R151-Z30

SP3 socket motherboard for the AMD EPYC Series Processor family

Service Guide

Rev. 1.0

Copyright

© 2018 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.
The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

Information in this manual is protected by copyright laws and is the property of GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

Documentation Classifications

In order to assist in the use of this product, GIGABYTE provides the following types of documentations:

- For detailed product information, carefully read the User's Manual.

For More Information

For related product specifications, the latest firmware and software, and related information, please visit our website at:

http://www.gigabyte.com

For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal:

http://reseller.b2b.gigabyte.com

For further information & technical assistance, please contact your GIGABYTE sales representative.
You may also message GIGABYTE server directly by email, Facebook or twitter

Email: server.grp@gigabyte.com

Facebook: https://www.facebook.com/gigabyteserver

Twitter: https://twitter.com/GIGABYTEServer

Conventions

The following conventions are used in this user's guide:

	**NOTE!** Gives bits and pieces of additional information related to the current topic.
	**CAUTION!** Gives precautionary measures to avoid possible hardware or software problems.
	**WARNING!** Alerts you to any damage that might result from doing or not doing specific actions.

Server Warnings and Cautions

Before installing a server, be sure that you understand the following warnings and cautions.



WARNING!

To reduce the risk of electric shock or damage to the equipment:

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.



WARNING!

To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.



WARNING!

This server is equipped with high speed fans. Keep away from hazardous moving fan blades during servicing.



CAUTION!

- Do not operate the server for long periods with the access panel open or removed. Operating the server in this manner results in improper airflow and improper cooling that can lead to thermal damage.
- Danger of explosion if battery is incorrectly replaced.
- Replace only with the same or equivalent type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

Electrostatic Discharge (ESD)

CAUTION!

ESD CAN DAMAGE DRIVES, BOARDS, AND OTHER PARTS. WE RECOMMEND THAT YOU PERFORM ALL PROCEDURES AT AN ESD WORKSTATION. IF ONE IS NOT AVAILABLE, PROVIDE SOME ESD PROTECTION BY WEARING AN ANTI-STATIC WRIST STRAP ATTACHED TO CHASSIS GROUND -- ANY UNPAINTED METAL SURFACE -- ON YOUR SERVER WHEN HANDLING PARTS.

Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges without any component and pin touching. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

System power on/off: To remove power from system, you must remove the system from rack. Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

Hazardous conditions, devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system and disconnect the cables attached to the system before servicing it. Otherwise, personal injury or equipment damage can result.

Electrostatic discharge (ESD) and ESD protection: ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground (any unpainted metal surface on the server) when handling parts.

ESD and handling boards: Always handle boards carefully. They can be extremely sensitive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Installing or removing jumpers: A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that can be gripped with fingertips or with a pair of fine needle nosed pliers. If the jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.



CAUTION!

Risk of explosion if battery is replaced incorrectly or with an incorrect type. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Table of Contents

Chapter 1 Hardware Installation 10
1-1 Installation Precautions 10
1-2 Product Specifications 11
1-3 System Block Diagram 14
Chapter 2 System Appearance 16
2-1 Front View 16
2-2 Rear View 16
2-3 Front Panel LED and Buttons 17
2-4 Rear System LAN LEDs 18
2-5 Hard Disk Drive LEDs 19
2-6 Power Supply Unit LED 20
Chapter 3 System Hardware Installation 22
3-1 Removing and Installing the Chassis Cover 23
3-2 Removing and Installing the Fan Duct 24
3-3 Removing and Installing the CPU and Heat Sink 25
3-4 Removing and Installing Memory 27
3-4-1 8-Channel Memory Configuration 27
3-4-2 Removing and Installing a Memory Module 28
3-4-3 DIMM Population Table 28
3-5 Removing and Installing the PCI Expansion Card 30
3-6 Removing and Installing the Hard Disk Drive 31
3-7 Installing and Removing an M.2 Solid State Drive 32
3-8 Replacing the Fan Assembly 33
3-8-1 Fan Connector Table 33
3-9 Removing and Installing the Power Supply 34
3-10 Cable Routing 35
Chapter 4 Motherboard Components 37
4-1 Motherboard Components 37
4-2 Jumper Setting 39
Chapter 1 BIOS Setup 41
5-1 The Main Menu 43
5-2 Advanced Menu 45
5-2-1 iSCSI Configuration 46
5-2-2 QLogic 577xx/578xx 10 Gb Ethernet BCM57810 47

5-2-3 VLAN Configuration 60
5-2-4 CPU Configuration 62
5-2-5 SATA Configuration 64
5-2-6 USB Configuration 65
5-2-7 AST2500 Super IO Configuration 67
5-2-8 Serial Port Console Redirection 70
5-2-9 PCI Subsystem Settings 75
5-2-10 Network Stack 77
5-2-11 CSM Configuration 78
5-2-12 Trusted Computing 80
5-2-13 NVMe Configuration 81
5-3 AMD CBS Menu 82
5-3-1 Zen Common Options 83
5-3-2 DF Common Options 86
5-3-3 UMC Common Options 87
5-3-4 NBIO Common Options 94
5-3-5 FCH Common Options 95
5-4 Chipset Setup Menu 97
5-4-1 North Bridge 98
5-4-2 Error Management 101
5-5 Server Management Menu 102
5-5-1 System Event Log 104
5-5-2 View FRU Information 105
5-5-3 BMC Network Configuration 106
5-5-4 IPv6 BMC Network Configuration 108
5-6 Security Menu 110
5-6-1 Secure Boot 111
5-7 Boot Menu 115
5-7-1 UEFI NETWORK Drive BBS Priorities 117
5-7-2 UEFI Application Boot Priorities 118
5-8 Save & Exit Menu 119
5-9 ABL POST Codes 120
5-9-1 StartProcessorTestPoints 120
5-9-2 Memory test points 120
5-9-3 PMU Test Points 120
5-9-4 Original Post Code 121
5-9-5 CPU test points 122
5-9-6 Topology test points 122
5-9-7 Extended memory test point 122
5-9-8 Gnb Earlier init 123
5-9-9 PMU test points 126

5-9-10 ABL0 test points 126
5-9-11 ABL5 test points 126
5-10 Agesa POST Codes 130
5-10-1 Universal Post Code 130
5-10-2 [0xA1XX] For CZ only memory Postcodes 130
5-10-3 S3 Interface Post Code 133
5-10-4 PMU Post Code 133
5-10-5 [0xA5XX] assigned for AGESA PSP Module 133
5-10-6 [0xA9XX, 0xAAXX] assigned for AGESA NBIO Module 136
5-10-7 [0xACXX] assigned for AGESA CCX Module 138
5-10-8 [0xADXX] assigned for AGESA DF Module 139
5-10-9 [0xAFXX] assigned for AGESA FCH Module 139
5-11 BIOS POST Beep code (AMI standard) 141
5-11-1 PEI Beep Codes 141
5-11-2 DXE Beep Codes 141
5-12 BIOS Recovery Instruction 142

Chapter 1 Hardware Installation

1-1 Installation Precautions

The motherboard/system contain numerous delicate electronic circuits and components which can become damaged as a result of electrostatic discharge (ESD). Prior to installation, carefully read the service guide and follow these procedures:

- Prior to installation, do not remove or break motherboard S/N (Serial Number) sticker or warranty sticker provided by your dealer. These stickers are required for warranty validation.
- Always remove the AC power by unplugging the power cord from the power outlet before installing or removing the motherboard or other hardware components.
- When connecting hardware components to the internal connectors on the motherboard, make sure they are connected tightly and securely.
- When handling the motherboard, avoid touching any metal leads or connectors.
- It is best to wear an electrostatic discharge (ESD) wrist strap when handling electronic components such as a motherboard, CPU or memory. If you do not have an ESD wrist strap, keep your hands dry and first touch a metal object to eliminate static electricity.
- Prior to installing the motherboard, please have it on top of an antistatic pad or within an electrostatic shielding container.
- Before unplugging the power supply cable from the motherboard, make sure the power supply has been turned off.
- Before turning on the power, make sure the power supply voltage has been set according to the local voltage standard.
- Before using the product, please verify that all cables and power connectors of your hardware components are connected.
- To prevent damage to the motherboard, do not allow screws to come in contact with the motherboard circuit or its components.
- Make sure there are no leftover screws or metal components placed on the motherboard or within the computer casing.
- Do not place the computer system on an uneven surface.
- Do not place the computer system in a high-temperature environment.
- Turning on the computer power during the installation process can lead to damage to system components as well as physical harm to the user.
- If you are uncertain about any installation steps or have a problem related to the use of the product, please consult a certified computer technician.

1-2 Product Specifications

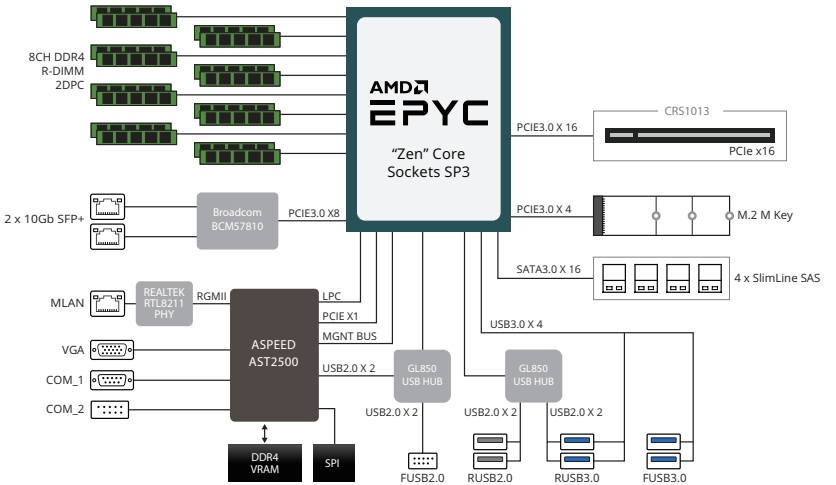
CPU	◆ AMD EPYC™ 7000 series processor family ◆ Single processor, 14nm, Socket SP3 ◆ Up to 32-core, 64 threads ◆ TDP up to 180W
Chipset	◆ System on Chip
Memory	◆ 16 x DIMM slots ◆ DDR4 memory supported only ◆ 8-channel memory architecture ◆ RDIMM modules up to 32GB supported ◆ LRDIMM modules up to 64GB supported ◆ Memory speed: 2667(1DPC)/2400/2133* MHz ◆ ◆ Note: Memory speed runs at 2133MHz when 1R/2R memory modules are fully populated
LAN	◆ 2 x SFP+ 10Gb/s LAN ports (Broadcom® BCM 57810S) ◆ 1 x 10/100/1000 management LAN
Expansion Slot	◆ 1 x Riser card: ◆ - 1 x CRS1013 ◆ * 1 x Full-height half-length slot with PCIe x16 (Gen3 x16 bus) slot ◆ ◆ 1 x M.2 slot: ◆ - M-key ◆ - PCIe Gen3 x4 ◆ - Supports NGFF-2280/2260/2242 cards
Video	◆ Integrated in Aspeed® AST2500 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp
Storage	◆ 4 x 3.5" SATA/SAS hot-swappable HDD/SSD bays ◆ 2.5" HDD/SSD supported ◆ SAS card is required for SAS devices support
SAS	◆ Supported via add-on SAS Card

Internal Connectors	◆ 1 x 24-pin ATX main power connector ◆ 2 x 8-pin ATX 12V power connectors ◆ 4 x SlimSAS connectors ◆ 1 x M.2 slot ◆ 2 x CPU fan headers ◆ 5 x System fan headers ◆ 1 x USB 3.0 header ◆ 1 x USB 2.0 header ◆ 1 x COM_2 header ◆ 1 x TPM header ◆ 1 x Front panel header ◆ 2 x LAN activity LED ◆ 1 x HDD back plane board header ◆ 1 x PMBus connector ◆ 1 x IPMB connector ◆ 1 x Clear CMOS jumper ◆ 1 x BIOS recovery jumper ◆ 1 x Buzzer
Front Panel LED/Buttons	◆ 2 x USB 3.0 ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x Reset button ◆ 1 x NMI button ◆ 1 x System status LED ◆ 1 x HDD activity LED ◆ 2 x LAN activity LEDs
Rear Panel I/O	◆ 2 x USB 3.0 ◆ 2 x USB 2.0 ◆ 1 x VGA ◆ 1 x COM_1 ◆ 2 x SFP+ ◆ 1 x MLAN ◆ 1 x ID button with LED
Backplane I/O	◆ 4 x SATA/SAS ports ◆ Bandwidth: SATAIII 6Gb/s or SAS 12Gb/s per port ◆ SAS card is required for SAS devices support
TPM	◆ 1 x TPM header with LPC interface ◆ Optional TPM2.0 kit: CTM000

System Management	◆ Aspeed® AST2500 management controller ◆ Avocent® MergePoint IPMI 2.0 web interface: ◆ Network settings ◆ Network security settings ◆ Hardware information ◆ Users control ◆ Services settings ◆ IPMI settings ◆ Sessions control ◆ LDAP settings ◆ Power control ◆ Fan profiles ◆ Voltages, fans and temperatures monitoring ◆ System event log ◆ Events management (platform events, trap settings, email settings) ◆ Serial Over LAN ◆ vKVM & vMedia (HTML5)
Power Supply	◆ 2 x 650W redundant PSUs ◆ 80 PLUS Platinum ◆ ◆ AC input: ◆ - 100-240Vac, 50-60Hz, 10-5A ◆ ◆ DC input: ◆ - 190-310Vdc, 5-3A ◆ ◆ DC output: ◆ - 650W
Environment Ambient Temperature Relative Humidity	◆ Operating temperature: 10°C to 35°C ◆ Operating humidity: 8%-80% (non-condensing) ◆ ◆ Non-operating temperature: -40°C to 60°C ◆ Non-operating humidity: 20%-95% (non-condensing)
System Dimension	◆ 1U ◆ 430mm (W) x 43.5mm (H) x 625mm (D)

* We reserve the right to make any changes to the product specifications and product-related information without prior notice.

1-3 System Block Diagram



Chapter 2 System Appearance

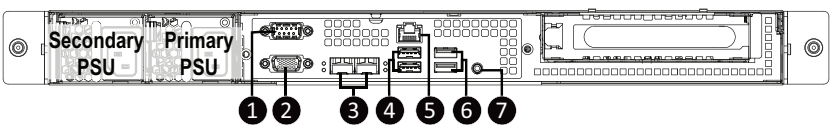
2-1 Front View



No.	Description
1.	USB 3.0 Ports
2.	Front Panel LEDs and buttons

- Refer to Chapter **2-3 Front Panel LED** and Buttons for a detailed description of the function of the LEDs.

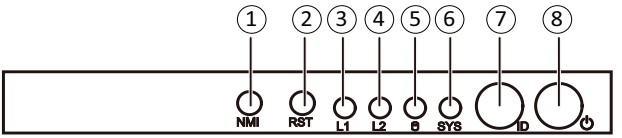
2-2 Rear View



No.	Description
1.	Serial port
2.	VGA port
3.	SFP+ LAN ports
4.	USB 3.0 ports
5.	10/100/1000 Server management LAN port
6.	USB 2.0 ports
7.	ID button with LED

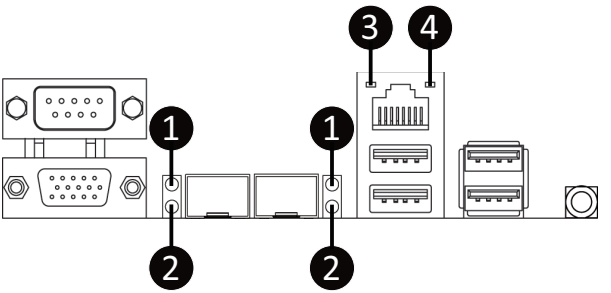
- Refer to Chapter **2-4 Rear System LAN LEDs** for a detailed description of the function of the LEDs.

2-3 Front Panel LED and Buttons



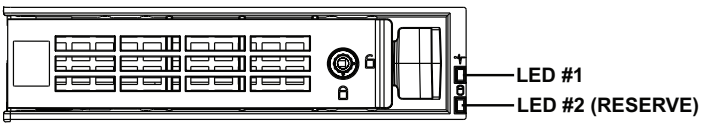
No.	Name	Color	Status	Description
1.	NMI button	--	--	Press this button for the server to generate a NMI to the processor. If multiple-bit ECC errors occur, the server will effectively be halted.
2.	Reset Button	--	--	Press this button to reset the system.
3/4.	LAN 1/2 Active/Link LEDs	Green	Solid On	Indicates a link between the system and the network or no access.
		Green	Blink	Indicates data trasmission or receiving is occuring
		N/A	Off	Indicates no data transmission or receiving is occuring
5.	HDD Status LED	Green	On	Indicates locating the HDD.
			Blink	Indicates accessing the HDD.
		Amber	On	Indicates HDD error.
		Green/ Amber	Blink	Indicates HDD rebuilding.
		N/A	Off	Indicates no HDD access or no HDD error.
6.	System Status LED	Green	Solid On	Indicates system is operating normally.
		Amber	Solid On	Indicates a critical condition, may include: -System fan failure -System temperature
			Blink	Indicates non-critical condition, may include: -Redundant power module failure -Temperature and voltage issue -Chassis intrusion
		N/A	Off	Indicates system is not ready, may include: -POST error -NMI error -Processor or terminator is missing
7.	ID Button	--	--	Press this button to activate system identification
8.	Power button with LED	Green	On	Indicates the system is powered on
		Green	Blink	System is in ACPI S1 state (sleep mode)
		N/A	Off	• System is not powered on or in ACPI S5 state (power off) • System is in ACPI S4 state (hibernate mode)

2-4 Rear System LAN LEDs



No.	Name	Color	Status	Description
1.	SFP+ LAN Link & Speed LED	Yellow	On	1 Gbps data rate
		Green	On	10 Gbps data rate
2.	SFP+ LAN Activity LED	Green	On	Link between system and network or no access
		Green	Blink	Data transmission or receiving is occurring
		N/A	Off	No data transmission or receiving is occurring
3.	10/100/ 1000 LAN LED	Yellow	On	1 Gbps data rate
		Green	On	100Mbps data rate
		N/A	Off	10Mbps data rate
4.	ID button/ LED	Blue	On	System identification is active
		N/A	Off	System identification is disabled

2-5 Hard Disk Drive LEDs



RAID SKU		LED1	Locate	HDD Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via HBA, PCH)	Disk LED (LED on Back Panel)	Green	ON(*1)	OFF		BLINK (*2)	OFF
		Amber	OFF	OFF		OFF	OFF
	Removed HDD Slot (LED on Back Panel)	Green	ON(*1)	OFF		--	--
		Amber	OFF	OFF		--	--
RAID configuration (via HW RAID Card or SW RAID Card)	Disk LED	Green	ON	OFF		BLINK (*2)	OFF
		Amber	OFF	ON	(Low Speed: 2 Hz)	OFF	OFF
	Removed HDD Slot	Green	ON(*1)	OFF	(*3)	--	--
		Amber	OFF	ON	(*3)	--	--

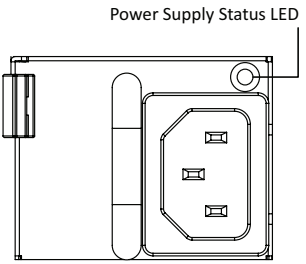
NOTE:

*1: Depends on HBA/Utility Spec.

*2: Blink cycle depends on HDD's activity signal.

*3: If HDD is pulled out during rebuilding, the disk status of this HDD is regarded as faulty.

2-6 Power Supply Unit LED



State	Description
Off	No AC power to all power supplies
0.5Hz Blink/Red	N+1, No AC power to all power supplies
Green/Blink	Only standby output ON
Green	Power supply DC output ON and OK
Red	Power supply failure
0.5Hz Blink Gren/Red	Power supply warning

Chapter 3 System Hardware Installation



Pre-installation Instructions

Computer components and electronic circuit boards can be damaged by discharges of static electricity. Working on computers that are still connected to a power supply can be extremely dangerous. Follow the simple guidelines below to avoid damage to your computer or injury to yourself.

- Always disconnect the computer from the power outlet whenever you are working inside the computer case.
- If possible, wear a grounded wrist strap when you are working inside the computer case. Alternatively, discharge any static electricity by touching the bare metal system of the computer case, or the bare metal body of any other grounded appliance.
- Hold electronic circuit boards by the edges only. Do not touch the components on the board unless it is necessary to do so. Do not flex or stress the circuit board.
- Leave all components inside the static-proof packaging until you are ready to use the component for the installation.

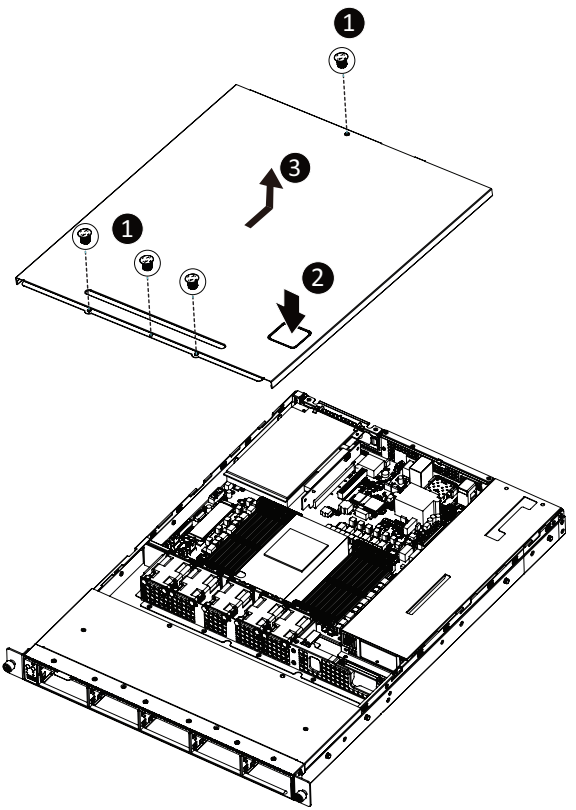
3-1 Removing and Installing the Chassis Cover

Before you remove or install the system cover

- Make sure the system is not turned on or connected to AC power.

Follow these instructions to remove the chassis cover:

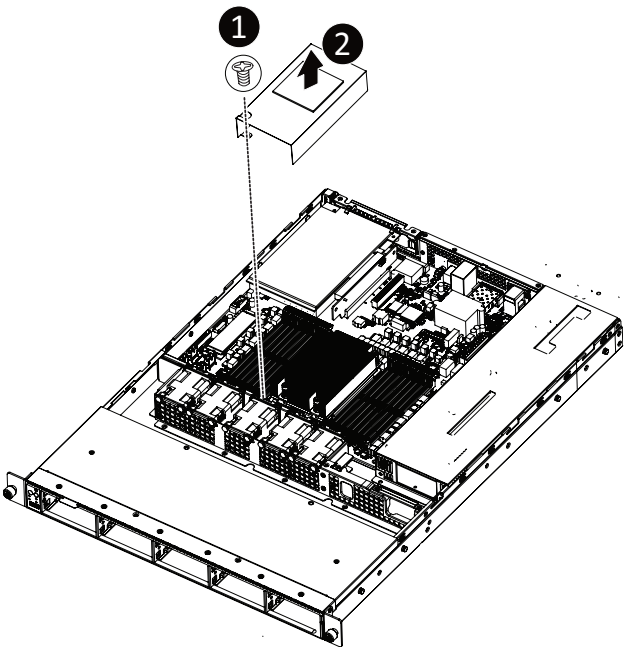
1. Loosen and remove the four screws securing the chassis cover.
2. Push down the indentation located at the side of the back chassis
3. Slide the cover horizontally to the back and remove the cover in the direction of the arrow
4. To reinstall the chassis cover follow steps 1-3 in reverse order.



3-2 Removing and Installing the Fan Duct

Follow these instructions to remove the fan duct:

1. Loosen and remove the screw securing the fan duct.
2. Lift up to remove the fan duct.
3. To reinstall the fan duct, align the fan duct so that the screw hole on the fan duct is above the screw hole on the mainboard. Install the screw to secure the fan duct.



3-3 Removing and Installing the CPU and Heat Sink

Read the following guidelines before you begin to install the CPU:

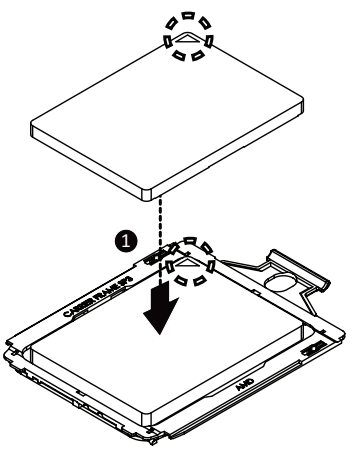
- Make sure that the motherboard supports the CPU.
- Always turn off the computer and unplug the power cord from the power outlet before installing the CPU to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system unit on a flat and stable surface.
- Open the system according to the instructions.

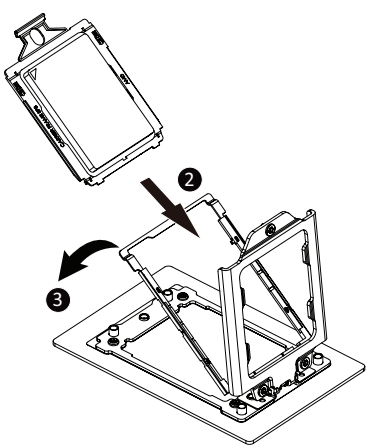
WARNING!

