enable or disable ports as required.

The BPDU contains the information about the transmitting switch and its ports including MAC address, bridge priority, port priority and port path cost. The BPDU packet is sent out by using the unique MAC address of the port itself as a source address, and the destination address of the STP multicast address 01:80:C2:00:00:00.

There are three types of BPDUs:

- Configuration BPDU – for spanning tree computation
- Topology Change Notification (TCN) BPDU – announces changes in network topology.
- Topology Change Notification Acknowledge (TCA) BPDU

The major operation of the spanning tree protocol includes a root bridge election, finding paths to a root bridge, determining the least cost path to root and disabling all other root paths. When a RSTP enabled switch is turned on, it automatically assumes that it is the root bridge in the spanning tree. The software in the switch will elect a switch as the root bridge based on the Bridge ID in the received BPDU. The Bridge ID is an 8-byte field which combines a high order two-byte bridge priority number and a lower order six-byte switch MAC address. The switch with the lowest Bridge ID will be elected as the root bridge.

All RSTP participating switches will use an algorithm to determine how close they are to the root bridge, which is known as Path Cost. The path with lowest cost will be selected as the active path. All others will be blocked (standby). TCN packets are injected into the network by a non-root switch and propagated to the root. Upon receipt of the TCN, the

root switch will set a Topology Change flag in its normal BPDUs. This flag is propagated to all other switches to instruct them to rapidly age out their forwarding table entries.

Port Transition State

When a device is connected to an RTSP or STP enabled switch port for the first time, it will not immediately start to forward data. Instead, it will go through a number of states while it processes BPDUs and determines the network topology.

There are five port states in the legacy 802.1d STP: *disabled*, *blocking*, *listening*, *learning* and *forwarding*. The RSTP combines the *disabled*, *blocking* and *listening* states used in 802.1d STP and creates a single state: *Discarding*. [Table C-7](#) lists the comparison of port states between 802.1d STP and 802.1w RSTP.

Table C-7. Comparison of Port States

State Displayed	802.1d STP	802.1w RSTP
Discarding	Disabled	Discarding
Discarding	Blocking	Discarding
Discarding	Listening	Discarding
Learning	Learning	Learning
Forwarding	Forwarding	Forwarding

RSTP Port Roles

RSTP will assign port roles for each port during the process receiving the BPDUs. Based on its port role, a port can either send or receive BPDUs and forward or block data traffic.

- **Root** – the port that provides the lowest cost path when the switch forwards packets to the root switch.
- **Designated** – the port closest to the root switch and forwarding traffic toward the root switch and sending BPDUs in a link segment. Each designated port is in a forwarding state.
- **Alternate** – this port provides an alternate path to the root bridge. This path is different than using the root port. The alternate port is in a blocking state.
- **Backup** – the port provides a backup/redundant path to a link segment to which another switch port already connects. This is a special case when two or more ports of the same switch are connected together.
- **Disabled** - Not a strictly part of RSTP, a network administrator can manually disable a port.

To configure the RAPID SPANNING TREE, click the SPANNING TREE folder on the left-hand side bar. There are two portions to configure: RSTP SWITCH SETTINGS and RSTP PORT SETTINGS, as shown in [Figure C-15](#).

The RSTP SWITCH SETTINGS allows the user to control RSTP parameters from the bridge point-of-view. ROOT STATUS shows status of the root bridge. BRIDGE SETTING shows the current bridge setup.

To turn on the Rapid Spanning Tree Protocol (RSTP), check on the ENABLE RSTP dialog box and click on the APPLY GLOBAL SETTINGS button.

Root Status

The settings for ROOT STATUS are shown below:

- **Designated Root Bridge** – The bridge identifier of the root of the spanning tree is determined by the RSTP protocol as executed by this node. The bridge identifier value is used as the Root Identifier parameter in all configuration Bridge PDUs originated by this node.
- **Max Age** – This indicates the maximum age of the root bridge. This is the maximum age of spanning tree protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
- **Hello Time** – This indicates the amount of hello time of the root bridge. Hello time is the amount of time between the transmission of configuration Bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so, in units of hundredths of a second.
- **Forward Delay** – This indicates the amount of forward delay of the root bridge. Forward delay is a time value, measured in units of hundredths of a second, which controls how fast a port changes its state. The value determines how long the port stays in each of the listening and learning states, which precede the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway.

Bridge Setting

Settings for Bridge Setting are shown below:

- **Priority** – This configures the priority of the current bridge.
- **Max Age** – This configures the maximum age of the current bridge. This is the maximum age of spanning tree protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
- **Hello Time** – This indicates the amount of hello time of the current bridge. Hello time is the amount of time between the transmission of configuration Bridge PDUs by this node on any port when it is the root of the spanning tree or trying to become so, in units of hundredths of a second.
- **Forward Delay** – This indicates the amount of forward delay of the current bridge. Forward delay is a time value, measured in units of hundredths of a second, which controls how fast a port changes its state. This value determines how long the port stays in each of the listening and learning states, which precede the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway.

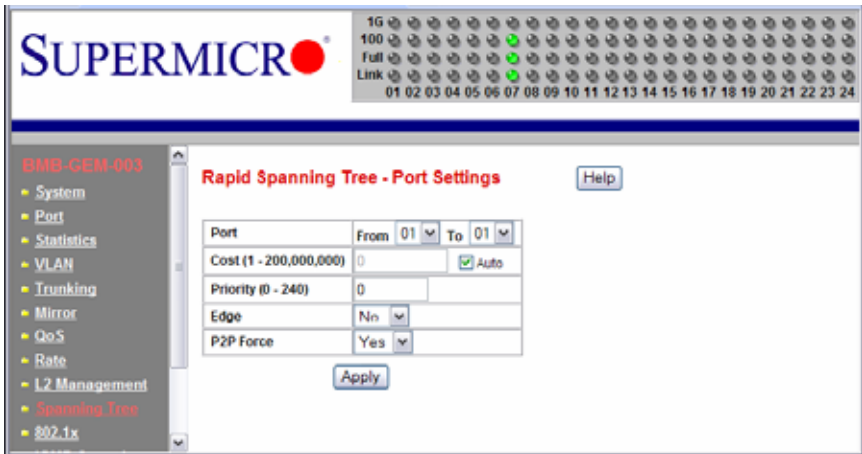
RSTP Port Settings

These settings control and monitor the port-based spanning tree status.

- **Participate** – This specifies if the RSTP is enabled or not for the selected port.
- **Cost** – Displays the cost of this port. “Cost” means the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Priority** – Displays the priority of this port. This is the value of the priority field contained in the first octet of the Port ID.
- **Edge** – This indicates if this port is the edge port. Once configured as an edge port, the port immediately transitions to the forwarding state. It is available only when the port is directly connected to an end terminal (or a file server) that has no influence on the spanning tree configuration. Since ports 11 to 24 are connected to blade server NIC ports, all of those ports can be configured as an Edge port.
- **P2P** – This indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
- **Status** – This displays the RSTP port status.
- **Role** – This displays the role of this port.

To modify the PORT SETTINGS for each port, click on the EDIT link next to PORT SETTING. Figure C-15 will appear.

Figure C-15. Rapid Spanning Tree Port Settings



Select a group of port numbers that you want to configure. Setting the COST to zero or checking AUTO will automatically set the default value depending on the link speed. The default cost is 20000 for a Gigabit port and is 100000 for a 100Mbps port.

C-11 IEEE 802.1x

IEEE 802.1x is a client-server based access control and authentication protocol that restricts unauthorized user devices from connecting to the LAN through publicly accessible ports. This port-based access control is accomplished by using a RADIUS server that is connected to a gigabit switch management port to authenticate client users trying to access a network through the switch. The gigabit switch will relay Extensible Authentication Protocol over LAN (EAPoL) packets between the user client and the RADIUS server. The 802.1x protocol consists of three components: client, authenticator and authentication server.

The Authentication Server is a remote device that runs the RADIUS server program (Windows 2000/2003 IAS™, freeRADIUS™ from open source). The role of the Authentication Server is to certify the identity of a client attempting to access the network. By exchanging secure information between the RADIUS server and the client through EAPoL packets, the Authentication Server will inform the switch whether or not the client is granted access to the LAN through the connected port.

The client is a workstation that wishes to access the network through a connected switch port. All workstations have to run a program (supplicant) that is compliant with the 802.1x protocol. Microsoft Windows XP™ and Vista™ should have this. A user can also install another third party package, such as Odyssey® from Funk Software®.