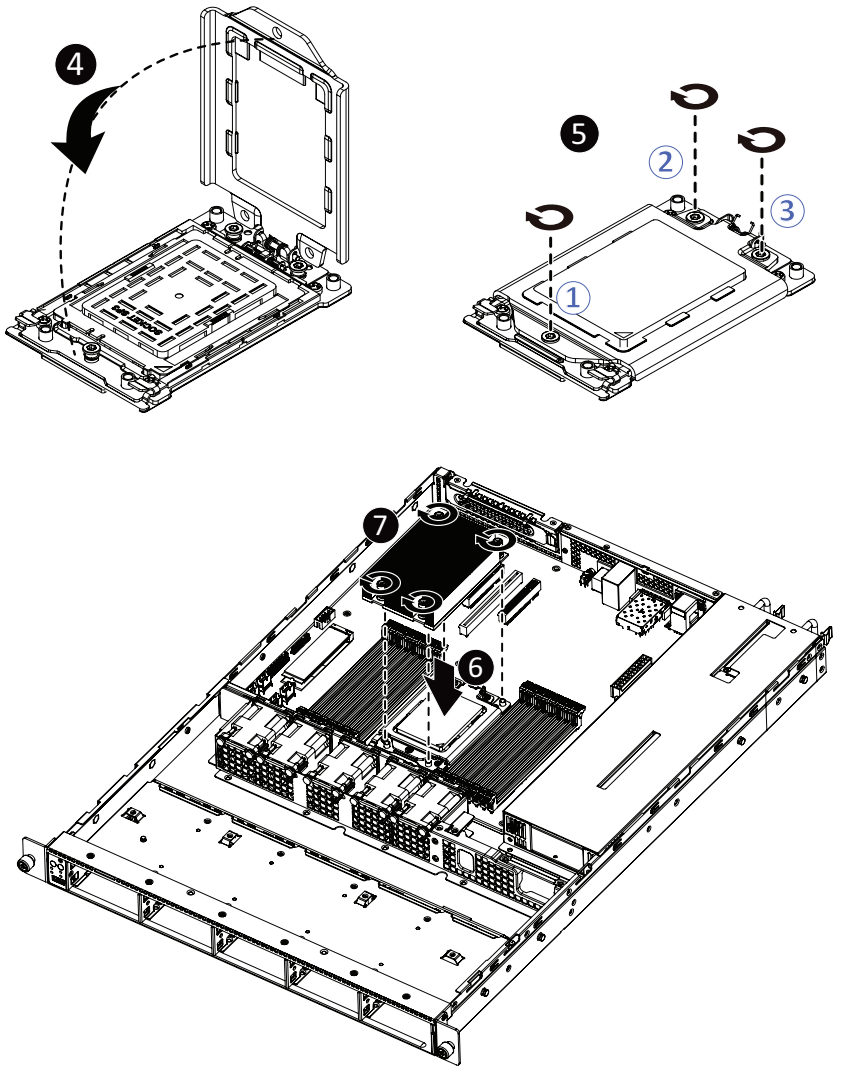
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

Follow these instructions to install the CPU:

1. Align and install the processor on the carrier, making sure to line up the triangle markers on the corner of the CPU to the triangle mark on the corner of the CPU cover.
2. Slide the carrier assembly into the channels of the carrier bracket
3. Close the carrier bracket so that it firmly latches on to the CPU socket.
4. Close the CPU socket cover.
5. Tighten and secure the CPU socket cover screws in the following order (3→2→1).
   NOTE: When removing the CPU socket cover, loosen the screws in reverse order (1→2→3).
   NOTE: Apply thermal compound evenly on the top of the CPU. Remove the protective cover from the underside of the heat sink.
6. Align and place the heatsink onto the top of the CPU socket.
7. To secure the heatsink, tighten the four screws to the CPU socket
8. To remove the heatsink and CPU follow steps 1-7 in reverse order.






4
5
2
3
1
7
6

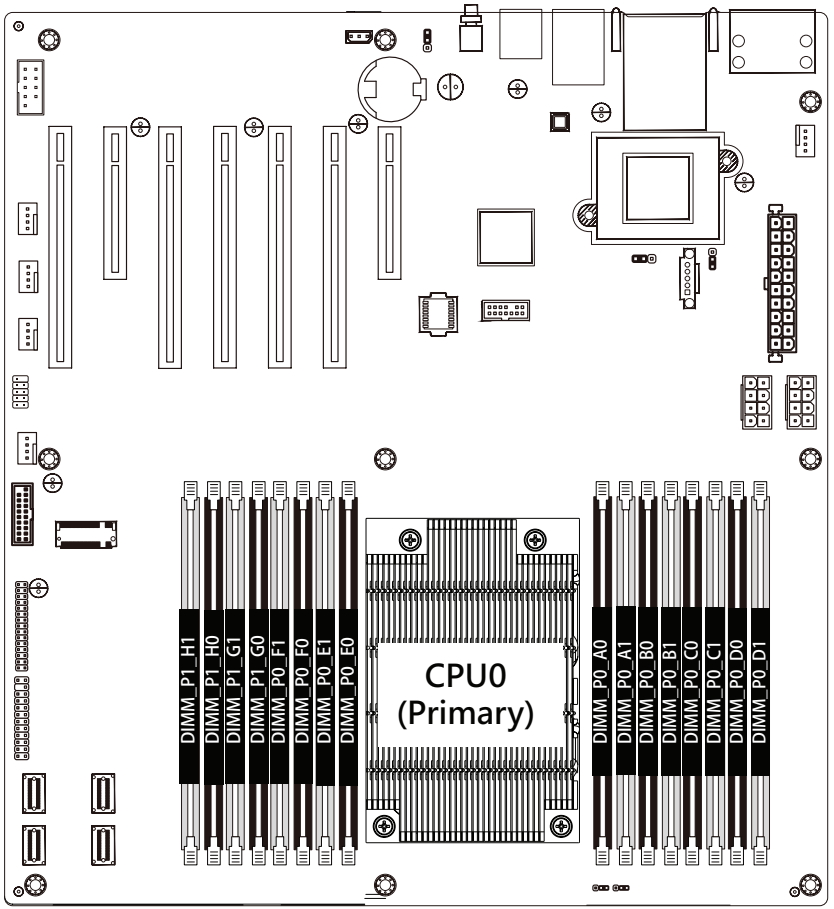
3-4 Removing and Installing Memory

Read the following guidelines before you begin to install memory:

- Make sure that the motherboard supports the memory module. It is recommended to use memory of the same capacity, brand, speed, and chipset.
- Always turn off the computer and unplug the power cord from the power outlet before installing the memory to prevent hardware damage.
- Memory modules have a foolproof design. A memory module can be installed in only one direction. If you are unable to insert the memory, switch the direction.

3-4-1 8-Channel Memory Configuration

This motherboard provides 16 DDR4 memory sockets and supports 8-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory. Enabling Four Channel memory mode will be four times of the original memory bandwidth.



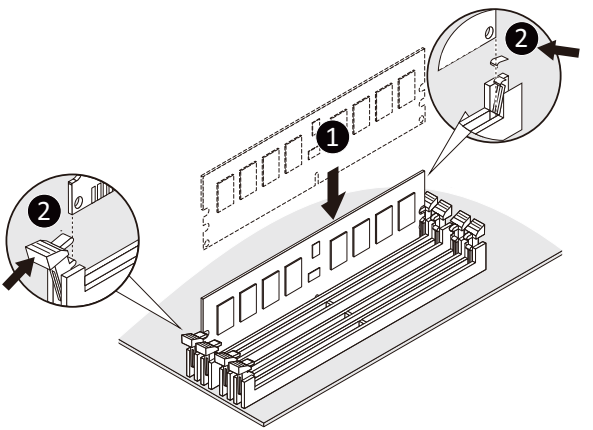
3-4-2 Removing and Installing a Memory Module

Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR4 DIMMs on to this motherboard.

Follow these instructions to install a DIMM module:

1. Insert the DIMM memory module vertically into the DIMM slot and push it down.
2. Close the plastic clip at both edges of the DIMM slots to lock the DIMM module.
3. Reverse the installation steps when you want to remove the DIMM module.



3-4-3 DIMM Population Table

RDIMM Maximum Frequency Supported Tablel

Slots	DIMMs Populated	DIMM			Frequency (MT/s)
		1R	2R 2DR	4DR	1.2V
1	1	1	--		2667
		--	1		2667
		--	--	1	Not Supported
2	1	1	--		2667
		--	1		2400
		--	--	1	Not Supported
	2	2	--		2133
		1	1		2133
		--	2		2133
		--	--	2	Not Supported
		1	--	1	Not Supported
		--	1	1	Not Supported

3DS RDIMM Maximum Frequency Supported Table

Slots	DIMMs Populated	DIMM			Frequency (MT/s)
		NA	2S2R 2S4R	4DR	1.2V
1	1	1	--		Not Supported
		--	1		2667
		--	--	1	Not Supported
2	1	1	--		Not Supported
		--	1		2400
		--	--	1	Not Supported
	2	2	--		Not Supported
		1	1		Not Supported
		--	2		1866
		--	--	2	Not Supported
		1	--	1	Not Supported

LRDIMM Maximum Frequency Supported Table

Slots	DIMMs Populated	DIMM			Frequency (MT/s)
		1R	2S4R	4DR	1.2V
1	1	1	--	--	Not Supported
		--	1	--	2667
		--	--	1	2667
2	1	1	--	--	Not Supported
		--	1	--	2667
		--	--	1	2667
	2	2	--	--	Not Supported
		1	1	--	Not Supported
		--	2	--	2133
		--	--	2	2133
		1	--	1	Not Supported
		--	1	1	2133

NOTE!

l 1R: 1 package rank of SDP DRAMs

l 2R: 2 package rank of SDP DRAMs

l 2DR: 2 package rank of DDP DRAMs

l 4DR: 2 package rank of DDP DRAMs

l 1S2R/1S4R/1S8R: 1 package rank of 2/4/8 high 3DS DRAMs

l 2S2R/2S4R/2S8R: 2 package rank of 2/4/8 high 3DS DRAMs

l DIMM must be populated in sequential alphabetic order, starting with bank A.

l When only one DIMM is used, it must be populated in memory slot A1.

3-5 Removing and Installing the PCI Expansion Card

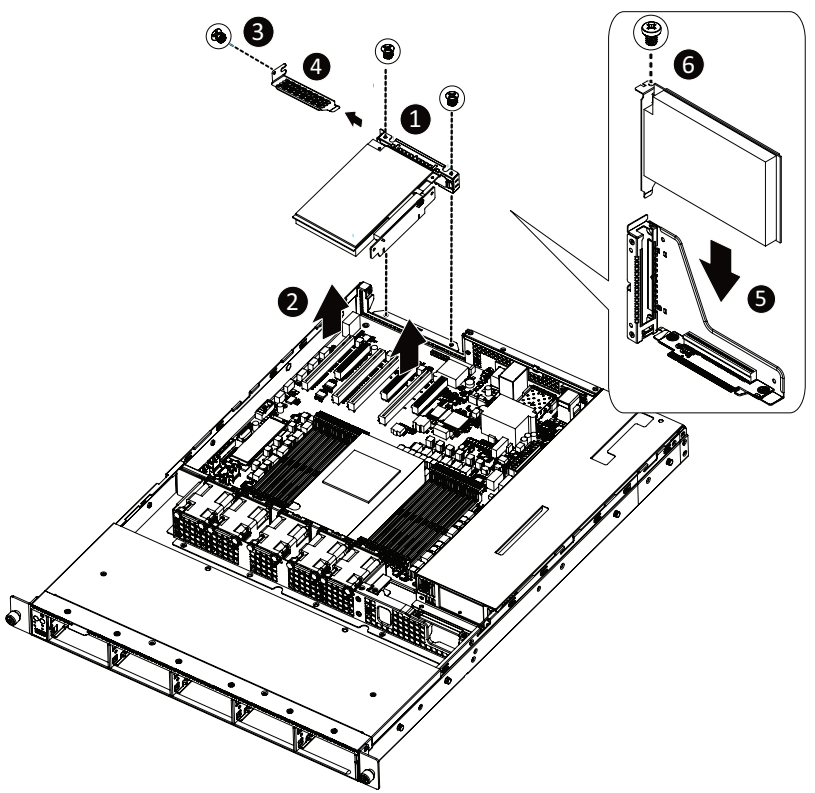
- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered off and all power sources have been disconnected from the server prior to installing a PCI card.

Failure to observe these warnings could result in personal injury or damage to equipment.

- The PCI riser assembly does not include a riser card or any cabling as standard. To install a PCI card, a riser card must be installed.

Follow these instructions to PCI Expansion card:

1. Remove the two screws securing the riser bracket.
2. Lift up the riser bracket out of system.
3. Remove the screw securing the slot cover from the riser bracket.
4. Remove the slot cover from the riser bracket.
5. Orient the PCIe card with the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCI card connector.
6. Secure the PCIe card to the riser bracket with one screw.
7. Reverse the steps 1 - 2 to install the riser bracket.



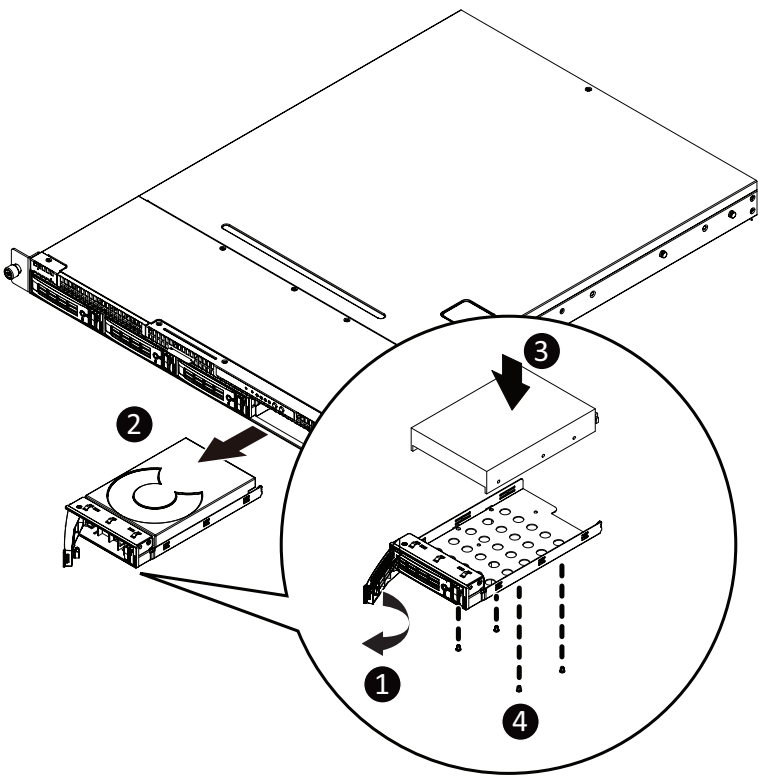
3-6 Removing and Installing the Hard Disk Drive

Read the following guidelines before you begin to install the Hard disk drive:

- Take note of the drive tray orientation before sliding it out.
- The tray will not fit back into the bay if inserted incorrectly.
- Make sure that the HDD is connected to the HDD connector on the backplane.

Follow these instructions to install a 3.5" hard disk drive:

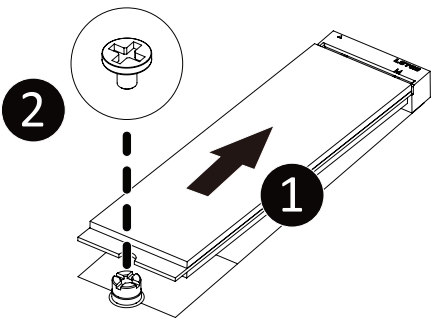
1. Press the release button to extend the locking lever.
2. Pull the locking lever to remove the HDD tray.
3. Slide the hard disk into the HDD tray.
4. Install 4 screws to secure the hard drive to the HDD tray.
5. Reinsert the HDD tray into the slot and close the locking lever.

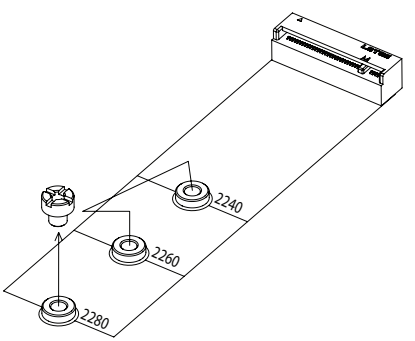


3-7 Installing and Removing an M.2 Solid State Drive

Follow these instructions to install an optional M.2 solid state drive (SSD):

1. Place the solid state drive into the M.2 connector.
2. Secure the solid state drive to the motherboard with a single screw.
   NOTE: The position of the screw will depend on the size of the SSD. Refer to the second image below for proper placement.
3. Reverse steps 1-2 to remove the solid state drive.



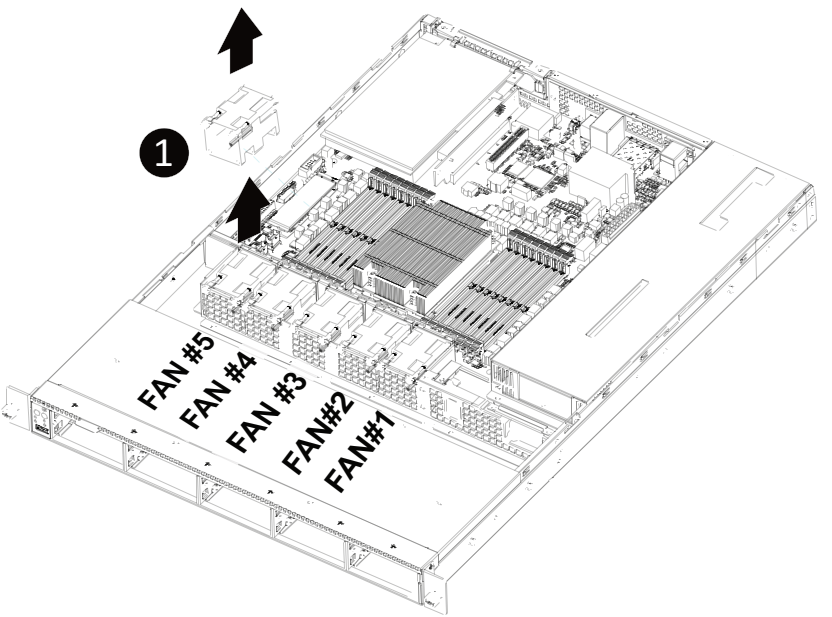


3-8 Replacing the Fan Assembly

Follow these instructions to replace the fan assembly:

NOTE: Before removing the fan, disconnect and unthread the two fan connectors from the server. Refer to the Fan Connector Table below for proper connection for the fan cables.

1. Lift up the fan assembly from the chassis
2. Reverse the previous steps to install the replacement fan assembly.



3-8-1 Fan Connector Table

Fan No.	Fan Cable	Port Connection
1	RED and BLACK	FAN13
	ORANGE and WHITE	FAN14
2	RED and BLACK	FAN11
	ORANGE and WHITE	FAN12
3	RED and BLACK	FAN9
	ORANGE and WHITE	FAN10
4	RED and BLACK	FAN8
	ORANGE and WHITE	FAN6
5	RED and BLACK	FAN15
	ORANGE and WHITE	FAN16

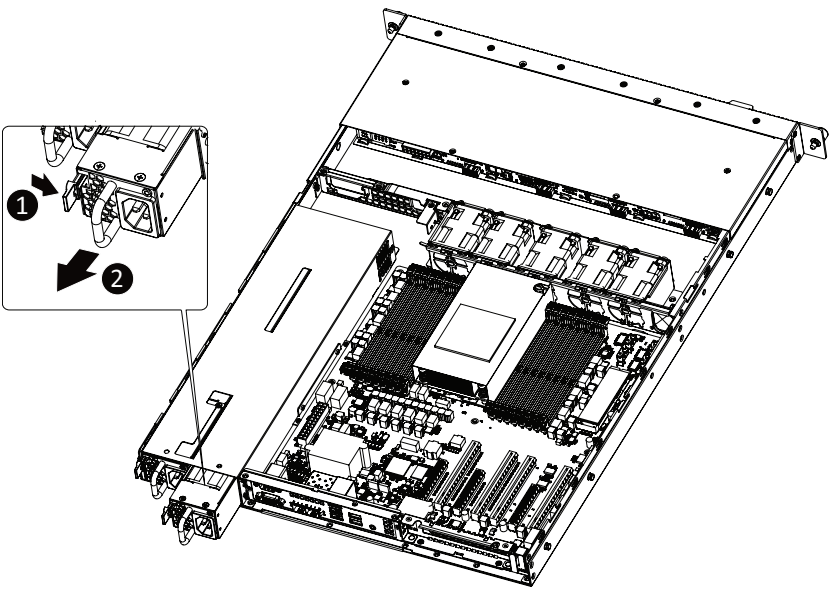
3-9 Removing and Installing the Power Supply

Before you remove or install the system cover

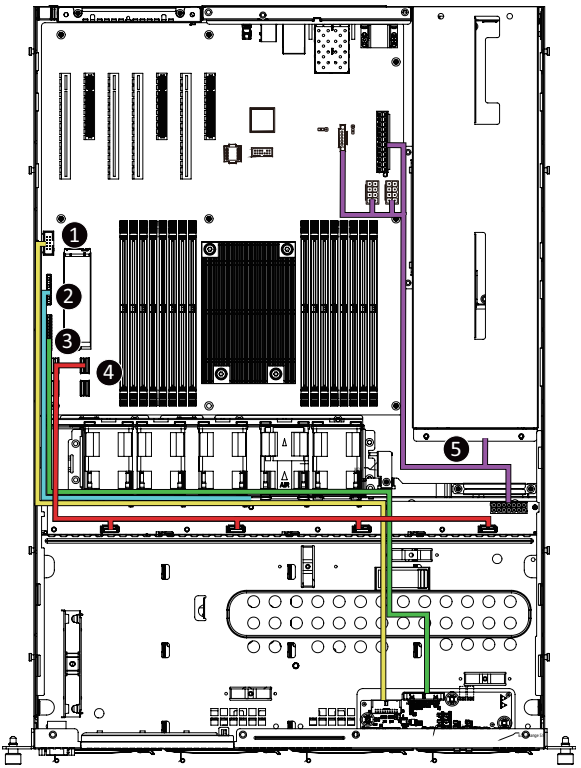
- Make sure the system is not turned on or connected to AC power.

Follow these instructions to replace the power supply:

1. Press the retaining clip on the left side of the power supply unit along the direction of the arrow.
2. Pull the power supply handle at the same time and pull out the power supply unit.
3. Insert the replacement power supply unit firmly into the chassis. Connect the AC power cord to the replacement power supply.
4. Repeat steps 1-3 for replacement of the second power supply.