When the GLOBAL RADIUS SETTING and SET STATUS of an individual port are enabled, that port will initially be placed into an unauthorized state. The client will initiate negotiations by sending an EAPoL START packet.

There are several EAP authentication methods available in Microsoft Windows XP, such as *EAP-MD5*, *EAP-TLS* and *EAP-PEAP*. Currently, the gigabit switch only supports *EAP-MD5* for 802.1x authentication.

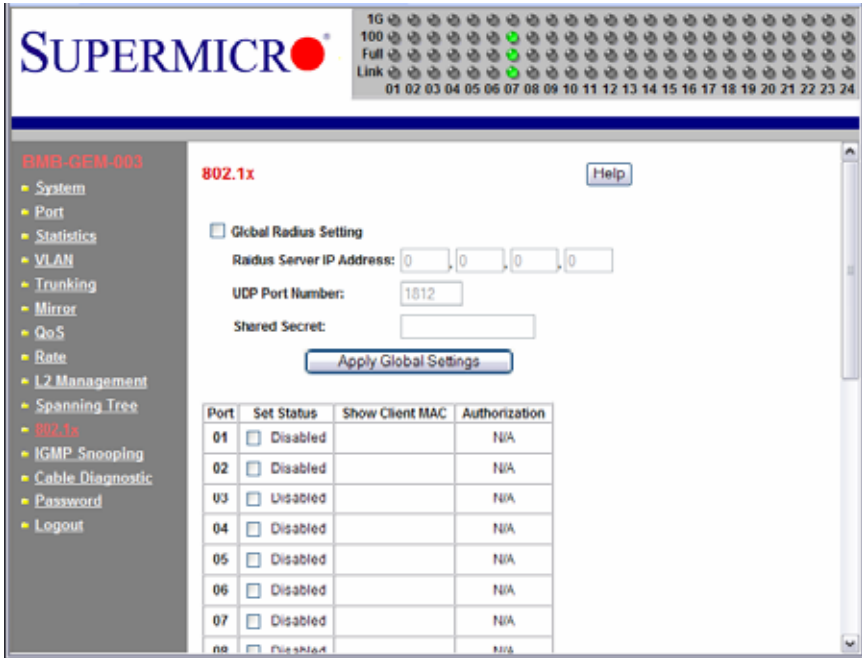
- **PEAP-MS-CHAP v2** uses password-based credentials and requires computer certificates on the RADIUS servers.
- **EAP-TLS** uses certificate-based credentials and requires user and computer certificates on the wire's client computers and computer certificates on the RADIUS servers.
- **EAP-MD5** (Message Digest 5) Challenge Handshake Authentication Protocol (MD5 CHAP), which uses passwords.

Wiring for 802.1x

The EAPoL packets are handled by a management processor in the switch. The processor communicates with the outside world through three ports. Two ports (eth0 and eth1) are connected to the CMM module's Ethernet port and the third port (eth2) is connected to all 24 switching ports. Only one port is enabled at any time. The regular configuration setup switch is managed through the CMM Ethernet port. Thus, for regular deployment, the RADIUS server should be located where it can be reached from the CMM Ethernet port.

802.1x Configuration

Figure C-16. 802.1x Configuration Screen



To configure 802.1x port based access control, click on the 802.1x folder in the left-hand side bar. The 802.1x configuration should display as shown in [Figure C-16](#). Check the GLOBAL RADIUS SETTING dialog box to enable 802.1x port based access control.

- **Radius Server IP Address** – This indicates the IP address of the RADIUS server.
- **UDP Port Number** – This specifies the UDP port number of the EAPOL control frame. 1812 is the default UDP port number. If the RADIUS server can't recognize them, other numbers can be used.
- **Shared Secret** – This is a 16-character string used by the RADIUS server as a password to identify EAPOL control frames.

The PORT AUTHENTICATION SETTINGS allows you to enable or disable authentication for individual ports. It also displays the results when a port is enabled for authentication.

- **Set Status** – This enables or disables port authentication. ENABLE PORT AUTHENTICATION STATUS means a port should be authorized by a RADIUS server to forward traffic. No traffic is forwarded if it is unauthorized. No authentication process is required for those ports in disabled status; traffic can be forwarded normally.
- **Show Client MAC** – This displays the last client in the MAC address who sent out the EAPOL control frame of the port.

- **Authorization** – This displays the authentication status of an enabled port. It includes the following status:
- **In Progress** – This indicates that the authentication is still in progress. Traffic is not forwarded before authentication is verified.
 - **Yes** indicates the port access is authorized.
 - **No** indicates the port access is not authorized.
 - **N/A** means no authentication required.

C-12 IGMP Snooping

IP multicast is often used to distribute video/audio multimedia data over the network. The layer 2 switch will flood multicast frames to all of ports of switch, which wastes a lot of unnecessary network bandwidth. IGMP is a standard defined in RFC1112 for IGMPv1 and in RFC2236 for IGMPv2. IGMP specifies how a host can register a router in order to receive specific multicast traffic. A layer 3 switch usually supports Internet Group Management Protocol (IGMP) to manage multicast groups by sending and processing IGMP packets. To prevent the unnecessary flooding, the gigabit layer 2 switch can enable the *IGMP snooping* function to control how IP multicast packets are forwarded to required ports by monitoring IGMP queries and response packets generated by layer 3 switches or the IGMP querier.

Currently, the gigabit switch supports IGMP snooping for IGMP v1/v2 packets. In the real network setup, the switch is seated between the Multicast Router/Server and the host. The Multicast Router/Server will periodically send an IGMP v2 query packet and the host will respond with an IGMP v2 report packet if the host is in the same multicast group. When the host wants to go away, it can send an IGMP v2 Leave packet. The switch will remove the connected port number from the multicast group entry of a table. If the host is just silently removed, then the switch will clean it from table when the timer expires.

[Figure C-17](#) shows the IGMP SNOOPING configuration screen. [Table C-8](#) describes each configuration item.