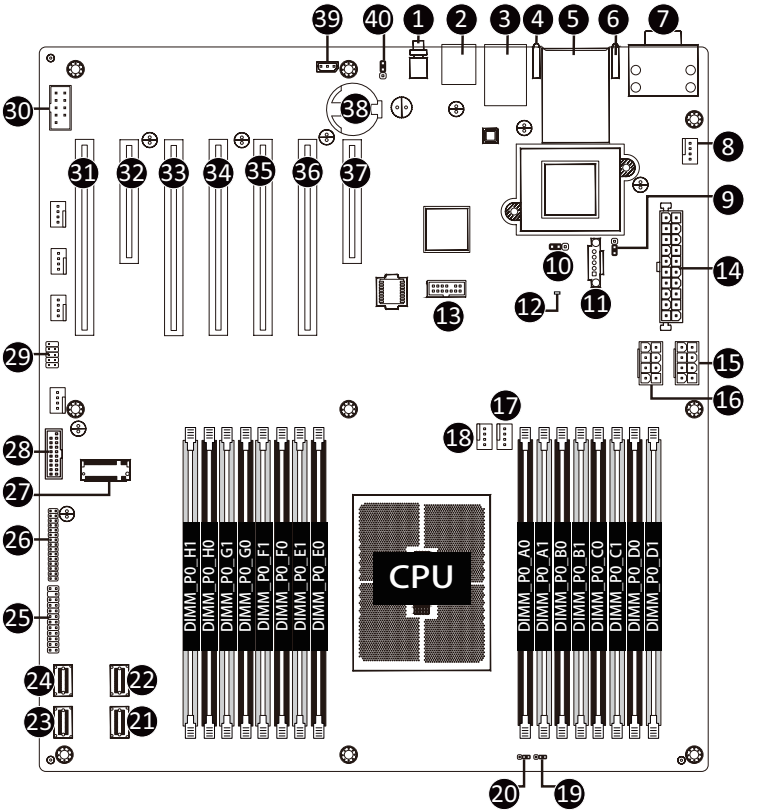
3-10 Cable Routing



No.	Cable	No.	Cable
1.	USB cable (Yellow)	2.	On board SATA to back plane board cable (Blue)
3.	Front switch cable/Front LED cable (Green)	4.	HDD back plane board signal cable (Red)
5.	HDD back plane board power cable (Purple)		

Chapter 4 Motherboard Components

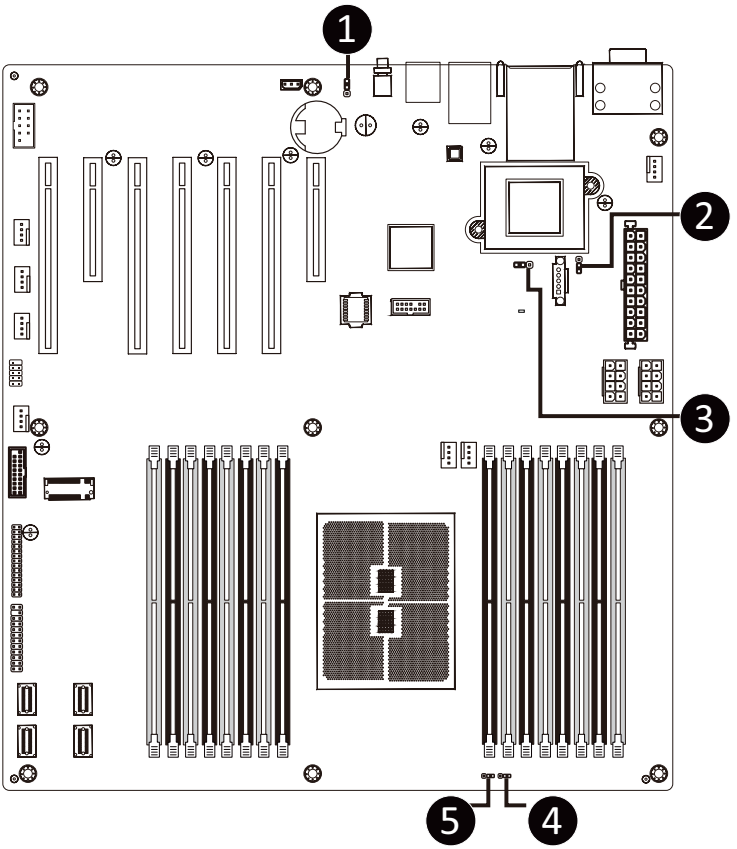
4-1 Motherboard Components



Item	Description
1	ID button with LED
2	USB 2.0 ports
3	Server management LAN port (top)/ USB 3.0 port (bottom)
4	SFP+ LAN port #1 active/link LEDs
5	SFP+ LAN port #1 / SFP+ LAN port #2
6	SFP+ LAN port #2 active/link LEDs
7	Serial port (top) / VGA port (bottom)
8	System fan connector #3
9	PMBus select jumper
10	S3 power on select jumper

11	PMBus connector
12	BMC firmware readiness LED
13	TPM connector
14	2 x 12 pin main power connector
15	2 x 4 pin power connector (for memory)
16	2 x 4 pin power connector (for CPU)
17	CPU fan connector #1
18	CPU fan connector #0
19	Clearing Supervisor Password jumper
20	BIOS recovery jumper
21	Slimline connector #0 (SATA 6Gb/s signal)
22	Slimline connector #1 (SATA 6Gb/s signal)
23	Slimline connector #2 (SATA 6Gb/s signal)
24	Slimline connector #3 (SATA 6Gb/s signal)
25	Front panel header
26	HDD back plane board header
27	M.2 slot (Gen 3/x4)
28	USB 3.0 header
29	System Fan connector #1
30	USB 2.0 header
31	System Fan connector #4
32	System Fan connector #5
33	System Fan connector #2
34	Serial port cable connector
35	PCIe x16 slot (Gen 3/x16)
36	PCIe x8 slot (Gen 3/x8)
37	PCIe x16 slot (Gen 3/x16)
38	PCIe x16 slot (Gen 3/x16)
39	PCIe x8 slot (Gen 3/x8)
40	PCIe x16 slot (Gen 3/x16)
41	PCIe x8 slot (Gen 3/x8)
42	Battery socket
43	IPMB connector
44	Clear CMOS jumper

4-2 Jumper Setting



Item	Description	Setting
1	Clear CMOS Jumper	1-2 Closed: Normal operation (default setting)
		2-3 Closed: Clear CMOS data
2	PMBus Address Selection Jumper	1-2 Closed: From core chipset
		2-3 Closed: From BMC (default setting)
3	S3 Power On Select Jumper	1-2 Closed: Stop an initial power on when BMC is not ready
		2-3 Closed: Keep initial power on (default setting)
4	Clearing Supervisor Password Jumper	1-2 Closed: Normal operation (default setting)
		2-3 Closed: Skip supervisor password
5	BIOS Recovery Jumper	1-2 Closed: Normal operation (default setting)
		2-3 Closed: BIOS recovery mode

Chapter 1 BIOS Setup

BIOS (Basic Input and Output System) records hardware parameters of the system in the EFI on the motherboard. Its major functions include conducting the Power-On Self-Test (POST) during system startup, saving system parameters and loading operating system, etc. BIOS includes a BIOS Setup program that allows the user to modify basic system configuration settings or to activate certain system features. When the power is turned off, the battery on the motherboard supplies the necessary power to the CMOS to keep the configuration values in the CMOS.

To access the BIOS Setup program, press the <DEL> key during the POST when the power is turned on.



- BIOS flashing is potentially risky, if you do not encounter problems of using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 1 for how to clear the CMOS values.)

BIOS Setup Program Function Keys

<←><→>	Move the selection bar to select the screen
<↑><↓>	Move the selection bar to select an item
<+>	Increase the numeric value or make changes
<->	Decrease the numeric value or make changes
<Enter>	Execute command or enter the submenu
<Esc>	Main Menu: Exit the BIOS Setup program Submenus: Exit current submenu
<F1>	Show descriptions of general help
<F3>	Restore the previous BIOS settings for the current submenus
<F9>	Load the Optimized BIOS default settings for the current submenus
<F10>	Save all the changes and exit the BIOS Setup program

- **Main**
  This setup page includes all the items in standard compatible BIOS.
- **Advanced**
  This setup page includes all the items of AMI BIOS special enhanced features.
  (ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)
- **AMD CBS**
  This setup page includes the common items for configuration of AMD motherboard-related information.
- **Chipset**
  This setup page includes all the submenu options for configuring the function of processor, network, North Bridge, South Bridge, and System event logs.
- **Server Management**
  Server additional features enabled/disabled setup menus.
- **Security**
  Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.
  A supervisor password allows you to make changes in BIOS Setup.
  A user password only allows you to view the BIOS settings but not to make changes.
- **Boot**
  This setup page provides items for configuration of boot sequence.
- **Save & Exit**
  Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)
  Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)

5-1 The Main Menu

Once you enter the BIOS Setup program, the Main Menu (as shown below) appears on the screen. Use arrow keys to move among the items and press <Enter> to accept or enter other sub-menu.

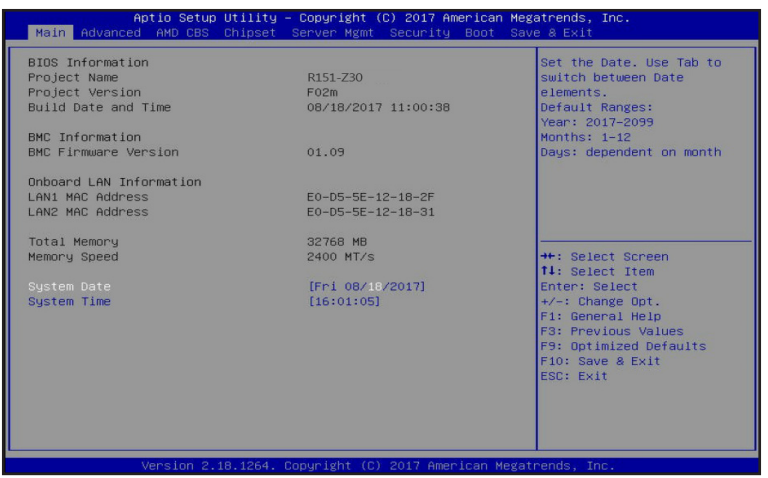
Main Menu Help

The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

Submenu Help

While in a submenu, press <F1> to display a help screen (General Help) of function keys available for the menu. Press <Esc> to exit the help screen. Help for each item is in the Item Help block on the right side of the submenu.

- When the system is not stable as usual, select the **Restore Defaults** item to set your system to its defaults.
- The BIOS Setup menus described in this chapter are for reference only and may differ by BIOS version.



☞ **Project Name**

Displays the project name information.

☞ **Project Version**

Displays version number of the BIOS setup utility.

☞ **Build Date and Time**

Displays the date and time when the BIOS setup utility was created.

☞ **BMC Information**(Note)

☞ **BMC Firmware Version**(Note)

Displays BMC firmware version information.

☞ **Onboard LAN Information**

☞ **LAN1 MAC Address**(Note)

Displays LAN1 MAC address information.

☞ **LAN2 MAC Address**(Note)

Displays LAN2 MAC address information.

☞ **Total Memory**(Note)

Displays the information for the installed memory size.

☞ **Memory Speed**(Note)

Displays the information for the installed memory speed.

☞ **System Date**

Sets the date following the weekday-month-day-year format.

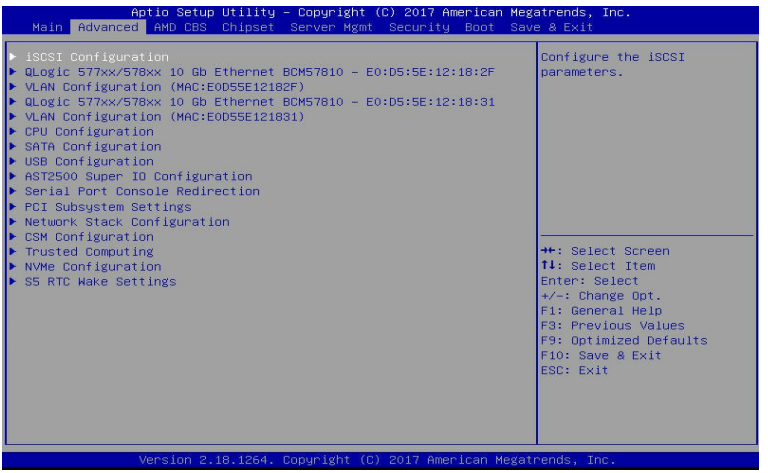
☞ **System Time**

Sets the system time following the hour-minute-second format.

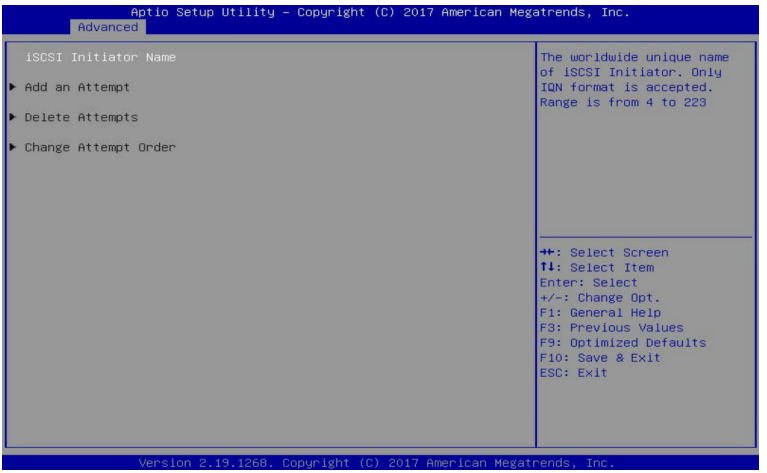
(Note) Functions available on selected models.

5-2 Advanced Menu

The Advanced menu display submenu options for configuring the function of various hardware components. Select a submenu item, then press [Enter] to access the related submenu screen.



5-2-1 iSCSI Configuration



☞ **iSCSI Initiator Name**

☞ **Add an Attempt**

Press [Enter] for configuration of advanced items.

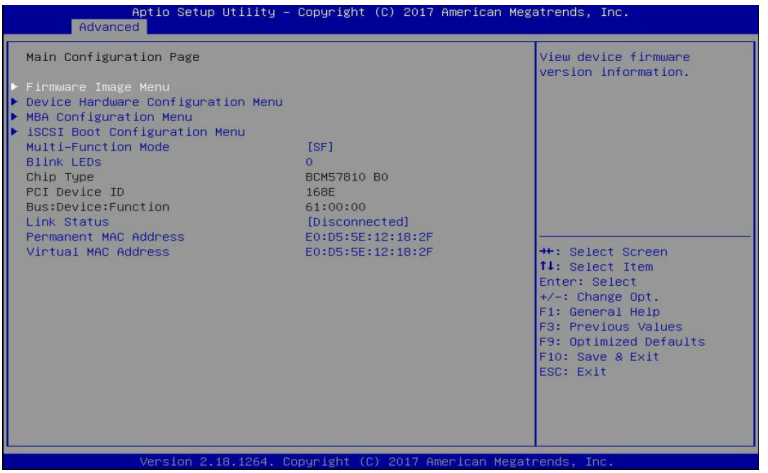
☞ **Delete Attempts**

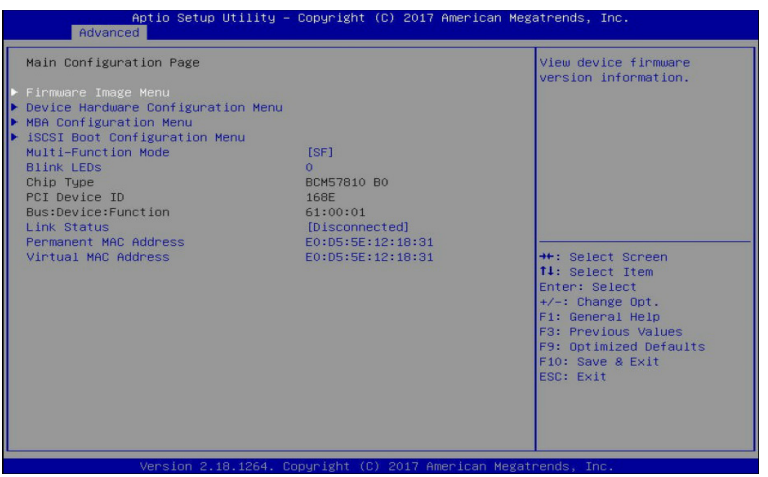
Press [Enter] for configuration of advanced items.

☞ **Change Attempt Order**

Press [Enter] for configuration of advanced items.

5-2-2 QLogic 577xx/578xx 10 Gb Ethernet BCM57810





☞ **Main Configuration Page**

☞ **Firmware Image Menu**

Press [Enter] to view device firmware version information.

☞ **Device Hardware Configuration Menu**

Press [Enter] to configure device and port specific parameters.

☞ **MBA Configuration Menu**

Press [Enter] to configure Multiple Boot Agent (MBA) parameters.

☞ **iSCSI Boot Configuration Menu**

Press [Enter] to configure iSCSI boot parameters.

☞ **Multi-Function Mode**

Virtualization mode configuration. System must be rebooted in order for changes to take effect.
Options available: SF/SR-IOV. Default setting is **SF**.

☞ **Blink LEDs**

Blink LEDs for a duration up to 15 seconds.
Default setting is **0**.

☞ **Chip Type**

Displays the chip type.

☞ **PCI Device ID**

Displays the PCI device ID.

☞ **Bus: Device: Function**

Displays the bus number, device number, and function number.

☞ **Link Status**

Displays the link status.

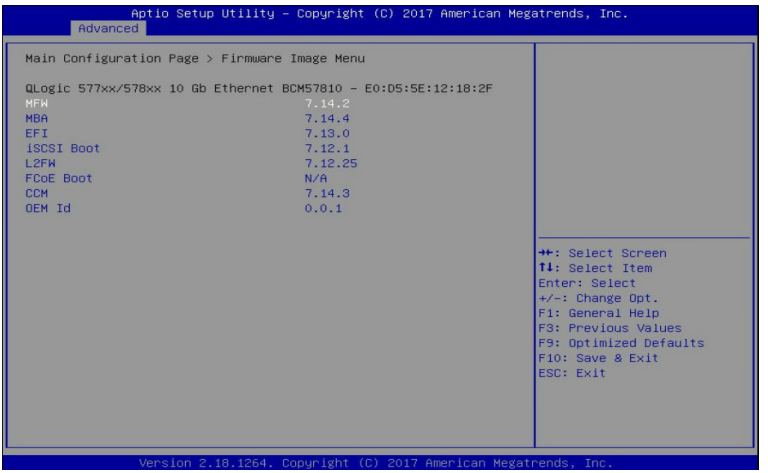
☞ **Parameter MAC Address**

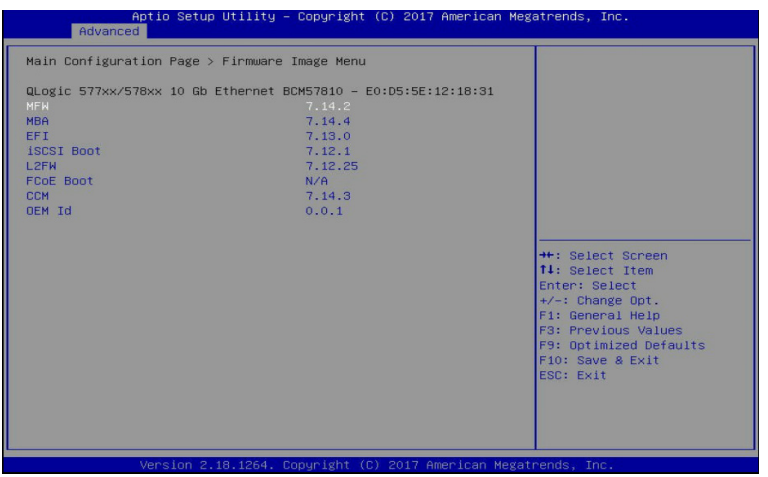
Displays the Permanent MAC Address.

☞ **Virtual MAC Address**

Displays the Virtual MAC Address.

5-2-2-1 Firmware Image Menu

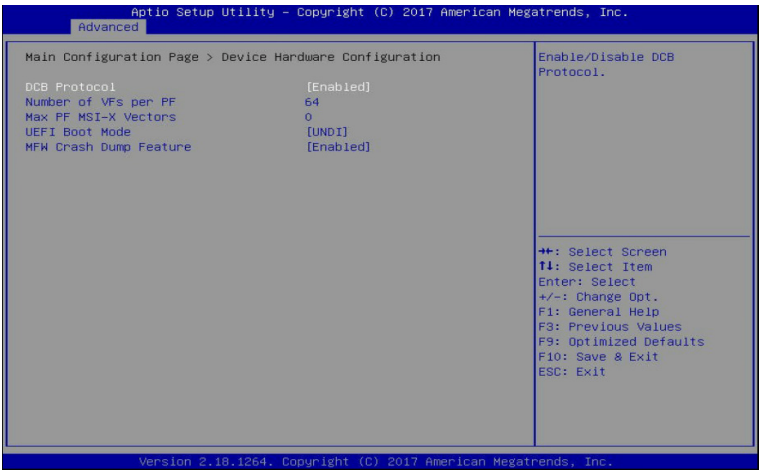




☞ **Main Configuration Page > Firmware Image Menu**

Displays the device's firmware version information.

5-2-2-2 Device Hardware Configuration Menu



☞ Main Configuration Page > Device Hardware Configuration Menu

Configures the device and port specific parameters. Please refer to help text defined per configurable parameter for more information.

☞ DCB Protocol

Enable/Disable the DCB Protocol.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ Number of VFs per PF

Displays the number of VFs per PF in multiple of 8 (0 to 64).

☞ Max PF MSI-X Vectors

Displays the maximum number of PF MSI-X Vectors. (0 to 64).

☞ UEFI Boot Mode

Specifies Driver Boot Mode in UEFI environment.

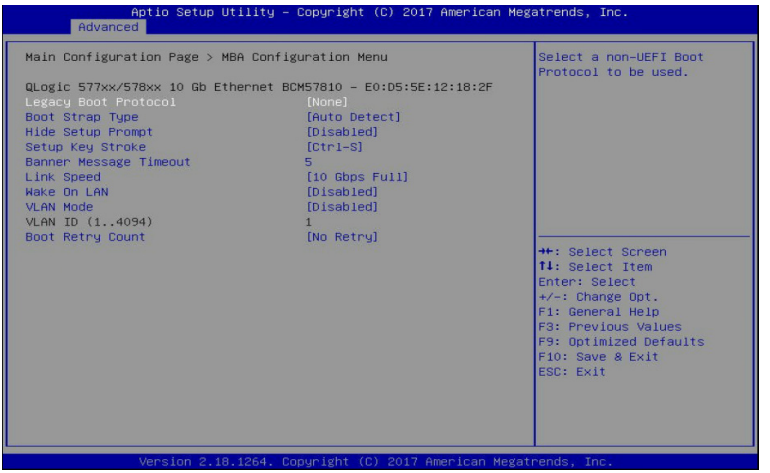
Default setting is **UNDI**.

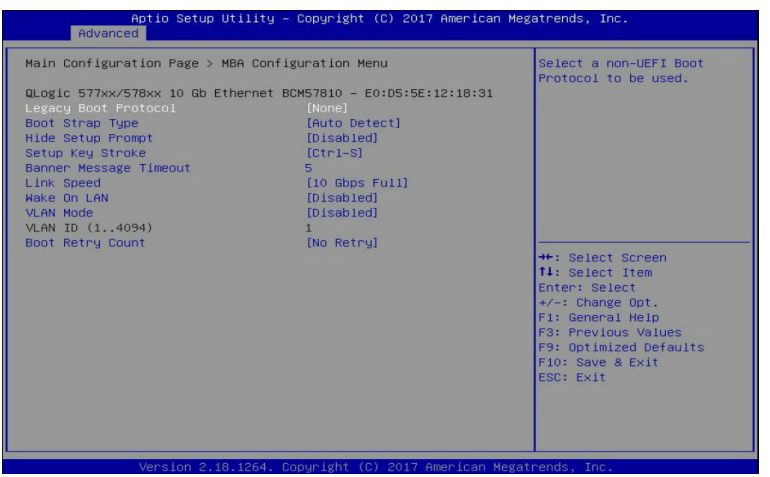
☞ MFW Crash Dump Feature

Enables MFW bootcode to collect critical device and system information during unanticipated system crash.

Options available: Enabled/Disabled. Default setting is **Enabled**.

5-2-2-3 MBA Configuration Menu





☞ **Main Configuration Page > MBA Configuration Menu**

Configures the Multiple Boot Agent (MBA) parameters.

☞ **QLogic 577xx/578xx 10 Gb Ethernet BCN57810**

☞ **Legacy Boot Protocol**

Selects a non-UEFI Boot Protocol to be used.

Options available: PXE/iSCSI/None. Default setting is **None**.

☞ Boot Strap Type

Selects the BIOS interrupt call type.

Auto Detect: Auto Detect interrupt type; BBS: BIOS Boot Specification; Int 18h: Interrupt vector to execute cassette BASIC; Int 19h: BIOS Interrupt vector used to load OS.

Options available: Auto Detect/BBS/Int 18h/Int 19h. Default setting is **Auto Detect**.

☞ Hide Setup Prompt

Configures whether Setup Prompt is displayed during ROM initialization.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ Setup Key Stroke

Configure key strokes to invoke configuration menu.

Options available: Ctrl-S/Ctrl-B. Default setting is **Ctrl-S**.

☞ Banner Message Timeout

Selects the timeout value. (0 defaults to 4 seconds, 15 is no delay, 1-14 is timeout value in seconds).

Default setting is **5**.

☞ Link Speed

Configures the link speed.

Default setting is **10 Gbps Full**.

☞ Wake On LAN

Configures Wake on LAN (WOL). This setting is per port.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ VLAN Mode

Configures the virtual LAN mode.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ VLAN ID (1..4094)

Displays the virtual LAN ID (1 to 4094).

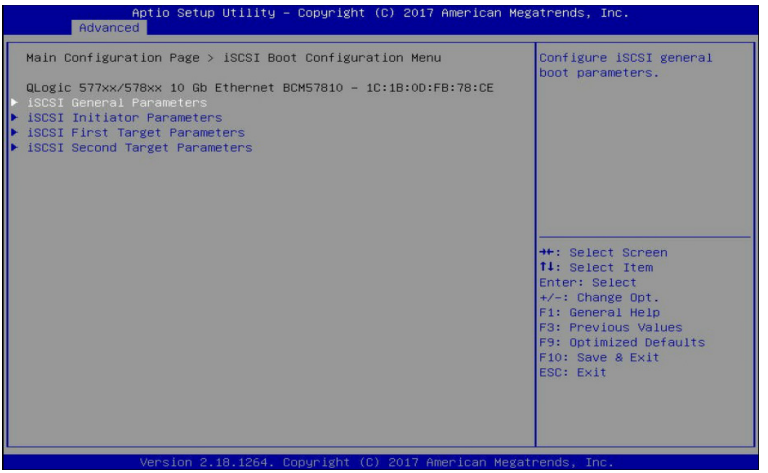
☞ Boot Retry Count

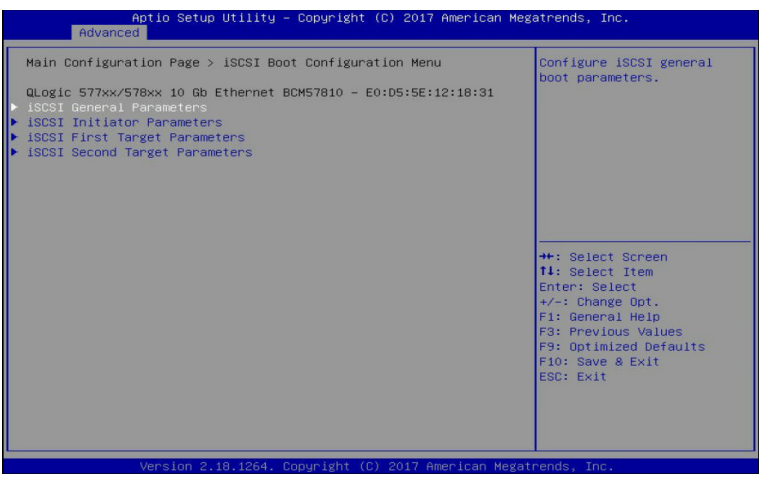
Selects the number of boot retries.