Figure C-17. IGMP Snooping Screen

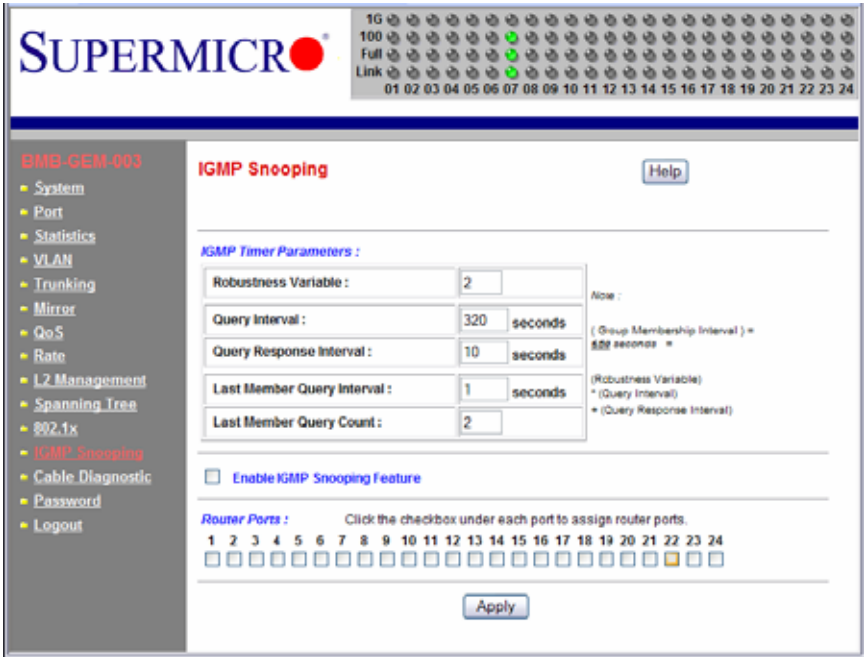


Table C-8. IGMP Snooping Screen Controls

Control	Description
Robustness Variable	This allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable-1) packet losses. The Robustness Variable must not be 0, and should not be 1. The default value is 2.
Query Interval	This is the interval between general queries sent by the querier. The default interval is 125 seconds. By varying the [Query Interval], an administrator may tune the number of IGMP messages on the subnet; larger values cause IGMP queries to be sent less often.
Query Response Interval	This is the maximum response time inserted into the periodic general queries. The default value is 100 (10 seconds) By varying the query response interval, an administrator can tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty, as host responses are spread out over a larger interval. The number of seconds represented by the query response interval must be less than the query interval.
Last Member Query Interval	This is the maximum response time inserted into group-specific queries sent in response to Leave Group messages, and is also the amount of time between group-specific query messages. The default value is 10 (1 second). This value may be tuned to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group.
Last Member Query Count	This is the number of Group-Specific Queries sent before the router assumes there are no local members. Default: the Robustness Variable.
Enable IGMP Snooping Feature	This is used to enable the IGMP snooping feature.
Router Ports	This specifies ports to which IGMP routers were connected.

C-13 SNMP

The SNMP agent in the gigabit switch supports SNMP v1 and v2c. It also supports the following MIB:

- RFC1213 MIBII with standard sets which include system, interfaces, IP, ICMP, TCP, UDP, Dot3, and SNMP.
- RFC2011 SNMPv2 MIB for IP using SMIv2
- RFC2665 EtherLike MIB

C-14 UpLink Failure Tracking (ULFT)

This feature applies for firmware version 1.09 and after.

Uplink Failure Tracking (ULFT) feature is provided to support network adapter Teaming or Channel Bonding on SuperBlade servers.

Installing two GbE switch modules can have additional connectivity to achieve network redundancy and fault tolerance. The connection between internal ports of the switch and each LAN port of the server blades is hardwired through the middle plane. The link will not be dropped unless either switch's internal port or the server blade's LAN port fails.

By enabling the ULFT feature with proper pair configuration, it can trigger a failover event in the Teaming or Channel Bonding program when all of a switch's external uplink member ports fail. The switch automatically enables the internal downlink ports once one of the uplink ports in the configured pair returns to service.



NOTE: By default, the switch's ULFT feature is disabled. The link status on the external uplink ports does not affect the link status of internal downlink ports.

To use ULFT, you must configure a Failure Tracking Pair and enable the ULFT feature. A Failure Tracking pair consists of uplink and downlink ports. The uplink tracking member contains port 1 to port 10. The downlink tracking member contains port 11 to port 24.

If the trunking on the external uplink ports is enabled, then you should put all of the trunk member ports as a tracking pair's uplink member. The link to the configured internal downlink member ports is disabled when all of the trunking uplink member ports fail.

[Figure C-18](#) shows the IGMP SNOOPING configuration screen. [Table C-9](#) describes each configuration item.