Options available: No Retry/1 Retry/2 Retries/3 Retries/4 Retries/5 Retries/6 Retries/Indefinite Retries.

Default setting is **No Retry**.

5-2-2-4 iSCSI Boot Configuration Menu





☞ **Main Configuration Page > iSCSI Boot Configuration Menu**

Configures the iSCSI boot parameters.

☞ **iSCSI General Parameters**

Press [Enter] for configuration of advanced items.

☞ **iSCSI Initiator Parameters**

Press [Enter] for configuration of advanced items.

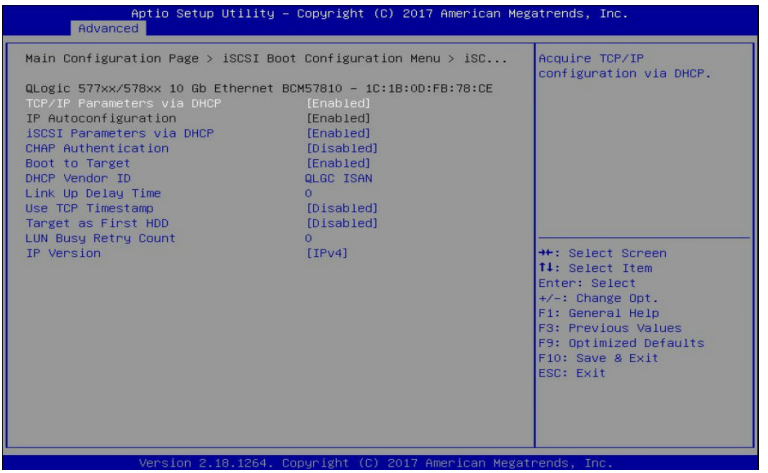
☞ **iSCSI First Target Parameters**

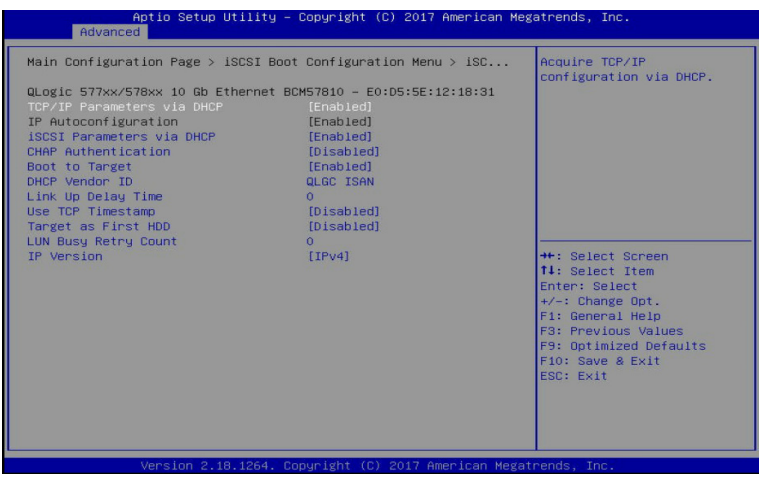
Press [Enter] for configuration of advanced items.

☞ **iSCSI Second Target Parameters**

Press [Enter] for configuration of advanced items.

5-2-2-4-1 iSCSI General Parameters





☞ **Main Configuration Page > iSCSI Boot Configuration Menu > iSCSI General Parameters**

Configures the iSCSI general boot parameters.

☞ **TCP/IP Parameters via DHCP**

Acquires the TCP/IP configuration via DHCP.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **IP Autoconfiguration**

Auto-configures the IP configuration.

Options available: Enabled/Disabled. Default setting is **Disabled**.

Please note that this item is configurable when TCP/IP Parameters via DHCP is set to Disabled.

☞ **iSCSI Parameters via DHCP**

Acquires the iSCSI parameters via DHCP.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **CHAP Authentication**

Enable/Disable the CHAP authentication.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Boot to Target**

Enable/Disable booting to iSCSI target after log-on.

Options available: Disabled/Enabled/One Time Disabled. Default setting is **Enabled**.

☞ **DHCP Vendor ID**

Press [Enter] to configures the DHCP vendor ID (up to 32 bytes long).

☞ **Link Up Delay Time**

Configures the link up to delay time in seconds (0..225).

☞ **Use TCP Timestamp**

Enable/Disable the TCP timestamp.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Target as first HDD**

Enable/Disable target appears as a first hard disk drive (HDD) in the system.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **LUN Busy Retry Count**

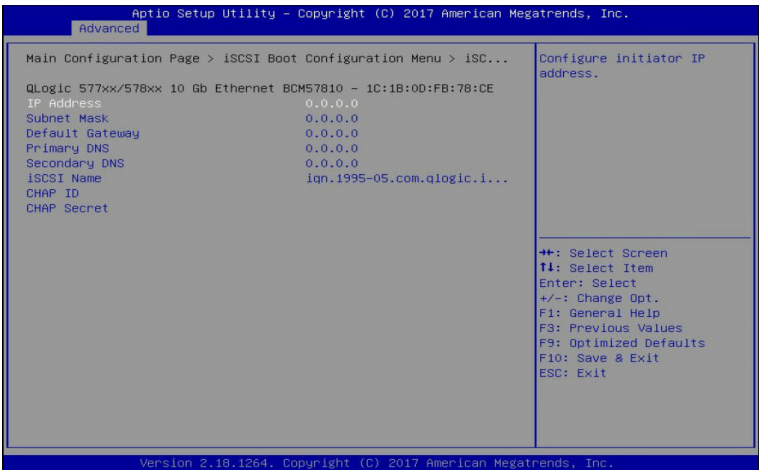
Configures the number of retries in 2 second intervals when LUN is busy (0..60).

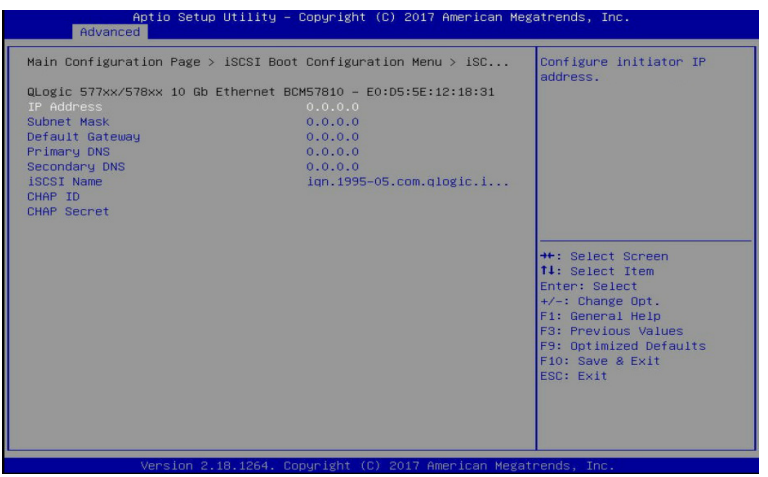
Default setting is **0**.

☞ **IP Version**

Displays the IP version supported. Modifying this parameter will reset all IP-related fields.

5-2-2-4-2 iSCSI Initiator Parameters





☞ **Main Configuration Page > iSCSI Boot Configuration Menu > iSCSI Initiator Parameters**

Configures the iSCSI initiator parameters.

☞ **IP Address**

Configures initiator IP address.

☞ **Subnet Mask**

Configures IP subnet mask.

☞ **Default Gateway**

Configures default gateway IP address.

☞ **Primary DNS**

Configures the primary DNS IP address.

☞ **Secondary DNS**

Configures the second DNS IP address.

☞ **iSCSI Name**

Configures the iSCSI name.

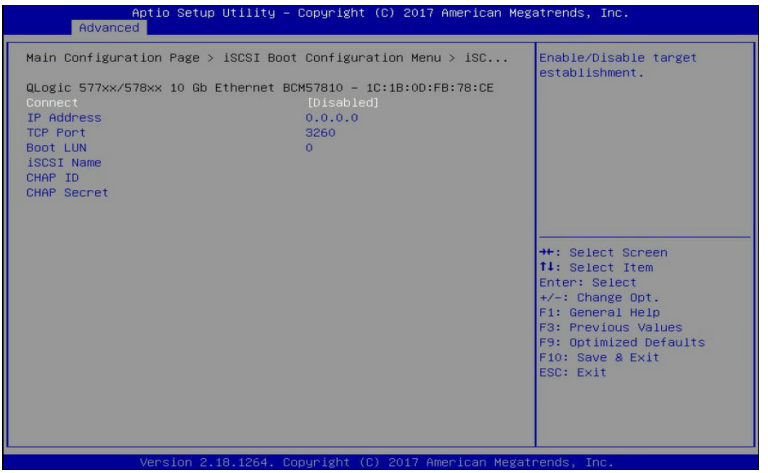
☞ **CHAP ID**

Configures the Challenge-Handshake Authentication Protocol (CHAP) ID (up to 128 characters in length).

☞ **CHAP Secret**

Configure the Challenge-Handshake Authentication Protocol (CHAP) Secret (12 to 16 characters in length).

5-2-2-4-3 iSCSI First Target/Second Target Parameters





☞ **Main Configuration Page > iSCSI Boot Configuration Menu > iSCSI First Target/ Second Target parameters**

Configures the iSCSI first target parameters.

☞ **Connect**

Enable/Disable the target establishment.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **IP Address**

Configures the target IP address.

☞ **TCP Port**

Configures the target TCP port number (13365535).

☞ **Boot LUN**

Configure the target boot LUN number (0..255).

☞ **iSCSI Name**

Configures the iSCSI name.

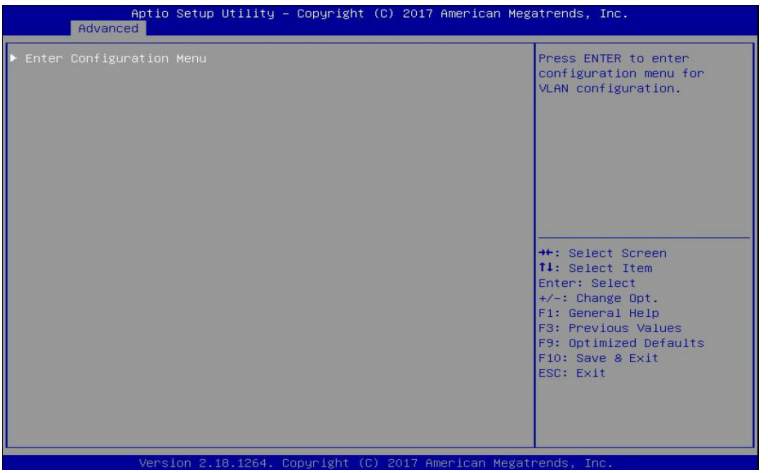
☞ **CHAP ID**

Configures the Challenge-Handshake Authentication Protocol (CHAP) ID (up to 128 characters in length).

☞ **CHAP Secret**

Configure the Challenge-Handshake Authentication Protocol (CHAP) Secret (12 to 16 characters in length).

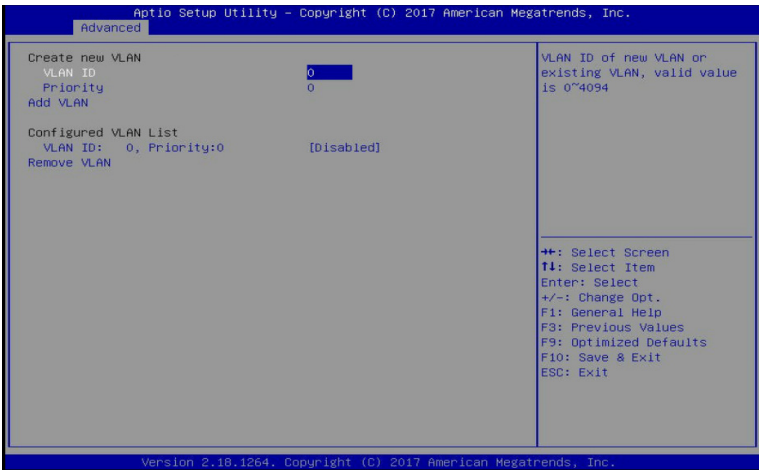
5-2-3 VLAN Configuration



☞ **Enter Configuration Menu**

Press [Enter] to enter configuration menu for VLAN configuration.

5-2-3-1 VLAN Configuration Menu



☞ **Create new VLAN**

☞ **VLAN ID**

Sets a VLAN ID of new VLAN or existing VLAN, valid value is 0 to 4094.

☞ **Priority**

Sets the 802.1Q Priority, valid value is 0 to 7.

☞ **Add VLAN**

Creates a new VLAN or update existing VLAN.

☞ **Configured VLAN List**

Displays the configured VLAN list information.

Options available: Enabled/Disabled. Default setting is **Disabled**.

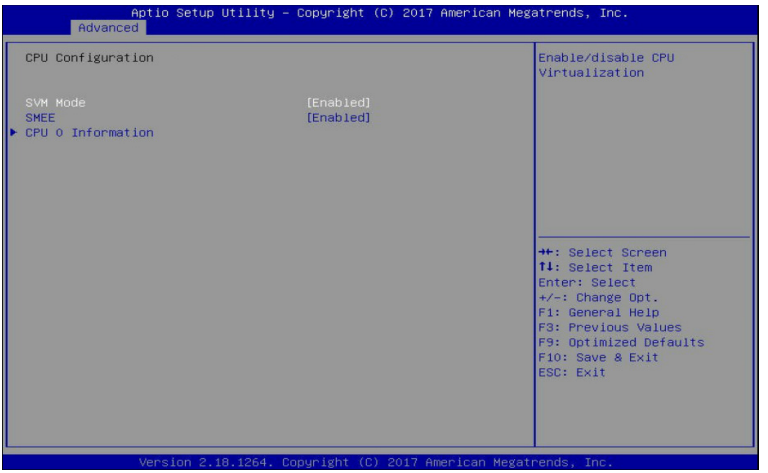
☞ **Remove VLAN**(Note)

Removes the selected VLANs.

Please note that this item is only executable when Configured VLAN List is set to Enabled, and once executed the Configured VLAN List will be updated accordingly.

(Note) Only Supported when **Configured VLAN List** is set to **Enabled**.

5-2-4 CPU Configuration



☞ **CPU Configuration**

☞ **SVM Mode**

Enable/disable the CPU Virtualization.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **SMEE**

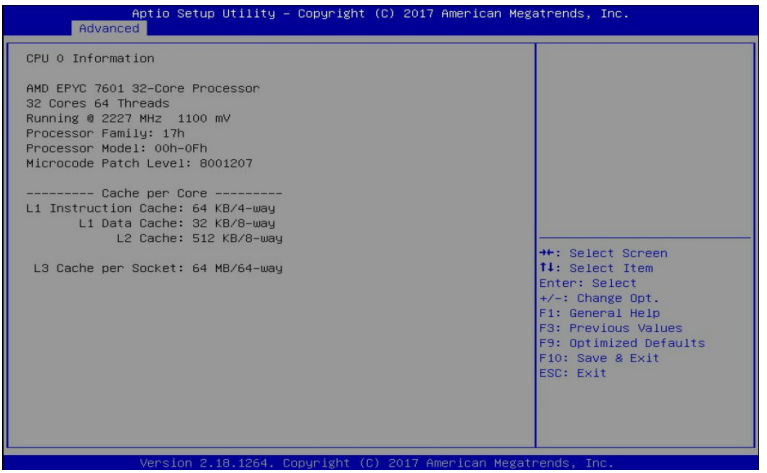
Controls the Secure Memory Encryption Enable (SMEE) function.

Options available: Enabled/Disabled. Default setting is **Enabled**.

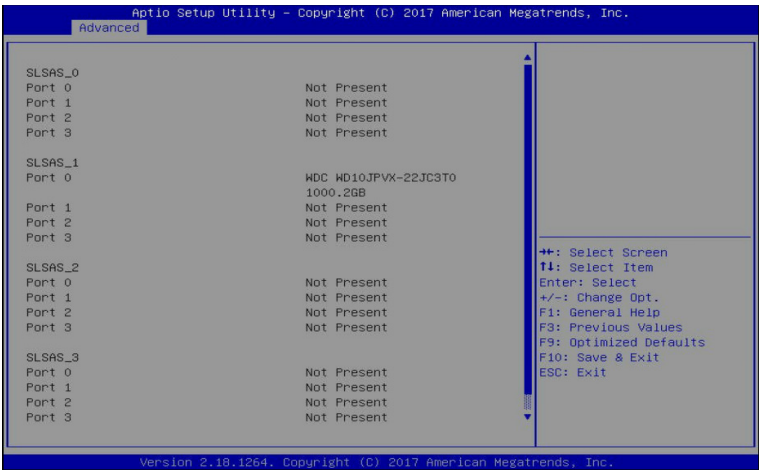
☞ **CPU 0 Information**

Press [Enter] to view the memory information related to CPU 0.

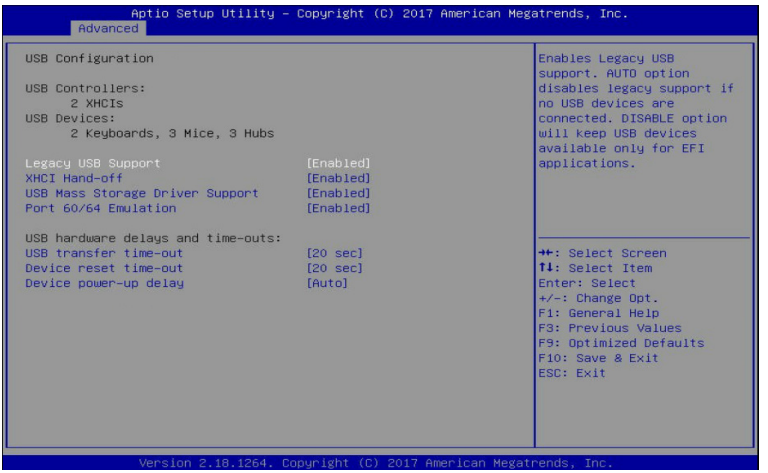
5-2-4-1 CPU 0 Information



5-2-5 SATA Configuration



5-2-6 USB Configuration



☞ **USB Configuration**

☞ **USB Controllers:**

Displays the supported USB controllers.

☞ **USB Devices:**

Displays the USB devices connected to the system.

☞ **Legacy USB Support**

Enable/disable the Legacy USB support fuction. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.

Options available: Enabled/Disabled/Auto. Default setting is **Enabled**.

☞ **XHCI Hand-off**

This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **USB Mass Storage Driver Support**(Note)

Enable/Disable the USB Mass Storage Driver Support.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **Port 60/64 Emulation**

Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB hardware OSes.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **USB hardware delays and time-outs:**

☞ **USB transfer time-out**

The time-out value for Control, Bulk, and Interrupt transfers.

Options available: 1 sec/5 sec/10 sec/20 sec. Default setting is **20 sec**.

(Note) This item is present only if you attach USB devices.

☞ **Device reset time-out**

USB mass storage device Start Unit command time-out.

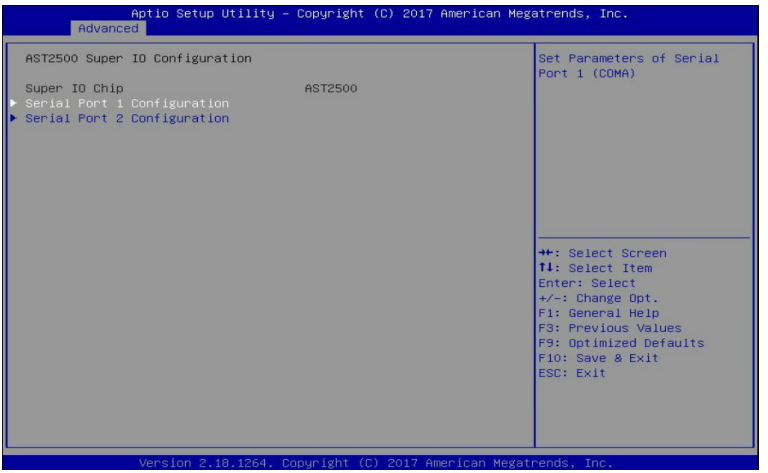
Options available: 10 sec/20 sec/30 sec/40 sec. Default setting is **20 sec**.

☞ **Device power-up delay**

Maximum time the device will take before it properly reports itself to the Host Controller. "Auto" uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

Options available: Auto/Manual. Default setting is **Auto**.

5-2-7 AST2500 Super IO Configuration



☞ **AST2500 Super IO Configuration**

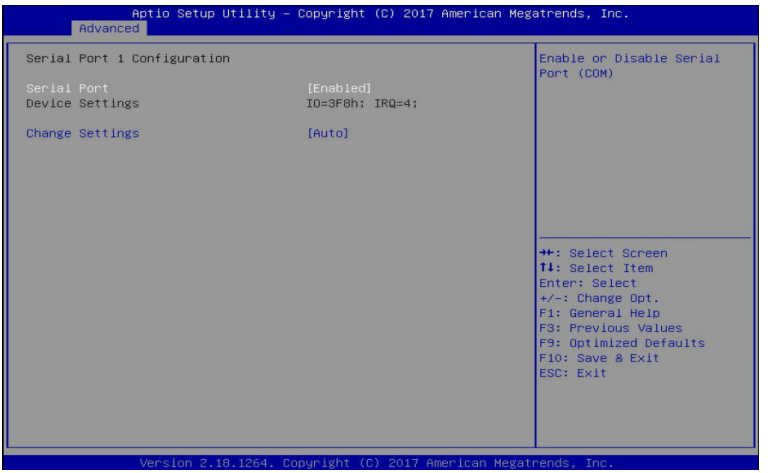
☞ **Super IO Chip**

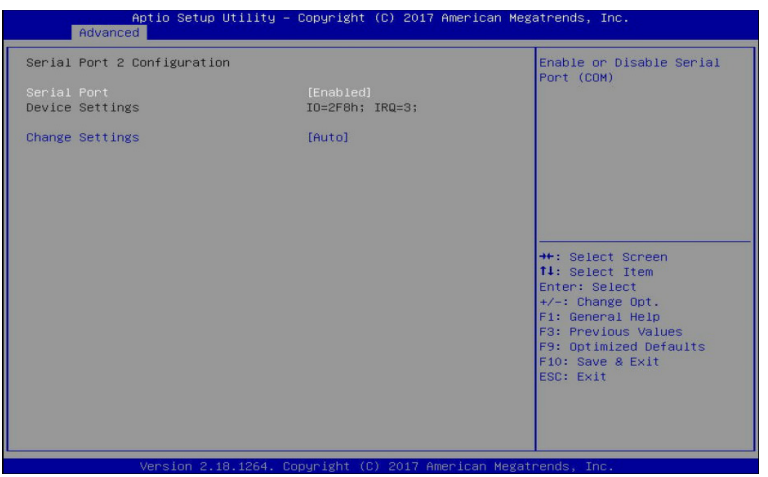
Displays the super IO chip information.

☞ **Serial Port 1/2 Configuration**

Press [Enter] for configuration of advanced items.

5-2-7-1 Serial Port 1/2 Configuration





☞ **Serial Port 1/2 Configuration**

☞ **Serial Port**(Note1)

Enable/Disable the Serial Port (COM). When set to Enabled allows you to configure the Serial port 1/2 settings. When set to Disabled, displays no configuration for the serial port.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **Devices Settings**(Note2)

Displays the Serial Port 1/2 device settings.

(Note1) Advanced items prompt when this item is defined. (Note)

(Note2) This item appears when **Serial Port** is set to **Enabled**.

☞ **Change Settings**[Note2]

Select an optimal settings for Super IO Device.

Options available for Serial Port 1:

Auto

IO=3F8h; IRQ=4;

IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

Default setting is **Auto**.

Options available for Serial Port 2:

Auto

IO=2F8h; IRQ=3;

IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

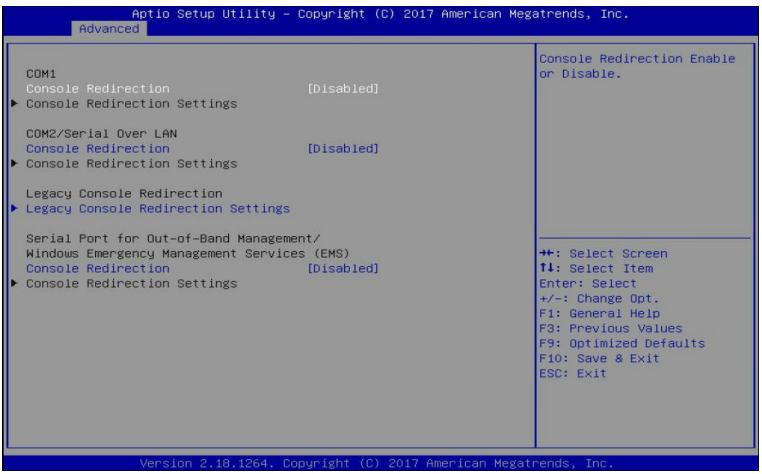
IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

Default setting is **Auto**.

Please note that this item is configurable when Serial Port is set to Enabled.

5-2-8 Serial Port Console Redirection



☞ **COM1/COM2 Serial Over LAN Console Redirection**(Note)

Select whether to enable console redirection for the specified device. Console redirection enables the users to manage the system from a remote location.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Legacy Console Redirection**

Selects a COM port for Legacy serial redirection. The options are dependent on the available COM ports.

☞ **Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS) Console Redirection**(Note)

Selects a COM port for EMS console redirection. EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.

Options available: Enabled/Disabled. Default setting is **Disabled**.

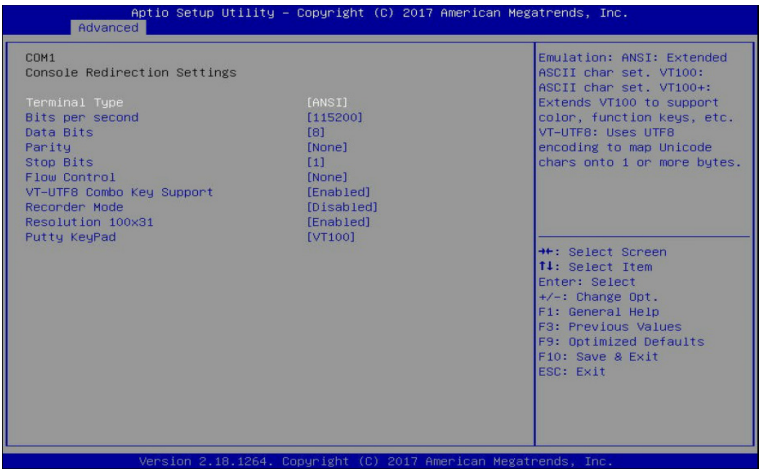
☞ **COM1/COM2 Serial Over LAN/Legacy/Serial Port for Out-of-Band EMS Console Redirection Settings**

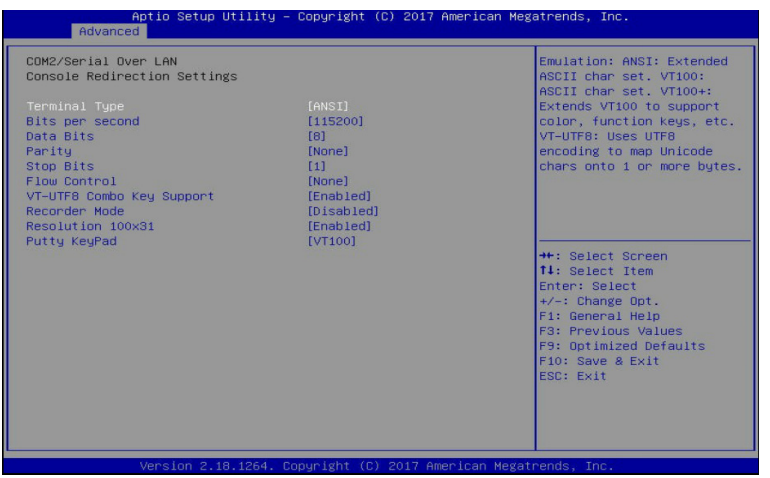
Press [Enter] for configuration of advanced items.

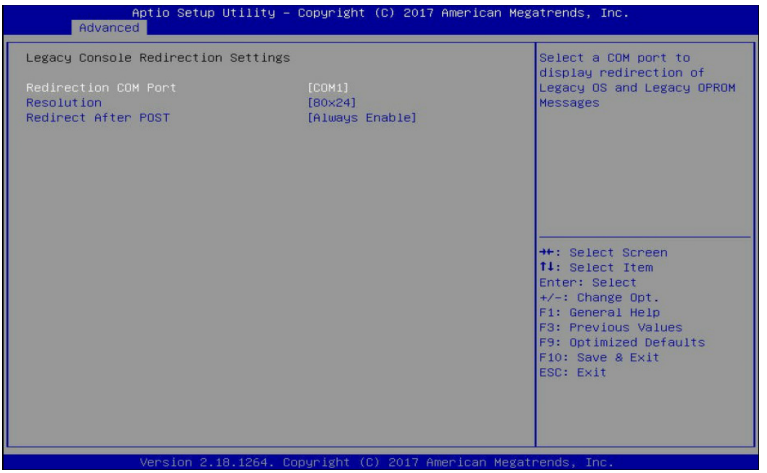
Please note that this item is configurable when COM1/COM2 Serial Over LAN/Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.

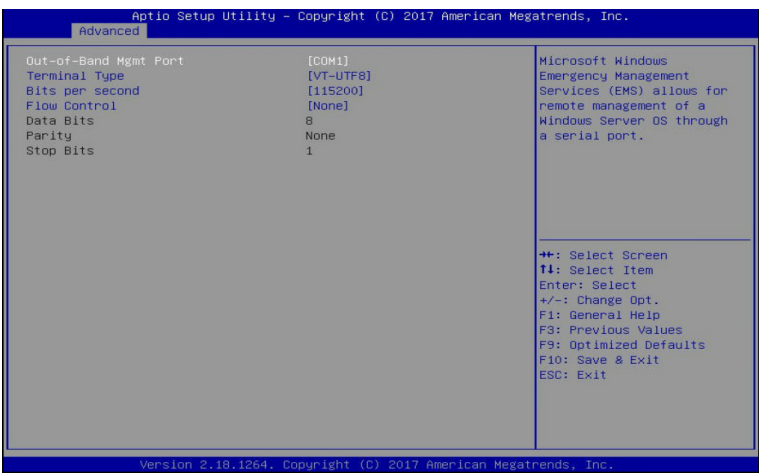
(Note) Advanced items prompt when this item is defined.

5-2-8-1 COM1/COM2 Serial Over LAN/Legacy/Serial Port for Out-of-Band EMS Console Redirection Settings









☞ COM1/COM2 Serial Over LAN Console Redirection Settings

☞ Terminal Type

Selects a terminal type to be used for console redirection.

Options available: VT100/VT100+/ANSI /VT-UTF8. Default setting is **ANSI**.

☞ Bits per second

Selects the transfer rate for console redirection.

Options available: 9600/19200/38400/57600/115200. Default setting is **115200**.

☞ Data Bits

Selects the number of data bits used for console redirection.

Options available: 7/8. Default setting is **8**.

☞ Parity

A parity bit can be sent with the data bits to detect some transmission errors.
Even: parity bit is 0 if the num of 1's in the data bits is even.
Odd: parity bit is 0 if num of 1's in the data bits is odd.
Mark: parity bit is always 1. Space: Parity bit is always 0.
Mark and Space Parity do not allow for error detection.
Options available: None/Even/Odd/Mark/Space. Default setting is **None**.

☞ Stop Bits

Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Options available: 1/2. Default setting is **1**.

☞ Flow control

Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
Options available: None/Hardware RTS/CTS. Default setting is **None**.

☞ VT-UTF8 Combo Key Support

Enable/Disable the VT-UTF8 Combo Key Support.
Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ Recorder Mode(Note)

When this mode enabled, only texts will be send. This is to capture Terminal data.
Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ Resolution 100x31(Note)

Enable/Disable extended terminal resolution.
Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ Putty KeyPad(Note)

Selects FunctionKey and KeyPad on Putty.
Options available: T100/LINUX/XTERMR6/SCO/ESCN/VT400. Default setting is **VT100**.

☞ Legacy Console Redirection Settings

☞ Redirection COM Port

Selects a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
Options available: COM1/COM2 Serial Over LAN. Default setting is **COM1**.

☞ Resolution

On Legacy OS, the Number of Rows and Columns supported redirection.
Options available: 80x24/80x25. Default setting is **80x24**.

☞ Redirect After POST

When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS.
When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS.
Options available: Bootloader/Always Enable. Default setting is **Always Enable**.

(Note) Advanced items prompt when this item is defined.

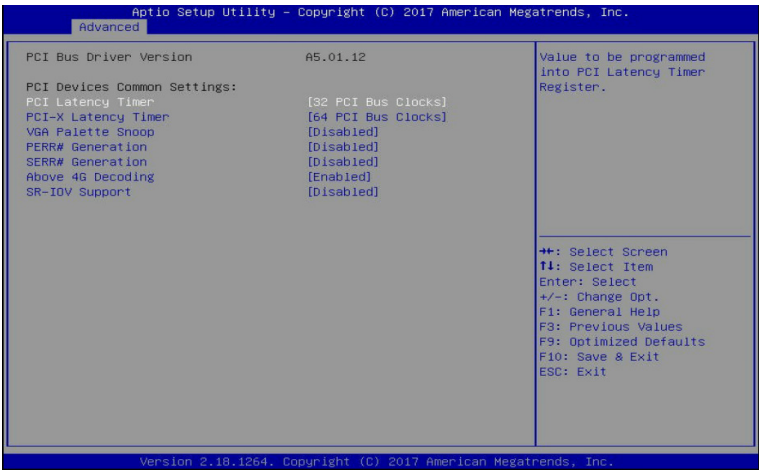
☞ **Serial Port for Out-of-Band EMS Console Redirection Settings**

☞ **Out-of-Band Mgmt Port**

Microsoft Windows Emerency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port.

Options available: COM1/COM2 Serial Over LAN. Default setting is **COM1**.

5-2-9 PCI Subsystem Settings



☞ PCI Bus Driver Version

Displays the PCI Bus Driver version information.

☞ PCI Devices Common Settings:

☞ PCI Latency Timer

Sets the value to be programmed into PCI Latency Timer Register.

Options available: 32 PCI Bus Clocks/64 PCI Bus Clocks/96 PCI Bus Clocks/128 PCI Bus Clocks/160 PCI Bus Clocks/192 PCI Bus Clocks/224 PCI Bus Clocks/248 PCI Bus Clocks.

Default setting is **32 PCI Bus Clocks**.

☞ PCI-X Latency Timer

Sets the value to be programmed into PCI-X Latency Timer Register.

Options available: 32 PCI Bus Clocks/64 PCI Bus Clocks/96 PCI Bus Clocks/128 PCI Bus Clocks/160 PCI Bus Clocks/192 PCI Bus Clocks/224 PCI Bus Clocks/248 PCI Bus Clocks.

Default setting is **64 PCI Bus Clocks**.

☞ VGA Palette Snoop

Enable/Disable VGA Palette Registers Snooping.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ PERR#/SERR# Generation

Enable/Disable PCI Device to Generate PERR#/SERR#.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ Above 4G Decoding

Enable/Disable 64-bit capable Devices to be decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).

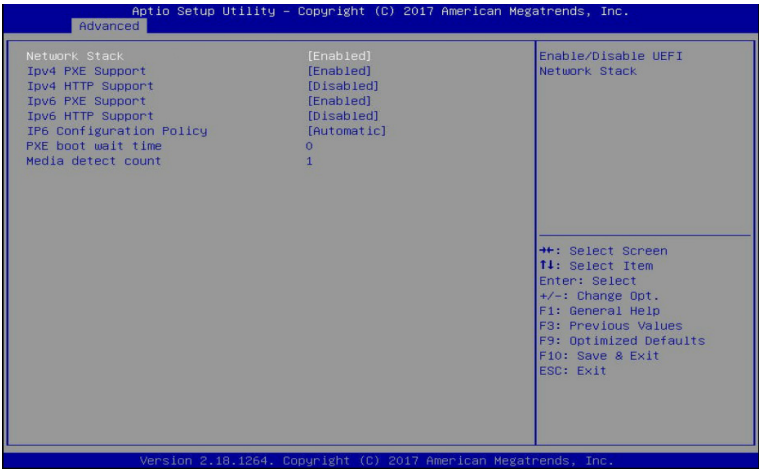
Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **SR-IOV Support**

If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support.

Options available: Enabled/Disabled. Default setting is **Disabled**.

5-2-10 Network Stack



☞ **Network stack**

Enable/Disable the UEFI network stack.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **Ipv4 PXE Support**(Note)

Enable/Disable the Ipv4 PXE feature.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **Ipv4 HTTP Support**(Note)

Enable/Disable the Ipv4 HTTP feature.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Ipv6 PXE Support**(Note)

Enable/Disable the Ipv6 PXE feature.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Ipv6 HTTP Support**(Note)

Enable/Disable the Ipv6 HTTP feature.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Ipv6 Configuration Policy**(Note)

Sets the IP6 Configuration Policy.

Options available: Automatic/Manual. Default setting is **Manual**.

☞ **PXE boot wait time**(Note)

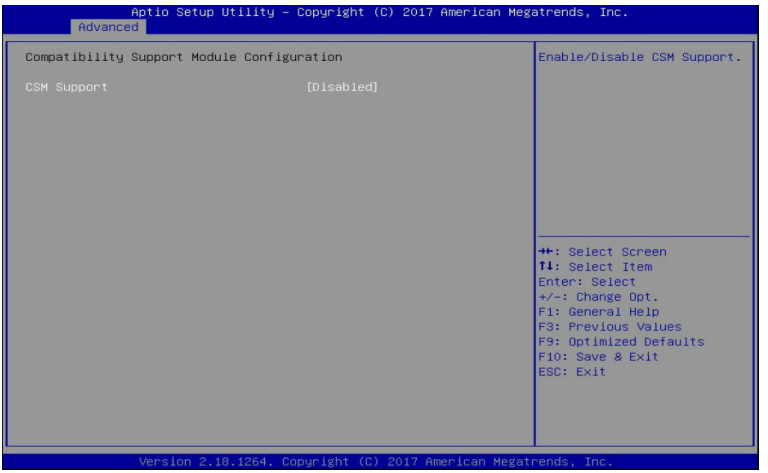
Press the <+> / <-> keys to increase or decrease the desired values.

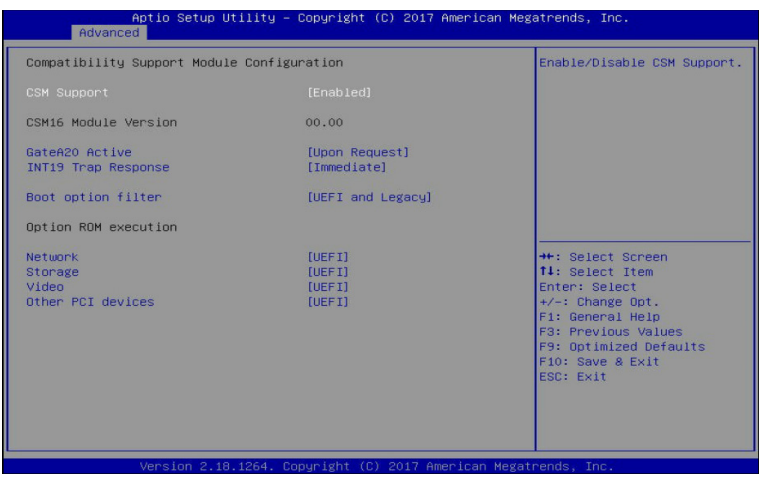
☞ **Media detect count**(Note)

Press the <+> / <-> keys to increase or decrease the desired values.

(Note) This item appears when **Network Stack** is set to **Enabled**.

5-2-11 CSM Configuration





☞ **Compatibility Support Module Configuration**

☞ **CSM Support**(Note)

Enable/Disable the Compatibility Support Module (CSM) support.
Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **CSM16 Module Version**

Displays the CSM module version information.
Please note that this item is visible when CSM Support is set to Enabled.

(Note) Advanced items prompt when this item is set to **Enabled**.

☞ GateA20 Active

When set to Upon Request, GA20 can be disabled using BIOS services. When set to Always, GA20 cannot be disabled; this option is useful when any RT code is executed above 1MB.

Options available: Upon Request/Always. Default setting is **Upon Request**.

Please note that this item is configurable when CSM Support is set to Enabled.

☞ INT19 Trap Response

Configures BIOS reaction on INT19 trapping by Option ROM. When set to Immediate, the system executes the trap right away. When set to Postponed, the system executes the trap during legacy boot.

Options available: Immediate/Postponed. Default setting is **Immediate**.

Please note that this item is configurable when CSM Support is set to Enabled.

☞ Boot option filter

Controls the Legacy/UEFI ROMs priority.

Options available: UEFI and Legacy/Legacy only/UEFI. Default setting is **UEFI and Legacy**.

Please note that this item is configurable when CSM Support is set to Enabled.

☞ Option ROM execution

☞ Network

Controls the execution of UEFI and Legacy PXE Option ROM.

Options available: Do not launch/UEFI/Legacy. Default setting is **UEFI**.

Please note that this item is configurable when CSM Support is set to Enabled.

☞ Storage

Controls the execution of UEFI and Legacy Storage Option ROM.

Options available: Do not launch/UEFI/Legacy. Default setting is **UEFI**.

Please note that this item is configurable when CSM Support is set to Enabled.

☞ Video

Controls the execution of UEFI and Legacy Video Option ROM.

Options available: Do not launch/UEFI/Legacy. Default setting is **UEFI**.

Please note that this item is configurable when CSM Support is set to Enabled.

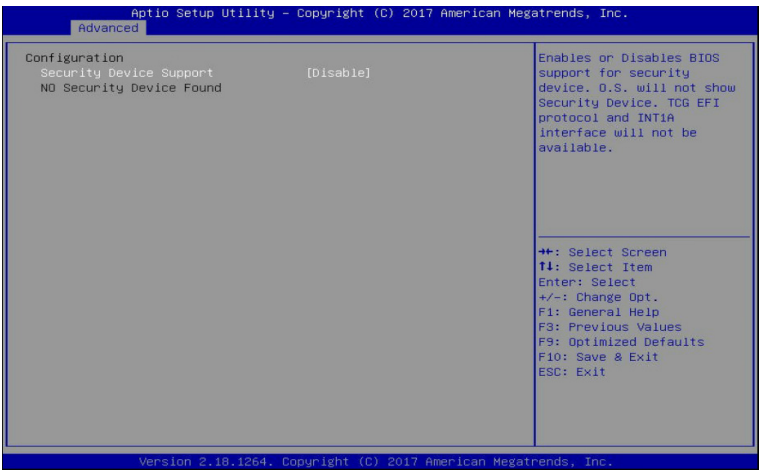
☞ Other PCI devices

Determines Option ROM execution policy for devices other than Network, Storage, or Video.

Options available: Do not launch/UEFI/Legacy. Default setting is **UEFI**.

Please note that this item is configurable when CSM Support is set to Enabled.

5-2-12 Trusted Computing



☞ **Configuration**

☞ **Security Device Support**

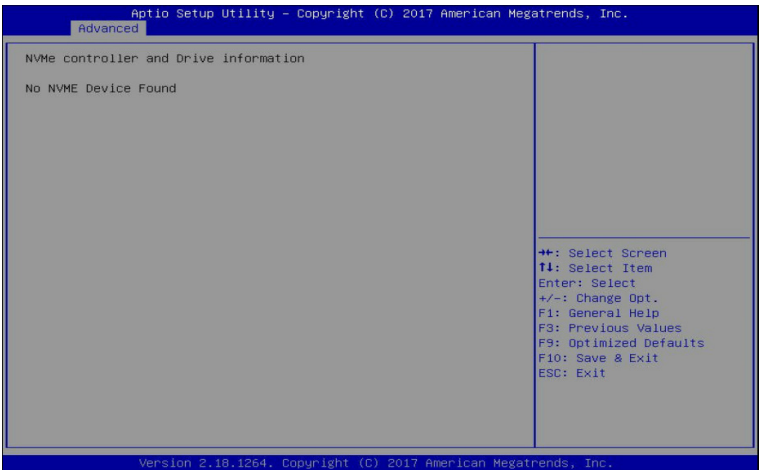
Enable/Disable the TPM support feature.

Options available: Enable/Disable. Default setting is **Disable**.

☞ **Current Status Information**

Displays current TPM status information.

5-2-13 NVMe Configuration



☞ **NVMe controller and Drive information**

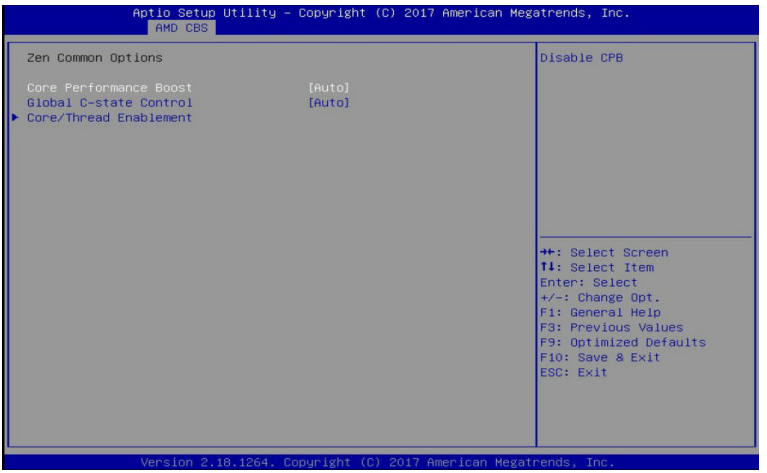
Displays the NVMe devices connected to the system.

5-3 AMD CBS Menu

AMD CBS menu displays submenu options for configuring the CPU-related information that the BIOS automatically sets. Select a submenu item, then press [Enter] to access the related submenu screen.



5-3-1 Zen Common Options



☞ **Zen Common Options**

☞ **Core Performance Boost**

Enable/disable the Core Performance Boost.

Options available: Disabled/Auto. Default setting is **Auto**.

☞ **Global C-state Control**

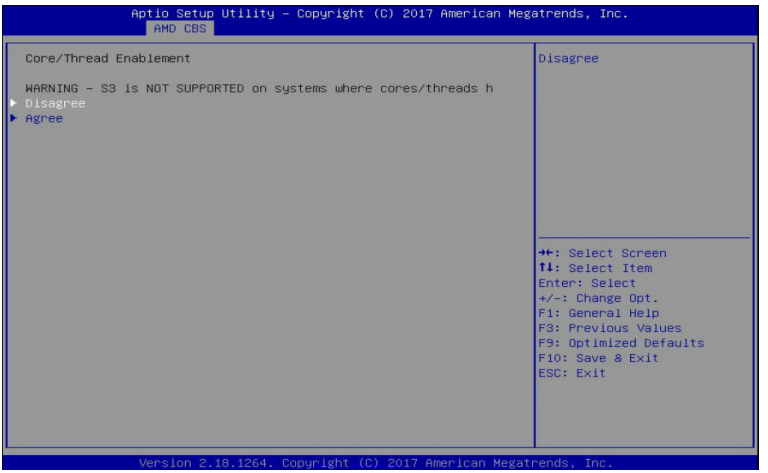
Controls the IO based C-state generation and DF C-states.

Options available: Disabled/Enabled/Auto. Default setting is **Auto**.

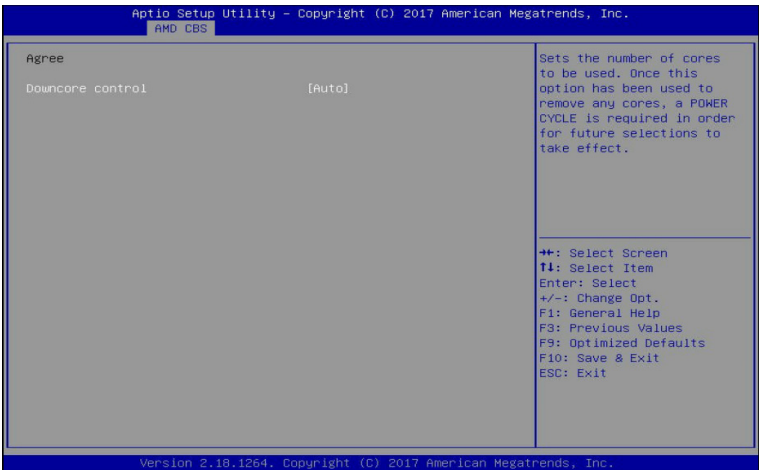
☞ **Core/Thread Enablement**

Press [Enter] for configuration of advanced items.

5-3-1-1 Core/Thread Enablement







☞ **Core/Thread Enablement**

Displays the Core/Thread Enablement information.

☞ **Disagree**

Disagrees with the Core/Thread Enablement settings.

☞ **Agree**

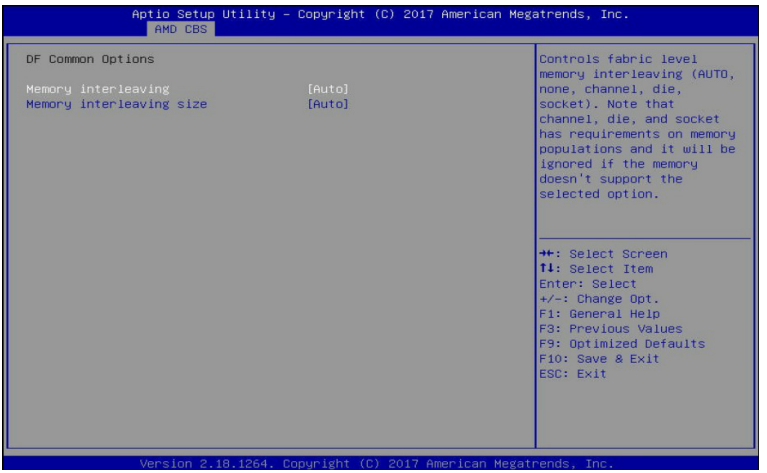
Agrees with the Core/Thread Enablement settings.