Figure C-18. Uplink Failure Tracking Configuration Screen

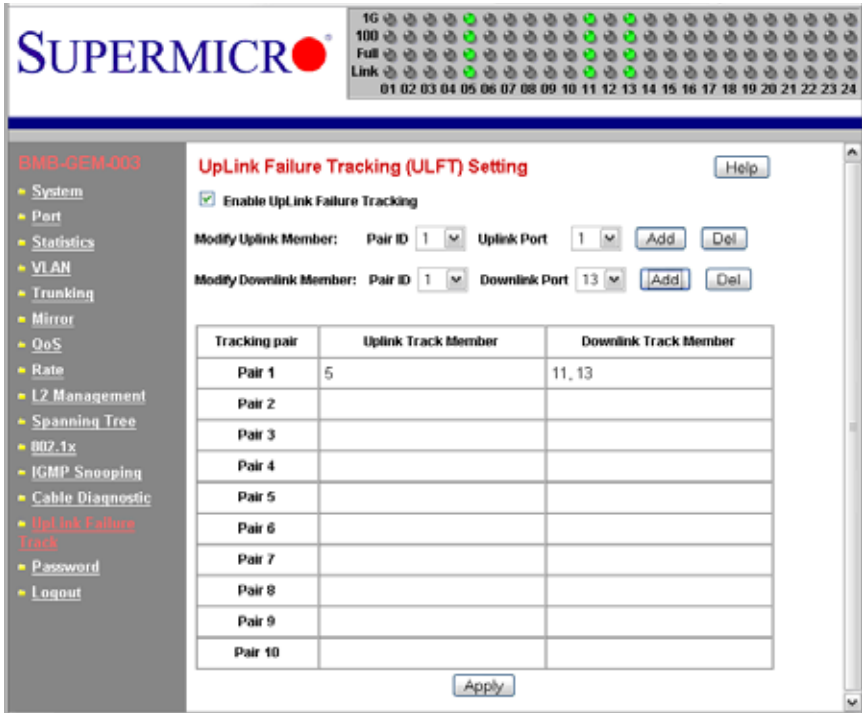


Table C-9. Uplink Failure Tracking Configuration Screen Controls

Control	Description
Enable UpLink Failure Tracking	Enables/Disables the UPLINK FAILURE TRACKING feature.
Modify Uplink Member	Select the pair ID and uplink port number to add/delete to/from uplink member of a pair.
Modify Downlink Member	Select the pair ID and downlink port number to add/delete to/from downlink member of a pair.
Uplink Track Member	This column defines member ports of an uplink in a ULFT pair.
Downlink Track Member	This column defines member ports of a downlink in a ULFT pair.

For example if your SuperBlade has two blade servers installed on slot 1 and slot 3, then each blade has two LAN ports, one connected to the internal port of the upper GbE switch and the other one connected to the internal port of the bottom GbE switch. To implement switch redundancy, you need to have two GbE switches installed. Each of these GbE switches should enable the UpLink Failure Tracking feature and have the proper configuration as shown in [Figure C-18](#).

The pair configuration defines the ULFT for blade 1 and blade 3. External port 5 of each switch is connected to an external third party switch through an Ethernet cable. This assumes that the Network Adapter Teaming or Channel Bonding has a proper configuration and is running on each of the blades.

If one of the external Ethernet cables is broken or the third party switch port to which the cable connects fails, then one of the SuperBlade GbE switches will detect a link drop on its external port 5 and turn down the link on its internal port 11 and 13. The Teaming or Channel Bonding software running on both of these blades then detects a link drop on one of its LAN ports and switches to another LAN port automatically. This allows network traffic to go through another GbE switch.

Appendix D

System Specifications

D-1 Blade Specifications

Table D-1. SBA-7141M-T Blade Specification Features

Mainboard	BHQME (proprietary form factor) Dimensions (W x D): 11 x 12.8 in (279 x 325 mm)
Processors	Four AMD Opteron 8300/8200 series processors Please refer to our web site for a complete listing of supported processors.
Chipset	NVidia MCP55 Pro chipset
Graphics Controller	ATI ES1000 (RN50) with 16 MB of SDRAM
BIOS	AMI® Flash ROM
Memory Capacity	Sixteen 240-pin DIMM sockets supporting up to 64 GB of ECC Registered DDR2-667/533/400 SDRAM. NOTE: See Section 5-6 for details.
SATA Controller	Intel 82571EB dual-port Gigabit controller
Hard Drive Bays	Single on-board 2.5" SATA disk drive

Table D-2. SBA-7121M-T1 Blade Specification Features

Mainboard	BHDME (proprietary form factor) Dimensions (W x D): 11 x 12.8 in (279 x 325 mm)
Processors	Two AMD Quad/Dual-Core Opteron 2000 series processors Please refer to our web site for a complete listing of supported processors.
Chipset	NVidia MCP55 Pro chipset
Graphics Controller	ATI ES1000 (RN50) with 16 MB of SDRAM
BIOS	AMI® Flash ROM
Memory Capacity	Eight 240-pin DIMM sockets supporting up to 64 GB of ECCRegistered DDR2-667/533/400 SDRAM. NOTE: See Section 5-6 for details.
SATA Controller	Intel 82571EB dual-port Gigabit controller
Hard Drive Bays	Two hot-plug 3.5" SATA disk drives

D-2 Enclosure Specifications

Table D-3. Enclosure Specification Features

Enclosure	SBE-710E or SBE-714D series rackmount blade enclosure Dimensions: (WxHxD) 18.5 x 12.1 x 29 in. (470 x 307 x 737 mm)
Blade Module Support	Up to 10 hot-plug blade modules (supports mixing of Intel and AMD blades)
System Cooling	Up to sixteen (16) cooling fans
Power Supplies (2 or 4 modules required)	Rated Output Power: 2000W (Part# PWS-2K01-BR, C-20 type socket) Rated Output Voltages: +12V (166A), +5Vsb (16A)
System Input Requirements	AC Input Voltage: 200-240V AC auto-range Rated Input Current: 10A - 14A Rated Input Frequency: 50 to 60 Hz
BTU Rating	7584 BTUs/hr (for rated output power of 2000W)