☞ **Downcore control**

Sets the number of cores to be used. Once this option has been used to remove any cores, a POWER CYCLE is required in order for future selections to take effect.

Options available: Two (1+1) / Two (2+0) / Three (3+0) / Four (2+2) / Four (4+0) / Six (3+3) / Auto. Default setting is **Auto**.

5-3-2 DF Common Options



☞ **DF Common Options**

☞ **Memory interleaving**

Controls fabric level memory interleaving (AUTO, none, channel, die, socket). Note that channel, die, and socket options have requirements on memory populations and it will be ignored if the memory doesn't support the selected option.

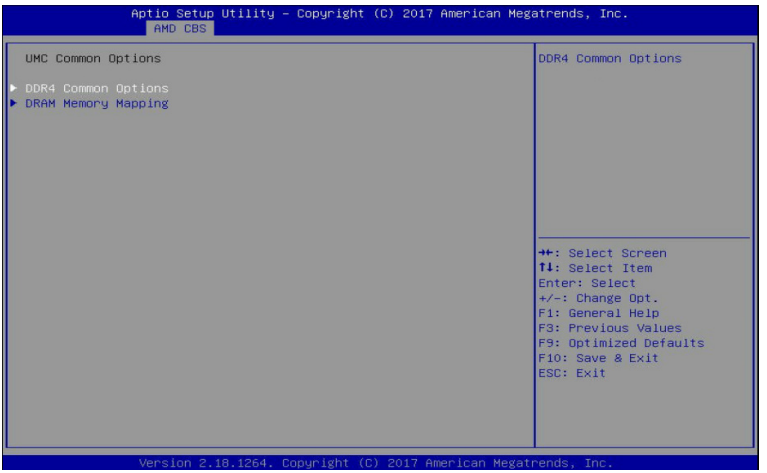
Options available: None/Channel/Die/Socket/Auto. Default setting is **Auto**.

☞ **Memory interleaving size**

Controls the memory interleaving size. The valid value are AUTO, 256 bytes, 512 bytes, 1Kbytes or 2Kbytes. This determines the starting address of the interleave (bit 8, 9, 10 or 11).

Options available: 256 Bytes/512 Bytes/1 KB/2KB/Aut. Default setting is **Auto**.

5-3-3 UMC Common Options



☞ **UMC Common Options**

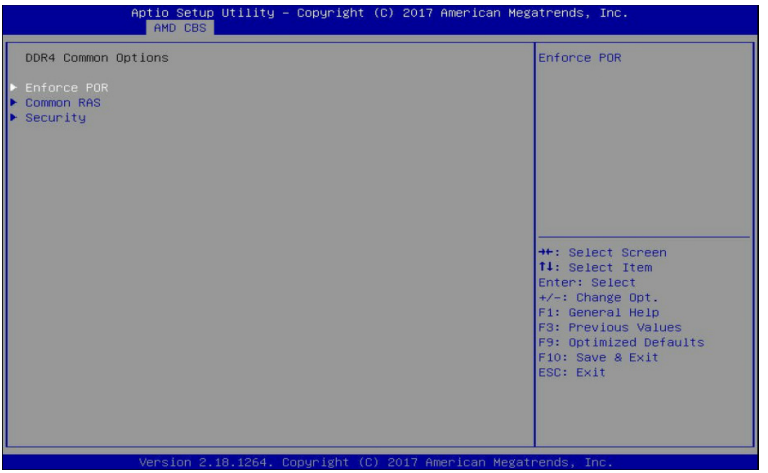
☞ **DDR4 Common Options**

Press [Enter] for configuration of advanced items.

☞ **DRAM Memory Mapping**

Press [Enter] for configuration of advanced items.

5-3-3-1 DDR4 Common Options



☞ **DDR4 Common Options**

☞ **Enforce POR**

Press [Enter] to configure the enforce POR.

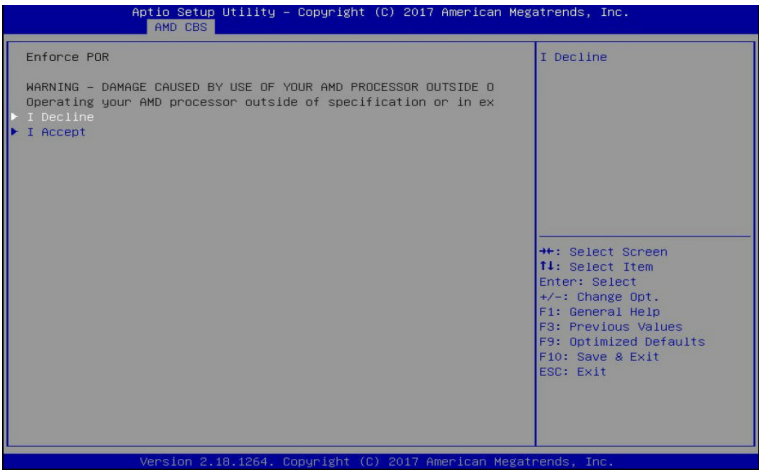
☞ **Common RAS**

Press [Enter] to configure the common RAS.

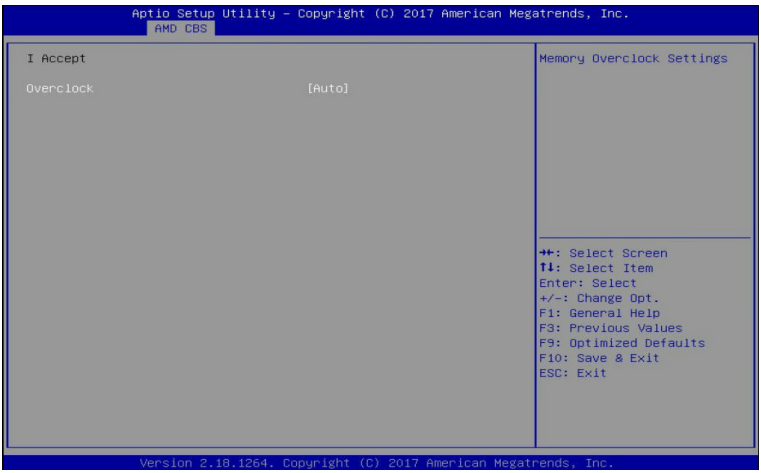
☞ **Security**

Press [Enter] to configure the security.

5-3-3-1-1 Enforce POR







☞ **Enforce POR**

Enables enforcement of Plan Of Record (POR) restrictions for DDR4 frequency and voltage programming. Memory speeds will be capped at Intel guidelines.

WARNING - DAMAGE CAUSED BY USE OF YOUR AMD PROCESSOR OUTSIDE OF SPECIFICATION OR IN EXCESS OF FACTORY SETTINGS ARE NOT COVERED UNDER YOUR AMD PRODUCT WARRANTY AND MAY NOT BE COVERED BY YOUR SYSTEM MANUFACTURER'S WARRANTY.

☞ **I Decline**

Declines enabling Enforce POR.

☞ **I Accept**

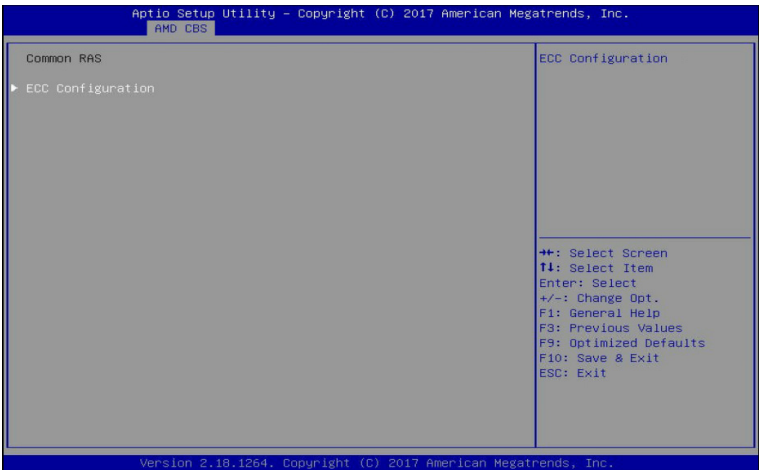
Accepts enabling Enforce POR.

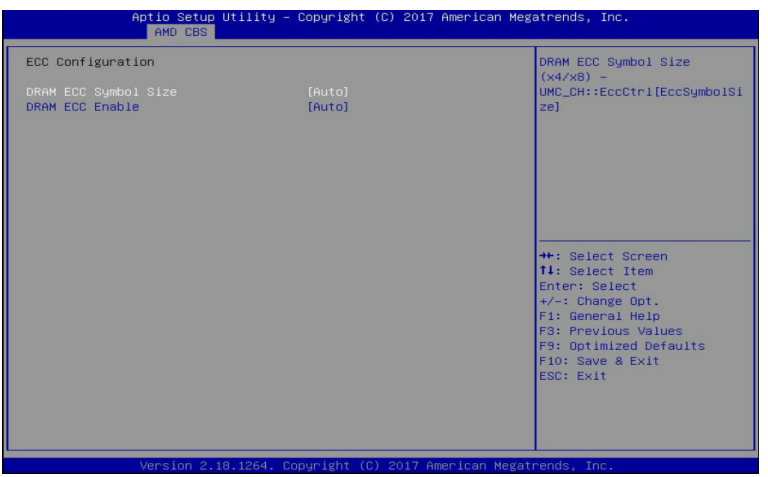
☞ **Overclock**

Configures the memory overclock settings.

Options available: Auto/Enabled. Default setting is **Auto**.

5-3-3-1-2 Common RAS





☞ **Common RAS**

☞ **ECC Configuration**

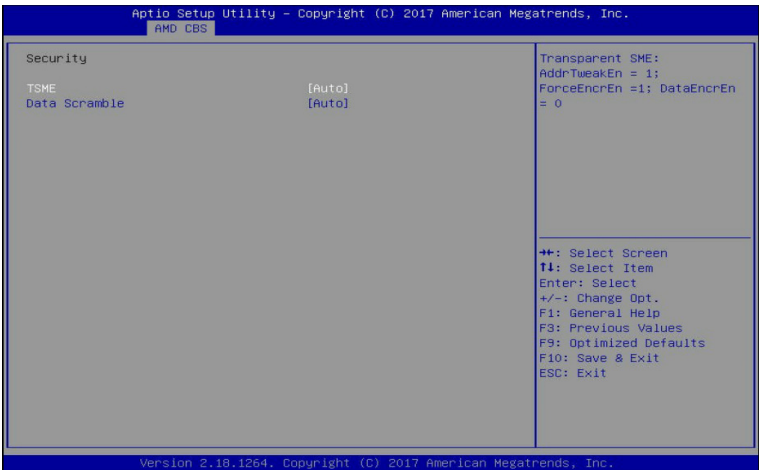
☞ **DRAM ECC Symbol Size**

Configures the DRAM ECC Symbol Size. (x4/x8) - EMC_CH::EccCtrl[ECCsymbolSize].
Options available: x4/x8/Auto. Default setting is **Auto**.

☞ **DRAM ECC Enable**

Enable/disable DRAM ECC. When set to Auto, it will set ECC to enable.
Options available: Disabled/Enabled/Auto. Default setting is **Auto**.

5-3-3-1-3 Security



☞ **Security**

☞ **TSME**

Transparent SME: AddrTweakEn = 1; ForceEncrEn = 1; DataEncrEn= 0.

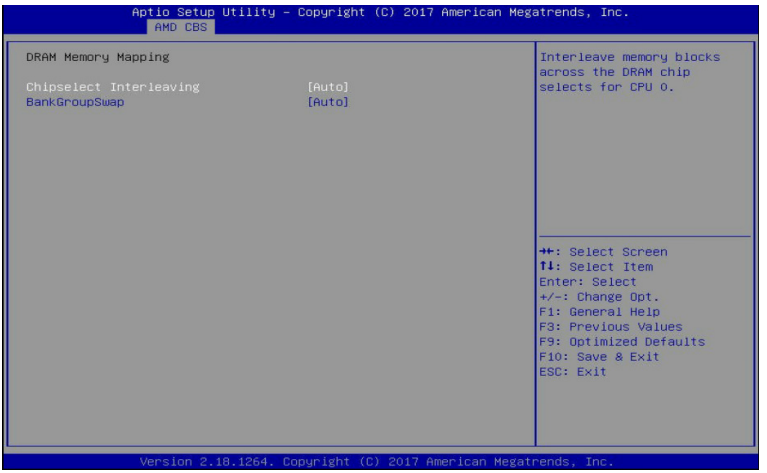
Options available: Enabled/Disabled/Auto. Default setting is **Auto**.

☞ **Data Scramble**

Data scrambling: DataScrambleEn.

Options available: Enabled/Disabled/Auto. Default setting is **Auto**.

5-3-3-2 DRAM Memory Mapping



☞ **DRAM Memory Mapping**

☞ **Chipselect Interleaving**

Interleave memory blocks across the DRAM chip selects for CPU 0.

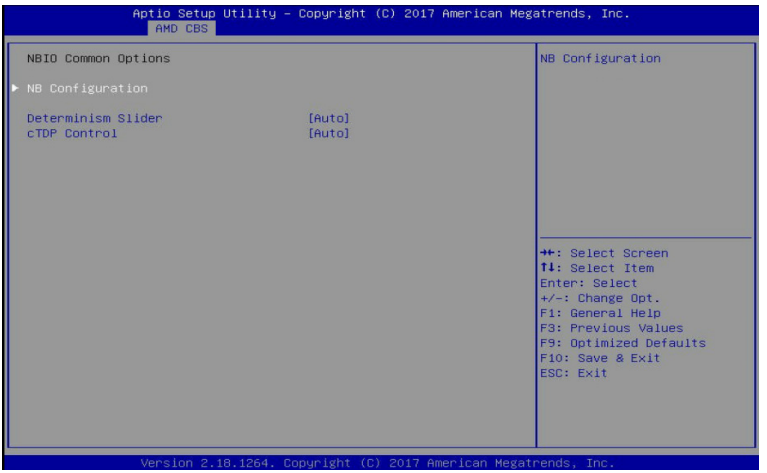
Options available: Disabled/Auto. Default setting is **Auto**.

☞ **BankGroupSwap**

Configures the BankGroupSwap. BankGroupSwap (BGS) is a new memory mapping option in AGESA that alters how applications get assigned to physical locations within the memory modules. When this option sets to Auto, it is null: No help string.

Options available: Enabled/Disabled/Auto. Default setting is **Auto**.

5-3-4 NBIO Common Options



☞ **NBIO Common Options**

☞ **NB Configuration**

Press [Enter] to configure the NB configuration.

☞ **Determinism Slider**

Auto = Use default performance determinism settings.

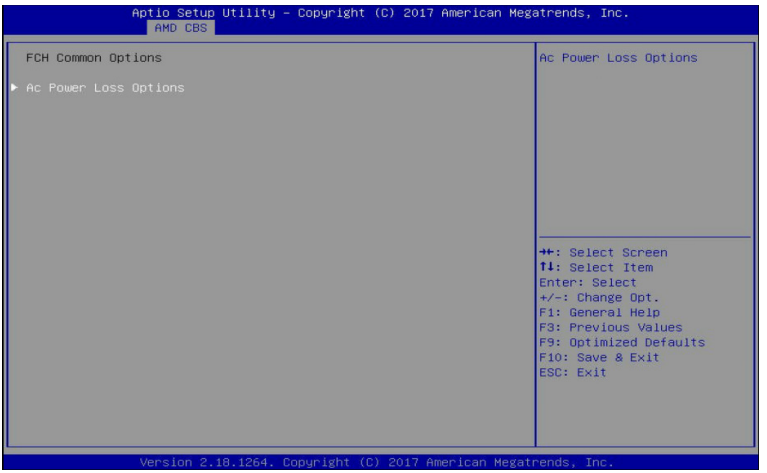
Options available: Auto/Power/Performance. Default setting is **Auto**.

☞ **cTDP Control**

Auto = Use the fused cTDP; Manual = User can set customized cTDP.

Options available: Manual/Auto. Default setting is **Auto**.

5-3-5 FCH Common Options



☞ **FCH Common Options**

☞ **AC Power Loss Options**

Press [Enter] to configure the AC loss control.

5-3-5-1 AC Power Loss Options



☞ **AC Power Loss Options**

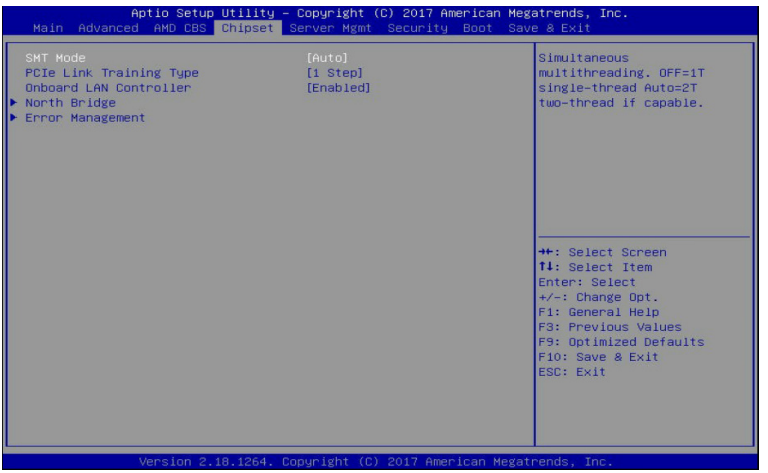
☞ **AC Loss Control**

Selects the AC Loss Control method.

Options available: Always Off/Always On/Reserved/Previous. Default setting is **Always Off**.

5-4 Chipset Setup Menu

Chipset Setup menu displays submenu options for configuring the function of the North Bridge. Select a submenu item, then press [Enter] to access the related submenu screen.



☞ SMT Mode

Enables imultaneous multithreading (SMT). Off=1T single-thread; Auto=2T two-thread if capable.
Options available: Off/Auto. Default setting is **Auto**.

☞ PCIe Link Training Type

Debugges the PCIe link training issue in 1 or 2 steps.
Options available: 1 Step/2 Step. Default setting is **2 Step**.

☞ Onboard LAN Controller

Enable/Disable LAN controller.
Options available: Enabled/Disabled. Default setting is **Enabled**.

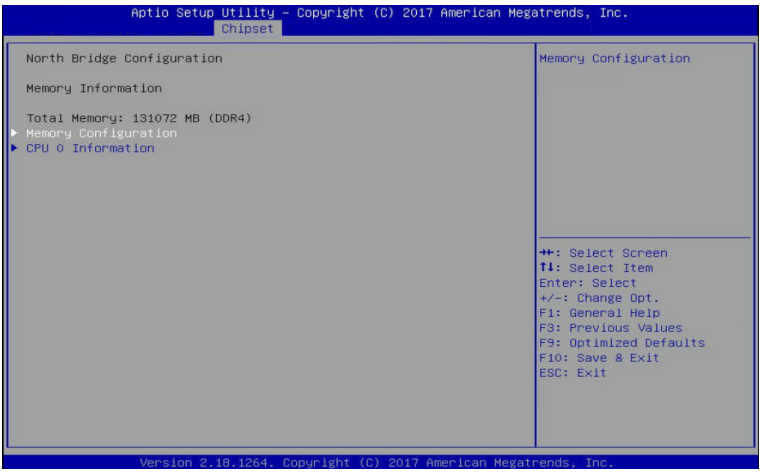
☞ North Bridge

Press [Enter] for configuration of advanced items.

☞ Error Management

Press [Enter] for configuration of advanced items.

5-4-1 North Bridge



☞ **North Bridge Configuration**

☞ **Memory Information**

☞ **Total Memory**

Displays the total memory information.

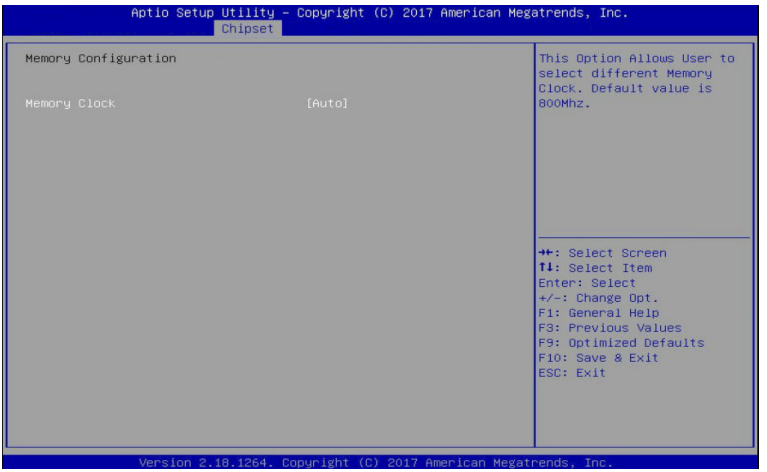
☞ **Memory Configuration**

Press [Enter] to configure the north bridge memory.

☞ **CPU 0 Information**

Press [Enter] to view information related to CPU 0.

5-4-1-1 Memory Configuration

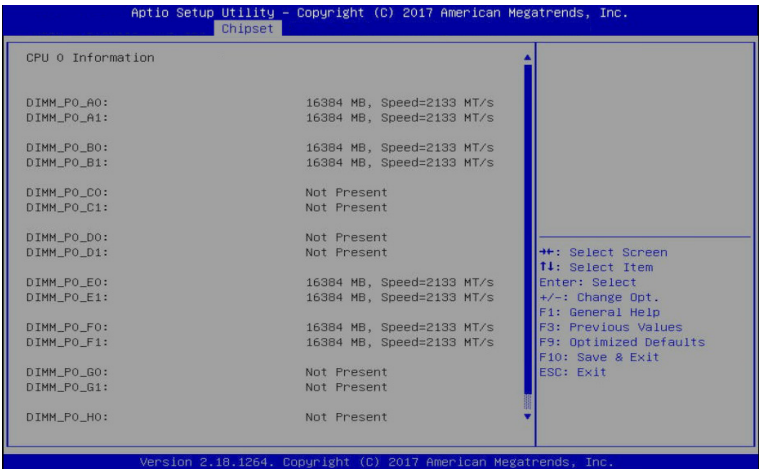


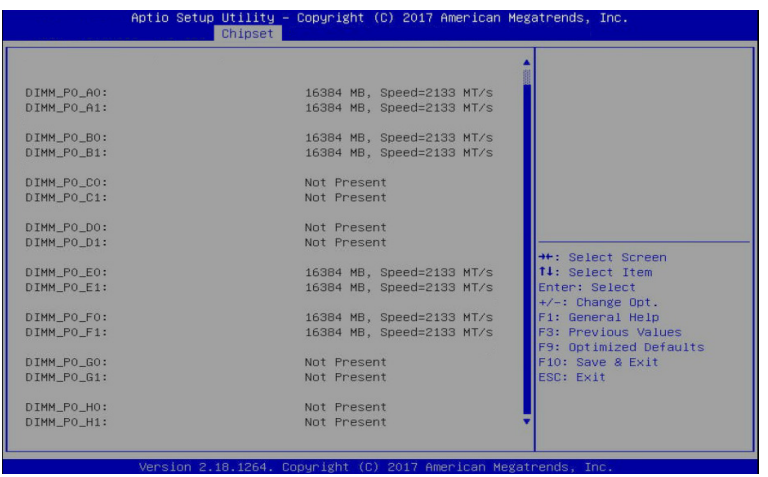
☞ **Memory Configuration**

☞ **Memory Clock**

This option allows user to select different memory clock. Default value is 800 Mhz.
Options available: Auto/1333MHz/1600MHz/1866MHz/2133MHz/2400MHz. Default setting is **Auto**.

5-4-1-2 CPU 0 Information





☞ **CPU 0 Information**

Displays the Information related to CPU 0.

5-4-2 Error Management



☞ **Error Management**

☞ **Platform First Error Handling**

Enable/Disable PFEH.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **MCA Error Threshold Count**

MCA Error Threshold Count. 0 - Disable Error.

Options available: 0/1/5/10/100/1000. Default setting is **10**.

☞ **DRAM Address/Command Parity With Replay**

☞ **RCD Parity**

Enable/disable Registering Clock Driver (RCD) Parity (RDimmParEn).

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **DRAM Address Command Parity Retry**

Enable/disable DRAM Address Command Parity Retry.

Options available: Enabled/Disabled. Default setting is **Disabled**.

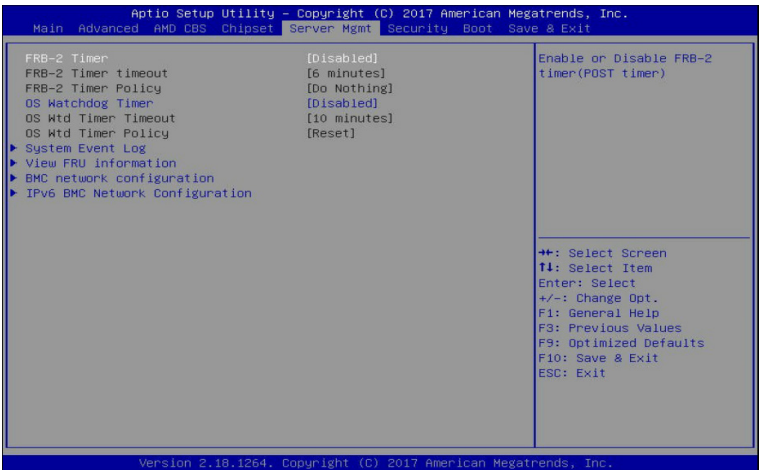
☞ **DRAM Write Data CRC with Retry**

☞ **Write CRC Enable**

If CRC is enabled, the memory is expecting CRC to be sent with the write data.