D-3 Environmental Specifications

Table D-4. Environmental Specification Features

Operating Environment	Operating Temperature: 10° to 35° C (50° to 95° F)
	Non-operating Temperature: -40° to 70° C (-40° to 158° F)
	Operating Relative Humidity: 8% to 90% (non-condensing)
	Non-operating Relative Humidity: 5 to 95% (non-condensing)
Regulatory Compliance	Electromagnetic Emissions: FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A
	Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)
Safety	EN 60950/IEC 60950-Compliant, UL Listed (USA), CUL Listed (Canada), TUV Certified (Germany), CE Marking (Europe) California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate "

D-4 Address Defaults

Table D-5. Address Default Features

CMM Module	IP Address: 192.168.100.100
	Gateway Address: 0.0.0.0
	Subnet Mask: 255.255.255.0
GbE Switch	User Name and Password: ADMIN and ADMIN (case sensitive)
	IP Address: 192.168.100.102
	Gateway Address: 192.168.100.1
	Subnet Mask: 255.255.255.0

D-5 Power Supply Power Calculations

Table D-6. Power Supply: Power Calculations (PWS-2K01-BR)

Calculation	Value
Watts	2000
Volts (High/Low)	240/200
Amps (High/Low)	12.3/10.3
Efficiency (High)	90%
Efficiency (Low)	80%
Power Factor (High)	98%
Power Factor (Low)	90%
10% Reserve (High)	1.2
10% Reserve (Low)	1.0
Amps (Total)	13.6@240 volts

Notes

Table D-7. Power Supply: Power Calculations (PWS-1K41-BR)

Calculation	Value
Watts	1400
Volts (High/Low)	240/100
Amps (High/Low)	14.0/7.2
Efficiency (High)	93%
Efficiency (Low)	80%
Power Factor (High)	99%
Power Factor (Low)	90%
10% Reserve (High)	1.4
10% Reserve (Low)	0.7
Amps (Total)	9.5@240 volts 15.4@100 volts

Appendix E

iSCSI Setup Procedure

This appendix covers the iSCSI setup procedure for Supermicro blade systems. If you do not wish to employ this optional interface for your blades, then skip this procedure in your blade setup.



NOTE: iSCSI installation requires two (2) network switch/pass-thru modules to implement.

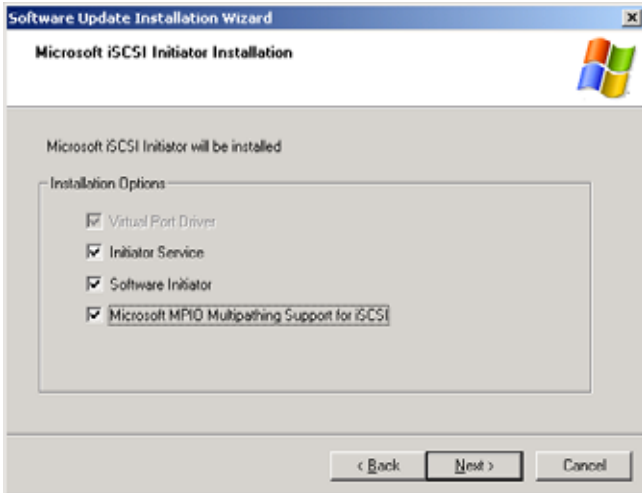
To implement iSCSI use in Supermicro blade systems, use the procedure below:

1. On boot-up press CTRL-D to go to the iSCSI PORT SELECTION screen.
2. Set one port to **Primary** and press <ENTER>.
3. Select the iSCSI BOOT CONFIGURATION option.
4. For DYNAMIC IP CONFIGURATION (DHCP) enter information for the following settings:
 - Initiator Name
 - Initiation IP
 - Subnet Mask
 - Gateway
 - VLAN ID
5. For USE DHCP FOR iSCSI TARGET INFORMATION enter information for the following settings, and then select OK to continue:
 - Target Name
 - Target IP
 - Target Port
 - Boot LUN
6. Select SAVE CHANGES AND EXIT on the setup screen.
7. Put the *Windows Installation CD* into the CD-ROM drive. In Windows press F6 to load the *Intel(R) iSCSI Setup* driver from the disc.
 - a. If you installed *Windows 2003 32-bit SP1 or SP1 R2* then install the *Microsoft Hotfix for Windows Server, KB902113 NDIS QFE*. Windows 2003 SP2 contains the QFE.
 - b. To Install Windows 2003 x64 you must first create an operating system installation media including a *Hot Fix* referenced from *KB article #934848* at:

<http://support.microsoft.com/kb/934848/en-us>

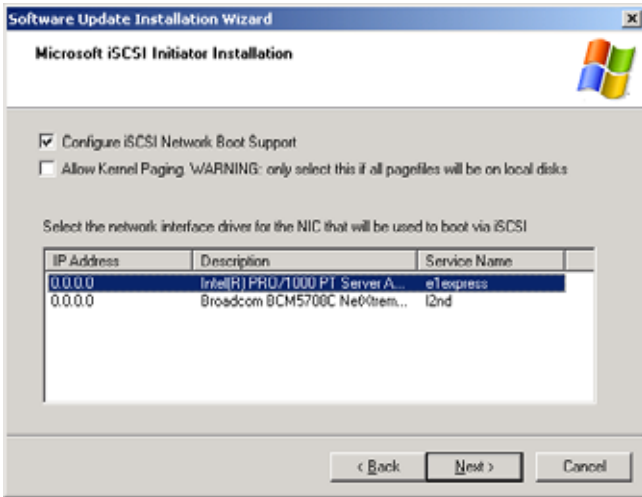
8. Copy the following Windows drivers to your desktop (or a convenient directory for later reference and use):
 - Intel Network Driver
 - Microsoft iSCSI Software Initiator with integrated software boot support
 - ISBOOT.exe
9. Bring up the WINDOWS DEVICE MANAGER screen, and under devices, highlight the second ETHERNET CONTROLLER (under OTHER DEVICES).
10. Select UPDATE DRIVER from the right-click menu. When prompted for the driver file, point to where you saved the driver files and windows will pick it up for installation.
11. Launch the MS ISCSI INITIATOR file that you saved previously, and do the following actions on the MICROSOFT ISCSI INITIATOR INSTALLATION screens that appear:
 - a. Go through the first two screens and on the third screen check the MICROSOFT MPIO MULTIPATHING SUPPORT FOR ISCSI check box (Figure E-1).

Figure E-1. Microsoft MPIO Multipathing Support for iSCSI Check Box



- b. On the next screen check the CONFIGURE ISCSI NETWORK BOOT SUPPORT check box and select the INTEL GIGABIT ADAPTER identified as **e1express** (Figure E-2).

Figure E-2. Configure iSCSI Network Boot Support Check Box



- c. In the next screen select AGREE.
 - d. In the final screen, click FINISH.
12. Reboot the system.
 13. Launch the *ISBOOT.exe* file. It will create an *Intel/12.3* folder on your system. In this new folder look for either the *WIN32* folder for 32-bit Windows installation, or the *WINX64* folder for 64-bit installation.
 14. In the *WIN32* folder launch the *iSCSIAPP.exe* file for 32-bit installation, or in the *WINX64* folder launch the *iSCSIAPP.exe* file. In the window that appears select first YES and then OK at the prompts.
 15. Reboot the system and press CTRL-D to go back to the iSCSI PORT SELECTION screen. In this screen disable the first primary port and then enable the second port to **Primary**.
 16. Repeat [step 3](#) through [step 6](#) above to configure the new port.
 17. Update the network driver in the WINDOWS DEVICE MANAGER for the **first** Ethernet controller by highlighting the first listed ETHERNET CONTROLLER (under OTHER DEVICES) and selecting UPDATE DRIVER from the right-click menu.

When prompted for the driver file, point to where you saved the driver files and windows will pick it up for installation.
 18. Uninstall the *Intel(R) iSCSI Setup* driver in the WINDOWS DEVICE MANAGER window (right-click UNINSTALL).

19. Open the WINDOWS COMMAND PROMPT terminal window and type

iscsibcg /verify /fix

in the window and press <ENTER>.

20. Reboot the system.