Options available: Enabled/Disabled. Default setting is **Disabled**.

5-5 Server Management Menu



☞ FRB-2 Timer (Note)

Enable/Disable FRB-2 timer (POST timer).

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ FRB-2 Timer timeout

Configure the FRB2 Timer timeout.

Options available: 3 minutes/4 minutes/5 minutes/6 minutes. Default setting is **6 minutes**.

Please note that this item is configurable when FRB-2 Timer is set to Enabled.

☞ FRB-2 Timer Policy

Configure the FRB2 Timer policy.

Options available: Do Nothing/Reset/Power Down. Default setting is **Do Nothing**.

Please note that this item is configurable when FRB-2 Timer is set to Enabled.

☞ OS Watchdog Timer (Note)

Enable/Disable OS Watchdog Timer function.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ OS Wtd Timer Timeout

Configure OS Watchdog Timer.

Options available: 5 minutes/10 minutes/15 minutes/20 minutes. Default setting is **10 minutes**.

Please note that this item is configurable when OS Watchdog Timer is set to Enabled.

☞ OS Wtd Timer Policy

Configure OS Watchdog Timer Policy.

Options available: Reset/Do Nothing/Power Down. Default setting is **Reset**.

Please note that this item is configurable when OS Watchdog Timer is set to Enabled.

(Note) Advanced items prompt when this item is set to **Enabled**.

☞ **System Event Log**

Press [Enter] for configuration of advanced items.

☞ **View FRU Information**

Press [Enter] to view the advanced items.

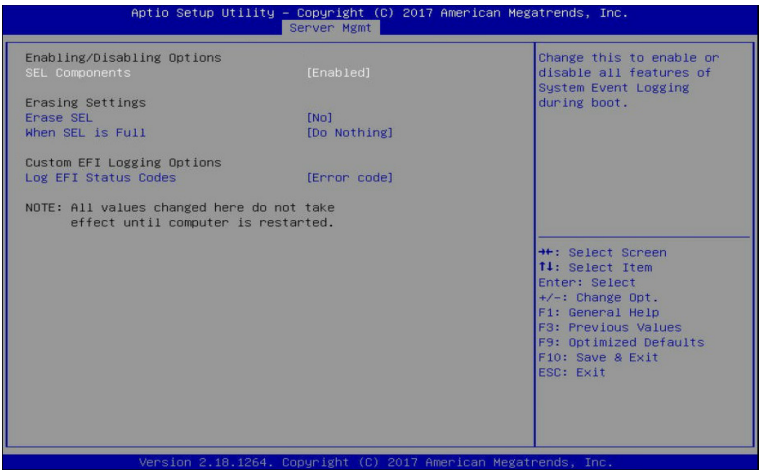
☞ **BMC network configuration**

Press [Enter] for configuration of advanced items.

☞ **IPv6 BMC Network Configuration**

Press [Enter] for configuration of advanced items.

5-5-1 System Event Log



☞ **Enabling/Disabling Options**

☞ **SEL Components**

Change this item to enable or disable all features of System Event Logging during boot.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **Erasing Settings**

☞ **Erasing SEL**

Choose options for erasing SEL.

Options available: No/Yes, On next reset/Yes, On every reset. Default setting is **No**.

☞ **When SEL is Full**

Choose options for reactions to a full SEL.

Options available: Do Nothing/Erase Immediately. Default setting is **Do Nothing**.

☞ **Custom EFI Logging Options**

☞ **Log EFI Status Codes**

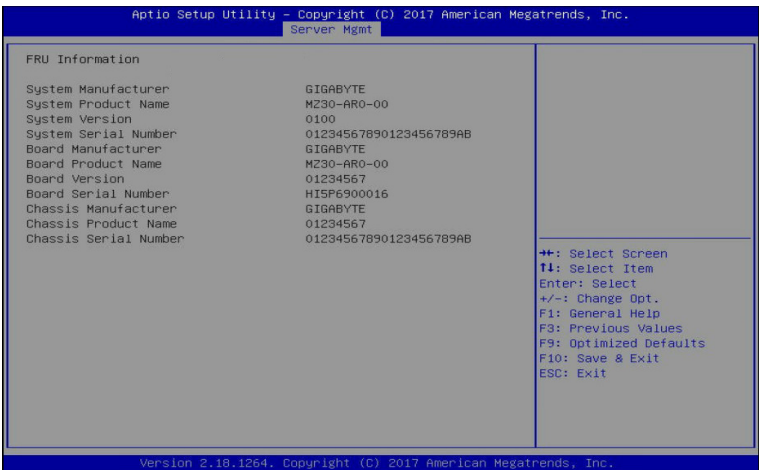
Enable/Disable the logging of EFI Status Codes (if not already converted to legacy).

Options available: Disabled/Both/Error code/Progress code. Default setting is **Error code**.

NOTE: All values changed here do not take effect until computer is restarted.

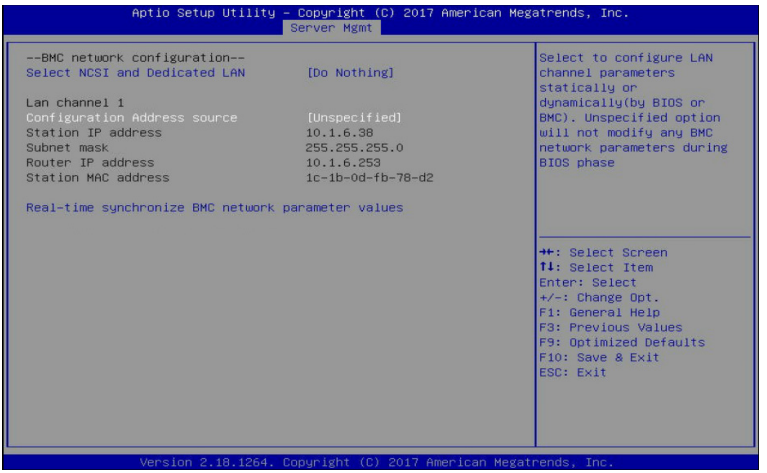
5-5-2 View FRU Information

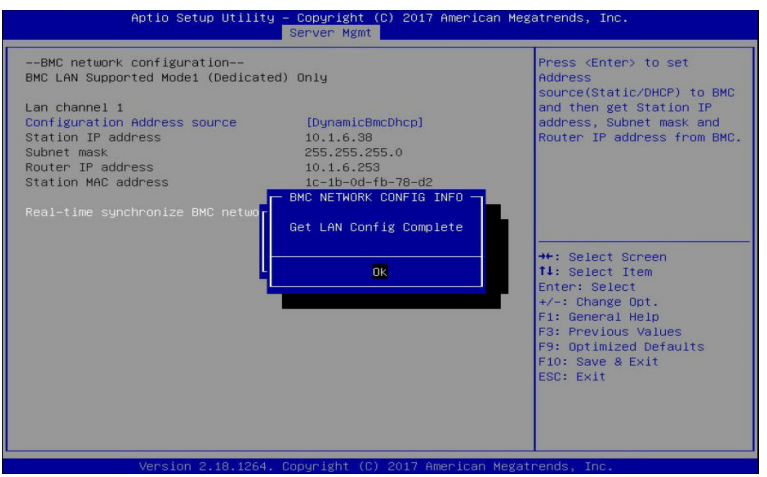
The FRU page is a simple display page for basic system ID information, as well as System product information. Items on this window are non-configurable.



(Note) The model name will vary depends on the product you purchased

5-5-3 BMC Network Configuration





☞ Select NCSI and Dedicated LAN

Selects to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Do nothing option will not modify any BMC network parameters during BIOS phase. If you select Mode1, Mode2, or Mode3 option, it will request you complete the network configurations.

Options available: Do Nothing/Mode1 (Dedicated)/Mode2(NSCI)/Mode3 (Failover).

Default setting is **Do Nothing**.

☞ **Lan Channel 1**

☞ **Configuration Address source**

Select to configure LAN channel parameters statically or dynamically (DHCP). Unspecified option will not modify any BMC network parameters during BIOS phase.

Options available: Unspecified/Static/DynamicBmcDhcp. Default setting is **Unspecified**.

☞ **Station IP address**

Displays IP Address information.

☞ **Subnet mask**

Displays Subnet Mask information.

Please note that the IP address must be in three digitals, for example, 192.168.000.001.

☞ **Router IP address**

Displays the Router IP Address information.

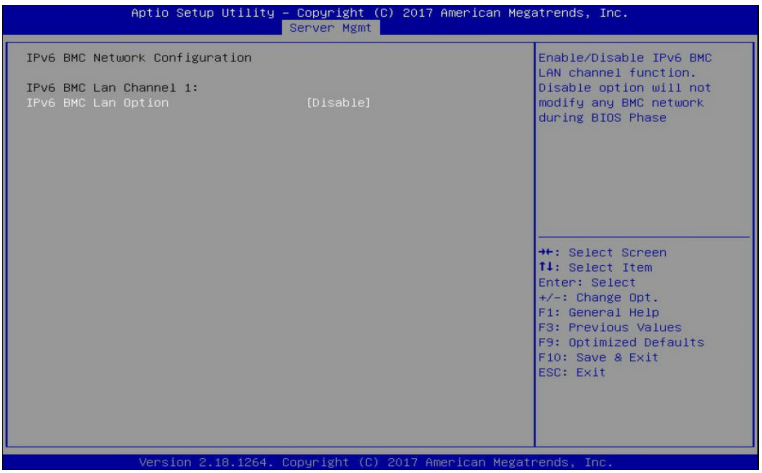
☞ **Station MAC address**

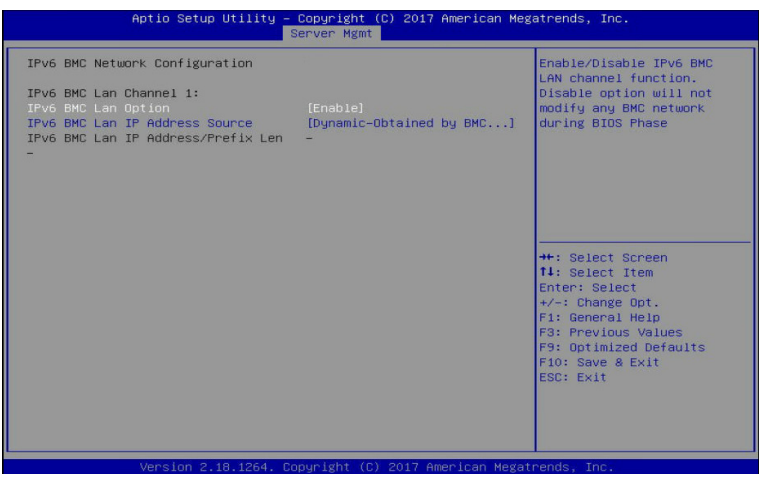
Displays the MAC Address information.

☞ **Real-time synchronize BMC network parameter values**

Press [Enter] to synchronize the BMC network parameter values.

5-5-4 IPv6 BMC Network Configuration





☞ **IPv6 BMC Lan Channel 1**

☞ **IPv6 BMC Lan Option**(Note)

Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase.

Options available: Enable/Disable. Default setting is **Disable**.

(Note) Advanced items prompt when this item is set to **Enable**.

☞ **IPv6 BMC Lan IP Address Source**

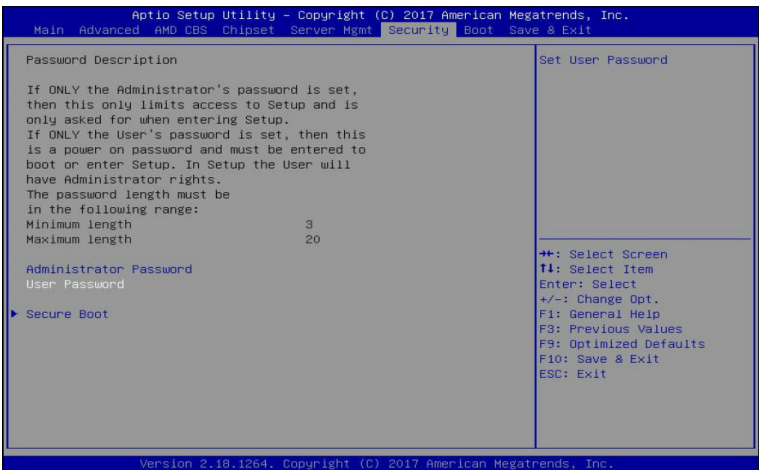
Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC).
Options available: Unspecified/Static/Dynamic-Obtained by BMC running DHCP.
Default setting is **Dynamic-Obtained by BMC running DHCP**.
Please note that this item is configurable when IPv6 BMC Lan Option is set to Enable.

☞ **IPv6 BMC Lan IP Address/Prefix Length**

Check if the IPv6 BMC LAN IP address matches those displayed on the screen.
Please note that this item is configurable when IPv6 BMC Lan Option is set to Enable.

5-6 Security Menu

The Security menu allows you to safeguard and protect the system from unauthorized use by setting up access passwords.



There are two types of passwords that you can set:

- Administrator Password

  Entering this password will allow the user to access and change all settings in the Setup Utility.

- User Password

  Entering this password will restrict a user's access to the Setup menus. To enable or disable this field, a Administrator Password must first be set. A user can only access and modify the System Time, System Date, and Set User Password fields.

☞ **Administrator Password**

Press [Enter] to configure the administrator password.

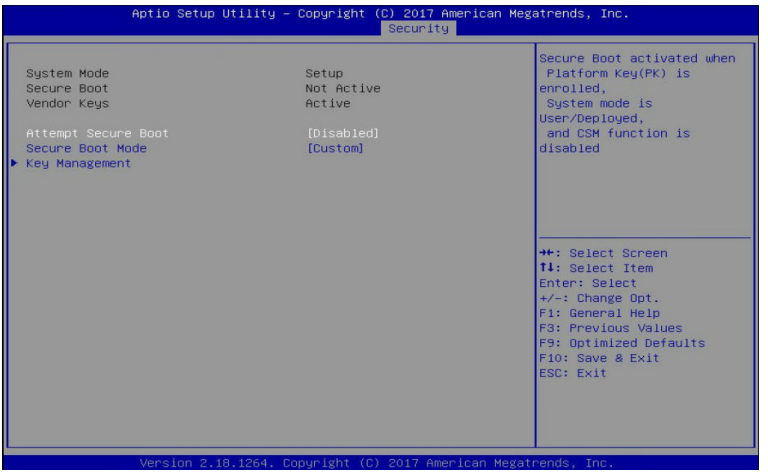
☞ **User Password**

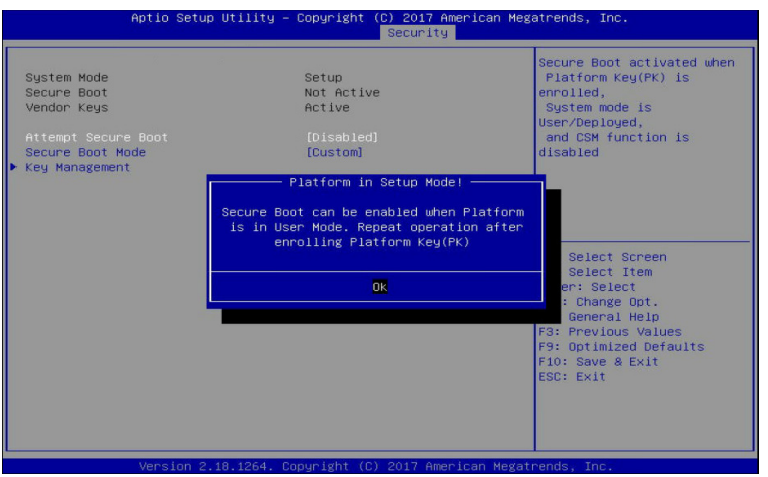
Press [Enter] to configure the user password.

☞ **Secure Boot**

Press [Enter] for configuration of advanced items.

5-6-1 Secure Boot





☞ **System Mode**

Displays the system is in User mode or Setup mode.

☞ **Secure Boot**

Displays the Secure Boot function is actived or not actived.

☞ **Vendor Keys**

Displays the Vendor Keys function is actived or not actived.

☞ **Attempt Secure Boot**

Secure Boot activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled.

When this option is set to **Enabled**, an "Platform in Setup Mode!" message will prompt to request re-enroll Platform Key (PK).

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ **Secure Boot Mode(Note)**

Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all the files being loaded before Windows loads and gets to the login screen have not been tampered with.

When set to Standard, it will automatically load the Secure Boot keys form the BIOS databases.

When set to Custom, you can customize the Secure Boot settings and manually load its keys from the BIOS database.

Options available: Standard/Custom. Default setting is **Custom**.

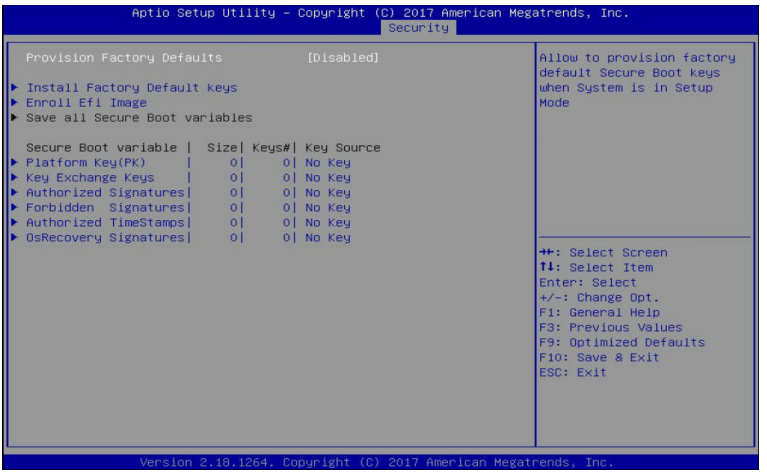
☞ **Key Management**

Press [Enter] for configuration of advanced items.

Please note that this item is configurable when Secure Boot Mode is set to Custom.

(Note) Advanced items prompt when this item is set to **Custom**.

5-6-1-1 Key Management



☞ Provision Factory Defaults

Allows to provision factory default Secure Boot keys when system is in Setup Mode.

Options available: Enabled/Disabled. Default setting is **Disabled**.

☞ Install Factory Default Keys

Installs all factory default keys. It will force the system in User Mode.

Options available: Yes/No.

☞ Enroll Efi Image

Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (DB).

☞ Save all Secure Boot variables

Press [Enter] to save all Secure Boot Keys and Key variables.

☞ Secure Boot variable

Displays the current status of the variables used for secure boot.

☞ Platform Key (PK)

Displays the current status of the Platform Key (PK).

Press [Enter] to configure a new PK.

Options available: Set New.

☞ Key Exchange Keys (KEK)

Displays the current status of the Key Exchange Key Database (KEK).

Press [Enter] to configure a new KEK or load additional KEK from storage devices.

Options available: Set New/Append.

☞ Authorized Signatures (DB)

Displays the current status of the Authorized Signature Database.

Press [Enter] to configure a new DB or load additional DB from storage devices.

Options available: Set New/Append.

☞ **Forbidden Signatures (DBX)**

Displays the current status of the Forbidden Signature Database.

Press [Enter] to configure a new dbx or load additional dbx from storage devices.

Options available: Set New/Append.

☞ **Authorized TimeStamps (DBT)**

Displays the current status of the Authorized TimeStamps Database.

Press [Enter] to configure a new DBT or load additional DBT from storage devices.

Options available: Set New/Append.

☞ **OsRecovery Signatures**

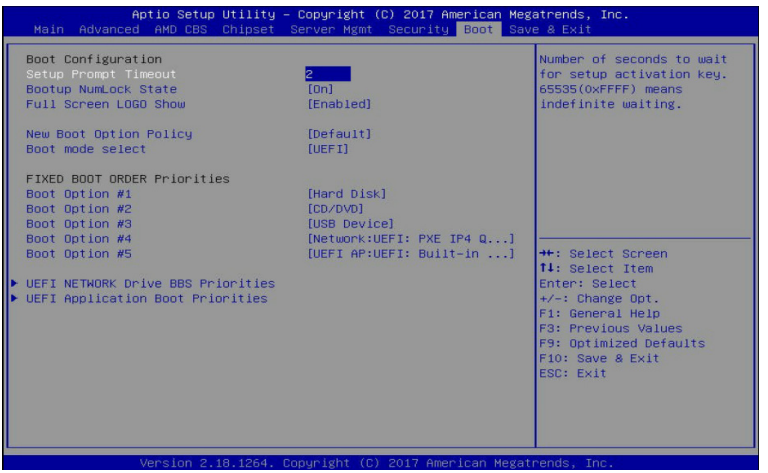
Displays the current status of the OsRecovery Signature Database.

Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.

Options available: Set New/Append.

5-7 Boot Menu

The Boot menu allows you to set the drive priority during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



☞ **Boot Configuration**

☞ **Setup Prompt Timeout**

Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.

☞ **Bootup NumLock State**

Enable/Disable the Bootup NumLock function.

Options available: On/Off. Default setting is **On**.

☞ **Full Screen LOGO Show**

Enable/Disable the Full Screen Logo Show option.

Options available: Enabled/Disabled. Default setting is **Enabled**.

☞ **New Boot Option Policy**

Controls the placement of newly detected UEFI boot options.

Options available: Default/Place First/Place Last. Default setting is **Default**.

☞ **Boot mode select**

Selects the boot mode.

Options available: LEGACY/UEFI. Default setting is **UEFI**.

☞ **FIXED BOOT ORDER Priorities**

☞ **Boot Option #1/#2/#3/#4/#5**

Press [Enter] to configure the boot priority.

By default, the server searches for boot devices in the following secquence:

1. Hard disk drive.
2. CD-COM/DVD drive.
3. USB device.
4. Network device.
5. UEFI device.

☞ **UEFI Network Drive BBS Priorities**

Press [Enter] to configure the boot priority.

☞ **UEFI Application Boot Priorities**

Press [Enter] to configure the boot priority.

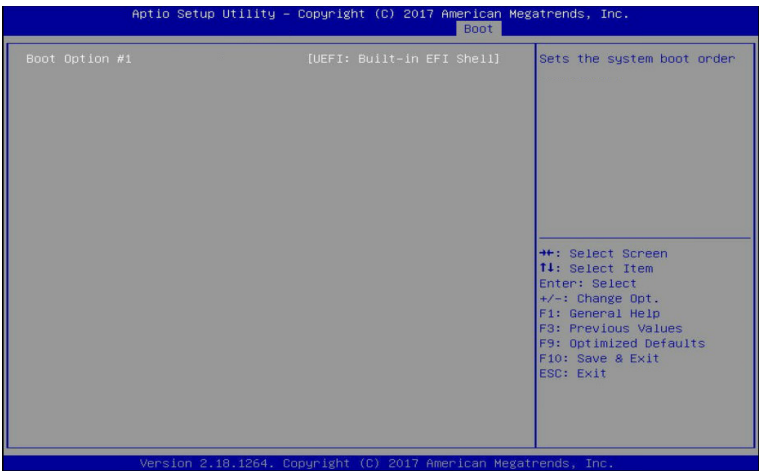
5-7-1 UEFI NETWORK Drive BBS Priorities

The UEFI network drive BBS priorities submenu allows you to specify the boot device priority from the available UEFI network drives during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



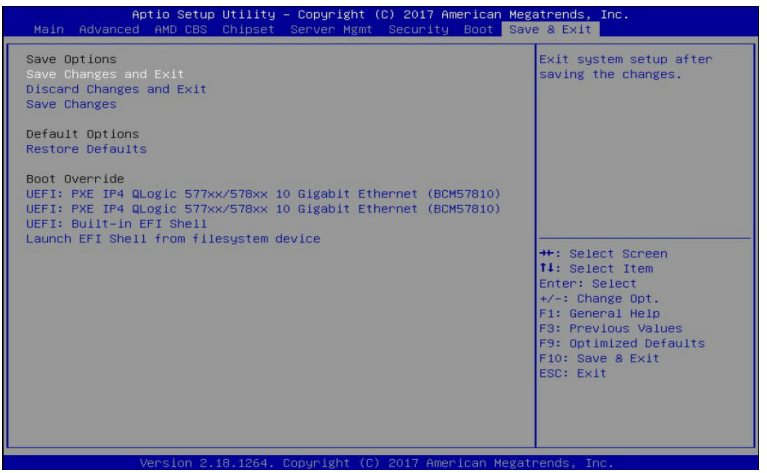
5-7-2 UEFI Application Boot Priorities

The UEFI application boot priorities submenu allows you to specify the boot device priority from the available UEFI applications during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



5-8 Save & Exit Menu

The Exit menu displays the various options to quit from the BIOS setup. Highlight any of the exit options then press **Enter**.



☞ **Save Options**

☞ **Save Changes and Exit**

Saves changes made and closes the BIOS setup.

Options available: Yes/No.

☞ **Discard Changes and Exit**

Discards changes made and exits the BIOS setup.

Options available: Yes/No.

☞ **Save Changes**

Saves changes made in the BIOS setup.

Options available: Yes/No.

☞ **Default Options**

☞ **Restore Defaults**

Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly.

Options available: Yes/No.

☞ **Boot Override**

Press [Enter] to configure the device as the boot-up drive.

5-9 ABL POST Codes

5-9-1 StartProcessorTestPoints

Entry used for range testing for @b Processor related TPs	0xE000

5-9-2 Memory test points

Memory structure initialization (Public interface)	0xE001
SPD Data processing (Public interface)	0xE002
Memory configuration (Public interface) Phase 1	0xE003
DRAM initialization	0xE004
ProcMemSPDChecking	0xE005
ProcMemModeChecking	0xE006
Speed and TCL configuration	0xE007
ProcMemSpdTiming	0xE008
ProcMemDramMapping	0xE009
ProcMemPlatformSpecificConfig	0xE00A
ProcMemPhyCompensation	0xE00B
ProcMemStartDcts	0xE00C
ProcMemBeforeDramInit (Public interface)	0xE00D
ProcMemPhyFenceTraining	0xE00E
ProcMemSynchronizeDcts	0xE00F
ProcMemSystemMemoryMapping	0xE010
ProcMemMtrrConfiguration	0xE011
ProcMemDramTraining	0xE012
ProcMemBeforeAnyTraining(Public interface)	0xE013

5-9-3 PMU Test Points

ABL Mem - PMU - Before PMU Firmware load	0xE014
ABL Mem - PMU - After PMU Firmware load	0xE015
ABL Mem - PMU Populate SRAM Timing	0xE016
ABL Mem - PMU Populate SRAM Config	0xE017
ABL Mem - PMU Write SRAM Msg Block	0xE018
ABL Mem - Wait for Phy Cal Complete	0xE019
ABL Mem - Phy Cal Complete	0xE01A
ABL Mem - PMU Start	0xE01B
ABL Mem - PMU Started	0xE01C
ABL Mem - PMU Waiting for Complete	0xE01D
ABL Mem - PMU Stage Dec Init	0xE01E
ABL Mem - PMU Stage Training Wr Lvl	0xE01F
ABL Mem - PMU Stage Training Rx En	0xE020
ABL Mem - PMU Stage Training Rd Dqs	0xE021
ABL Mem - PMU Stage Traning Rd 2D	0xE022

ABL Mem - PMU Stage Training Wr 2D	0xE023
ABL Mem - PMU Queue Empty	0xE024
ABL Mem - PMU US message Start	0xE025
ABL Mem - PMU US message End	0xE026
ABL Mem - PMU Complete	0xE027
ABL Mem - PMU - After PMU Training	0xE028
ABL Mem - PMU - Before Disable PMU	0xE029

5-9-4 Original Post Code

ProcMemTransmitDqsTraining	0xE02A
ABL Mem - Start write sweep	0xE02B
ABL Mem - Set Transmit DQ delay	0xE02C
ABL Mem - Write test pattern	0xE02D
ABL Mem - Read Test pattern	0xE02E
ABL Mem - Compare Test pattern	0xE02F
ABL Mem - Update results	0xE030
ABL Mem - Start Find passing window	0xE031
ABL Mem - ProcMemMaxRdLatencyTraining	0xE032
ABL Mem - Start sweep	0xE033
ABL Mem - Set delay	0xE034
ABL Mem - Write test pattern	0xE035
ABL Mem - Read Test pattern	0xE036
ABL Mem - Compare Test pattern	0xE037
ABL Mem - Online Spare init	0xE038
ABL Mem - Chip select Interleave Init	0xE039
ABL Mem - Node Interleave Init	0xE03A
ABL Mem - Channel Interleave Init	0xE03B
ABL Mem - ECC initialization	0xE03C
ABL Mem - Platform Specific Init	0xE03D
ABL Mem - Before callout for "AgesaReadSpd"	0xE03E
ABL Mem - After callout for "AgesaReadSpd"	0xE03F
ABL Mem - Before optional callout "AgesaHookBeforeDramInit"	0xE040
ABL Mem - After optional callout "AgesaHookBeforeDramInit"	0xE041
ABL Mem - Before optional callout "AgesaHookBeforeDQSTraining"	0xE042
ABL Mem - After optional callout "AgesaHookBeforeDQSTraining"	0xE043
ABL Mem - Before optional callout "AgesaHookBeforeDramInit"	0xE044
ABL Mem - After optional callout "AgesaHookBeforeDramInit"	0xE045
ABL Mem - After MemDataInit	0xE046
ABL Mem - Before InitializeMCT	0xE047
ABL Mem - Before LV DDR3	0xE048
ABL Mem - Before InitMCT	0xE049

ABL Mem - Before OtherTiming	0xE04A
ABL Mem - Before UMAMemTyping	0xE04B
ABL Mem - Before SetDqsEccTmgs	0xE04C
ABL Mem - Before MemClr	0xE04D
ABL Mem - Before On DIMM Thermal	0xE04E
ABL Mem - Before DMI	0xE04F
ABL MEM - End of phase 3 memory code	0xE050

5-9-5 CPU test points

Entry point CPU init after training	0xE051
Exit point CPU init after training	0xE052
Entry point CPU APOB CCX map init	0xE053
Exit point CPU APOB CCX map init	0xE054
Entry point CPU Optimized boot init	0xE055
Exit point CPU Optimized boot init	0xE056
Entry point CPU APOB EDC info init	0xE057
Exit point CPU APOB EDC info init	0xE058

5-9-6 Topology test points

ProcTopologyEntry	0xE071
ProcTopologyDone	0xE07C

5-9-7 Extended memory test point

ProcMemSendMRS2	0xE080
Sedding MRS3	0xE081
Sending MRS1	0xE082
Sending MRS0	0xE083
Continuous Pattern Read	0xE084
Continuous Pattern Write	0xE085
Mem: 2d RdDqs Training begin	0xE086
Mem: Before optional callout to platform BIOS to change External Vref during 2d Training	0xE087
Mem: After optional callout to platform BIOS to change External Vref during 2d Training	0xE088
Configure DCT For General use begin	0xE089
Configure DCT For training begin	0xE08A
Configure DCT For Non-Explicit	0xE08B
Configure to Sync channels	0xE08C
Allocate C6 Storage	0xE08D
Before LV DDR4	0xE08E
Before LV DDR3	0xE08F

5-9-8 Gnb Earlier init

TP0x90	0xE090
GNB earlier interface	0xE091
GNB internal debug code	0xE092
GNB internal debug code	0xE093
GNB internal debug code	0xE094
GNB internal debug code	0xE095
GNB internal debug code	0xE096
GNB internal debug code	0xE097
GNB internal debug code	0xE098
GNB internal debug code	0xE099
GNB internal debug code	0xE09A
GNB internal debug code	0xE09B
GNB internal debug code	0xE09C
GNB internal debug code	0xE09D
GNB internal debug code	0xE09E
GNB internal debug code	0xE09F
TP0xA0	0xE0A0
GNB internal debug code	0xE0A1
GNB internal debug code	0xE0A2
GNB internal debug code	0xE0A3
GNB internal debug code	0xE0A4
GNB internal debug code	0xE0A5
GNB internal debug code	0xE0A6
GNB internal debug code	0xE0A7
GNB internal debug code	0xE0A8
GNB internal debug code	0xE0A9
GNB internal debug code	0xE0AA
GNB internal debug code	0xE0AB
GNB internal debug code	0xE0AC
GNB internal debug code	0xE0AD
GNB internal debug code	0xE0AE
GNB internal debug code	0xE0AF
Abl1Begin	0xE0B0
ABL 1 Initialization	0xE0B1
ABL 1 DF Early	0xE0B2
ABL 1 DF Pre Training	0xE0B3
ABL 1 Debug Synchronization	0xE0B4
ABL 1 Error Detected	0xE0B5
ABL 1 Global memory error detected	0xE0B6
ABL 1 End	0xE0B7

ABL 2 Begin	0xE0B8
ABL 2 Initialization	0xE0B9
ABL 2 After Training	0xE0BA
ABL 2 Debug Synchronization	0xE0BB
ABL 2 Error detected	0xE0BC
ABL 2 Global memory error detected	0xE0BD
ABL 2 End	0xE0BE
ABL 3 Begin	0xE0BF
ABL 3 Initialziation	0xE0C0
ABL 3 GMI/xGMI Initialization Stage 1	0xB1C0
ABL 3 GMI/xGMI Initialization Stage 1 Warning	0xF1C0
ABL 3 GMI/xGMI Initialization Stage 2 Error	0xE2C0
ABL 3 GMI/xGMI Initialization Stage 2	0xB2C0
ABL 3 GMI/xGMI Initialization Stage 2 Warning	0xF2C0
ABL 3 GMI/xGMI Initialization Stage 2 Error	0xE3C0
ABL 3 GMI/xGMI Initialization Stage 3	0xB3C0
ABL 3 GMI/xGMI Initialization Stage 3 Warning	0xF3C0
ABL 3 GMI/xGMI Initialization Stage 3 Error	0xE4C0
ABL 3 GMI/xGMI Initialization Stage 4	0xB4C0
ABL 3 GMI/xGMI Initialization Stage 4 Warning	0xF4C0
ABL 3 GMI/xGMI Initialization Stage 4 Error	0xE5C0
ABL 3 GMI/xGMI Initialization Stage 5	0xB5C0
ABL 3 GMI/xGMI Initialization Stage 5 Warning	0xF5C0
ABL 3 GMI/xGMI Initialization Stage 5 Error	0xE6C0
ABL 3 GMI/xGMI Initialization Stage 6	0xB6C0
ABL 3 GMI/xGMI Initialization Stage 6 Warning	0xF6C0
ABL 3 GMI/xGMI Initialization Stage 6 Error	0xE7C0
ABL 3 GMI/xGMI Initialization Stage 7	0xE8C0
ABL 3 GMI/xGMI Initialization Stage 8	0xE9C0
ABL 3 GMI/xGMI Initialization Stage 9	0xF9C0
ABL 3 GMI/xGMI Initialization Stage 9 Error	0xEAC0
ABL 3 GMI/xGMI Initialization Stage 10	0xFAC0
ABL 3 GMI/xGMI Initialization Stage 10 Error	0xE0C1
Abl3ProgramUmcKeys	0xE0C2
ABL 3 DF Finial Initalization	0xE0C3
ABL 3 Execute Synchronization Function	0xE0C4
ABL 3 Debug Synchronization Function	0xE0C5
ABL 3 Error Detected	0xE0C6
ABL 3 Global memroy error detected	0xE0C7
ABL 4 Initialiation - cold boot	0xE0C8
ABL 4 Memory test - cold boot	0xE0C9

ABL 4 APOB Initialzation - cold boot	0xE0CA
ABL 4 Finalize memory settings - cold boot	0xE0CB
ABL 4 CPU Initialize Optimized Boot - cold boot	0xE0CC
ABL 4 Gmi Pcie Training - cold boot	0xE0CD
ABL 4 Cold boot End	0xE0CE
ABL 4 Initialization - Resume boot	0xE0CF
ABL 4 Resume End	0xE0D0
ABL 4 End Cold/Resume boot	0xE0D1
ABL 2 memory initialization	0xE0D2
ABL 3 memory initialization	0xE0D3
ABL 3 End	0xE0D4
ABL 1 Enter Memory Flow	0xE0D5
Memorry flow memory clock synchronization	0xE0D6
IfAmdReadEventLogEntry	0xE0D7
Exiting from AmdReadEventLog	0xE0D8
Entry to AmdGetApicId	0xE0D9
Exiting from AmdGetApicId	0xE0DA
Entry to AmdGetPciAddress	0xE0DB
Exiting from AmdGetPciAddress	0xE0DC
Entry to AmdIdentifyCore	0xE0DD
TExiting from AmdIdentifyCore	0xE0DE
After IDS calls out to run code on an AP	0xE0DF
After IDS calls out to run code on an AP	0xE0E0
Before IDS calls out to get IDS data	0xE0E1
After IDS calls out to get IDS data	0xE0E2
Before the heap manager calls out to allocate a buffer	0xE0E3
After the heap manager calls out to allocate a buffer	0xE0E4
Before the heap manager calls out to deallocate a buffer	0xE0E5
After the heap manager calls out to deallocate a buffer	0xE0E6
Before the heap manager calls out to locate a buffer	0xE0E7
After the heap manager calls out to locate a buffer	0xE0E8
Memory flow P-State synchronization	0xE0E9
After the BSP calls out to run code on an AP	0xE0EA
Before the BSP calls out to run code on an AP	0xE0EB
After the BSP calls out to run code on an AP	0xE0EC
Before the S3 save code calls out to allocate a buffer	0xE0ED
After the S3 save code calls out to allocate a buffer	0xE0EE
Before the memory S3 save code calls out to allocate a buffer	0xE0EF
After the memory S3 save code calls out to allocate a buffer	0xE0F0
Before the memory code calls out to locate a buffer	0xE0F1
After the memory code calls out to locate a buffer	0xE0F2

Before the memory code calls out to locate a buffer	0xE0F3
After the memory code calls out to locate a buffer	0xE0F4
Before the memory code calls out to locate a buffer	0xE0F5
After the memory code calls out to locate a buffer	0xE0F6
Before the memory code calls out to locate a buffer	0xE0F7
After the memory code calls out to locate a buffer	0xE0F8
Ready to boot event	

5-9-9 PMU test points

Failed PMU training	0xE0F9
End of phase 1 memory code	0xE0FA
End of phase 2 memory code	0xE0FB

5-9-10 ABL0 test points

Abl0Begin	0xE0FC
ABL 0 End	0xE0FD

5-9-11 ABL5 test points

ABL 5 End	0xE100
sume boot	0xE101
ABL 6 End	0xE102
ABL 6 Initialization	0xE103
End of phase 1b memory code	0xE104
ABL 1b memory initialization	0xE105
ABL 6 Global memroy error detected	0xE106
ABL 1b Debug Synchronization Function	0xE107
ABL 4b Debug Synchronization Function	0xE108
AblbBegin	0xE109
Ab4bBegin	0xE10A
BSP encountered HMAC fail on APOB Header	0xE10B
ABL Eroor General ASSERT	0xE2A0
Unknown Error	0xE2A1
ABL Error Log Inig Error	0xE2A2
ABL Error for On DIMM thermal Heap allocation error	0xE2A3
ABL Error for memory test error	0xE2A4
ABL Error while executing memory test error	0xE2A5
ABL Error DDR Post Packge Repair Mem Auto Heap Alloc error	0xE2A6
ABL Error for DDR Post Package repair Apob Heap Alloc error	0xE2A7
ABL Error for DDR Post Package Repair No PPR Table Heap Aloc error	0xE2A8
ABL Error for Ecc Mem Auto Aloc Error error	0xE2A9
ABL Error for Soc Scan Heap Aloc error	0xE2AB

ABL Error for Soc Scan No Die error	0xE2AC
ABL Error for Nb Tech Heap Aloc error	0xE2AD
ABL Error for No Nb Constructor error	0xE2AE
ABL Error for No Tech Constructor error	0xE2AE
ABL Error for ABL1b Auto Alocation error	0xE2B0
ABL Error for ABL1b No NB Constructor error	0xE2B1
ABL Error for ABL2 No Nb Constructor error	0xE2B2
ABL Error for ABL3 Auto Allocation error	0xE2B3
ABL Error for ABL3 No Nb Constructor error	0xE2B4
ABL Error for ABL1b General error	0xE2B5
ABL Error for ABL2 General error	0xE2B6
ABL Error for ABL3 General error	0xE2B7
ABL Error for Get Target Speed error	0xE2B8
ABL Error for Flow P1 Family Support error	0xE2B9
ABL Error for No Valid Ddr4 Dimms error	0xE2BA
ABL Error for No Dimm Present error	0xE2BB
ABL Error for Flow P2 Family Supprot error	0xE2BC
ABL Error for Heap Deallocation for PMU Sram Msg Block error	0xE2BD
ABL Error for DDR Recovery error	0xE2BE
ABL Error for RRW Test error	0xE2BF
ABL Error for On Die Thermal error	0xE2C1
ABL Error for Heap Allocation For Dct Struct Amd Ch Def structure error	0xE2C2
ABL Error for Heap Allocation for PMU SRAM Msg block error	0xE2C3
ABL Error for Heap Phy PLL lock Flure error	0xE2C4
ABL Error for Pmu Training error	0xE2C5
ABL Error for Failure to Load or Verify PMU FW error	0xE2C6
ABL Error for Allocate for PMU SRAM Msg Block No Init error	0xE2C7
ABL Error for Failure BIOS PMU FW Mismatch AGESA PMU FW version error	0xE2C8
ABL Error for Deallocate for PMU SRAM Msg Block error	0xE2CA
ABL Error for Module Type Mismatch RDIMM error	0xE2CB
ABL Error for Module type Mismatch LRDIMM error	0xE2CC
ABL Error for MEm Auto NVDIM error	0xE2CD
ABL Error for Unknowm Responce error	0xE2CE
ABL Error for Over Clock Error RRW Test Results Error	0xE2CF
ABL Error for Over Clock Error PMU Training Error	0xE2D0
ABL Error for ABL1 General Error	0xE2D1
ABL Error for ABL2 General Error	0xE2D2
ABL Error for ABL3 General Error	0xE2D3
ABL Error for ABL4 General Error	0xE2D4

ABL Error over clock Mem Init Error	0xE2D5
ABL Error over clock Mem Other Error	0xE2D6
ABL Error for ABL6 General Error	0xE2D7
ABL Error Event Log Error	0xE2D8
ABL Error FATAL ABL1 Log Error	0xE2D9
ABL Error FATAL ABL2 Log Error	0xE2DA
ABL Error FATAL ABL3 Log Error	0xE2DB
ABL Error FATAL ABL4 Log Error	0xE2DC
ABL Error Slave Sync function execution Error	0xE2DD
ABL Error Slave Sync communicaton with data set to master Error	0xE2DE
ABL Error Slave broadcast communication from master to slave Error	0xE2DF
ABL Error FATAL ABL6 Log Error	0xE2E0
ABL Error Slave Offline Error	0xE2E1
ABL Error Slave Informs Master Error Info Error	0xE2E2
ABL Error Error Heap Locate for PMU SRAM Msg Block Error	0xE2E3
ABL Error ABL2 Auto Error	0xE2E4
ABL Error Flow P3 Family support Error	0xE2E5
ABL Error Abl 4 Gen Error	0xE2EB
ABL Error MBIST Heap Allocation Error	0xE2EC
ABL Error MBIST Results Error	0xE2EE
ABL Error NO Dimm Smcus Info Error	0xE2EE
ABL Error Por Max Freq Table Error	0xE2EF
ABL Error Unsupproted DIMM Config Error	0xE2F0
ABL Error No Ps Table Error	0xE2F1
ABL Error Cad Bus Timing Not Found Error	0xE2F2
ABL Error Data Bus Timing Not Found Error	0xE2F3
ABL Error LrDIMM IBT Not Found Error	0xE2F4
ABL Error Unsupprote Dimm Config Max Freq Error Error	0xE2F5
ABL Error Mr0 Not Found Error	0xE2F6
ABL Error Obt Pattern Not found Error	0xE2F7
ABL Error Rc10 Op Speed Not FOund Error	0xE2F8
ABL Error Rc2 Ibt Not Found Error	0xE2F9
ABL Error Rtt Not Found Error	0xE2FA
ABL Error Checksum ReStrt Results Error	0xE2FB
ABL Error No Chipselect Results Error	0xE2FC
ABL Error No Common Cas Latency Results Error	0xE2FD
ABL Error Cas Latecncy exceeds Taa Max Error	0xE2FE
ABL Error Nvdimm Arm Missmatch Power Policy Error	0xE2FF
ABL Error Nvdimm Arm Missmatch Power Source Error	0xE300
ABL Error ABL 1 Mem Init Error	0xE301

ABL Error ABL 2 Mem Init Error	0xE302
ABL Error ABL 4 Mem Init Error	0xE303
ABL Error ABL 6 Mem Init Error	0xE304
ABL Error ABL 1 error repor Error	0xE305
ABL Error ABL 2 error repor Error	0xE306
ABL Error ABL 3 error repor Error	0xE307
ABL Error ABL 4 error repor Error	0xE308
ABL Error ABL 6 error repor Error	0xE30A
ABL Error message slave sync function execution Error	0xE30B
ABL Error slave offline Error	0xE30C
ABL Error Sync Master Error	0xE30D
ABL Error Slave Informs Master Info Message Error	0xE30E
ABL Error General Assert Error	0xE30F
ABL Error No Dimms On Any Channel in sysem	0xE310
ABL Alert PMU Major Message captured	0xE311
ABL Alert PMU REsults Rx Timing captured	0xE312
ABL Alert PMU REsults Tx Timing captured	0xE313
ABL Alert PMU REsults Rx Vref captured	0xE314
ABL Alert PMU REsults Tx Vref captured	0xE315
EndAgesas	0xEFFF

5-10 Agesa POST Codes

5-10-1 Universal Post Code

Universal ACPI entry	0xA001
Universal ACPI exit	0xA002
Universal ACPI abort	0xA003
Universal SMBIOS entry	0xA004
Universal SMBIOS exit	0xA005
Universal SMBIOS abort	0xA006

5-10-2 [0xA1XX] For CZ only memory Postcodes

Memory structure initialization (Public interface)	0xA101
SPD Data processing (Public interface)	0xA102
Memory configuration (Public interface)	0xA103
DRAM initialization	0xA104
TpProcMemSPDChecking	0xA105
TpProcMemModeChecking	0xA106
Speed and TCL configuration	0xA107
TpProcMemSpdTiming	0xA108
TpProcMemDramMapping	0xA109
TpProcMemPlatformSpecificConfig	0xA10A
TPProcMemPhyCompensation	0xA10B
TpProcMemStartDcts	0xA10C
(Public interface)	0xA10D
TpProcMemPhyFenceTraining	0xA10E
TpProcMemSynchronizeDcts	0xA10F
TpProcMemSystemMemoryMapping	0xA110
TpProcMemMtrrConfiguration	0xA111
TpProcMemDramTraining	0xA112
(Public interface)	0xA113
TpProcMemWriteLevelizationTraining	0xA114
Below 800Mhz first pass start	0xA115
Above 800Mhz second pass start	0xA116
Target DIMM configured	0xA117
Prepare DIMMS for WL	0xA118
Configure DIMMS for WL	0xA119
TpProcMemReceiverEnableTraining	0xA11A
Start sweep loop	0xA11B
Set receiver Delay	0xA11C
Write test pattern	0xA11D
Read test pattern	0xA11E
Compare test pattern	0xA11F

Calculate MaxRdLatency per channel	0xA120
TpProcMemReceiveDqsTraining	0xA121
Set Write Data delay	0xA122
Write test pattern	0xA123
Start read sweep	0xA124
Set Receive DQS delay	0xA125
Read Test pattern	0xA126
Compare Test pattern	0xA127
Update results	0xA128
Start Find passing window	0xA129
TpProcMemTransmitDqsTraining	0xA12A
Start write sweep	0xA12B
Set Transmit DQ delay	0xA12C
Write test pattern	0xA12D
Read Test pattern	0xA12E
Compare Test pattern	0xA12F
Update results	0xA130
Start Find passing window	0xA131
TpProcMemMaxRdLatencyTraining	0xA132
Start sweep	0xA133
Set delay	0xA134
Write test pattern	0xA135
Read Test pattern	0xA136
Compare Test pattern	0xA137
Online Spare init	0xA138
Bank Interleave Init	0xA139
Node Interleave Init	0xA13A
Channel Interleave Init	0xA13B
ECC initialization	0xA13C
Platform Specific Init	0xA13D
Before callout for "AgesaReadSpd"	0xA13E
After callout for "AgesaReadSpd"	0xA13F
Before optional callout "AgesaHookBeforeDramInit"	0xA140
After optional callout "AgesaHookBeforeDramInit"	0xA141
Before optional callout "AgesaHookBeforeDQSTraining"	0xA142
After optional callout "AgesaHookBeforeDQSTraining"	0xA143
Before optional callout "AgesaHookBeforeDramInit"	0xA144
After optional callout "AgesaHookBeforeDramInit"	0xA145
After MemDataInit	0xA146
Before InitializeMCT	0xA147
Before LV DDR3	0xA148

Before InitMCT	0xA149
Before OtherTiming	0xA14A
Before UMAMemTyping	0xA14B
Before SetDqsEccTmgs	0xA14C
Before MemClr	0xA14D
Before On DIMM Thermal	0xA14E
Before DMI	0xA14F
End of memory code	0xA150
Entry point S3Init	0xA151
Sending MRS2	0xA180
Sedding MRS3	0xA181
Sending MRS1	0xA182
Sending MRS0	0xA183
Continuous Pattern Read	0xA184
Continuous Pattern Write	0xA185
Mem: 2d RdDqs Training begin	0xA186
Mem: Before optional callout to platform BIOS to change External Vref during 2d Training	0xA187
Mem: After optional callout to platform BIOS to change External Vref during 2d Training	0xA188
Configure DCT For General use begin	0xA189
Configure DCT For training begin	0xA18A
Configure DCT For Non-Explicit	0xA18B
Configure to Sync channels	0xA18C
Allocate C6 Storage	0xA18D
Before LV DDR4	0xA18E
// BR CPU	
BR before AP launch	0xA190
Install AP launched PPI	0xA191
BR after AP launch	0xA192
Before CPU PM	0xA193
Enable IO Cstate	0xA194
Enable C6	0xA195
Install CCX PEI complete PPI	0xA196
BR CPU memory done call back entry	0xA197
Before APM weights	0xA198
After APM weights	0xA199
BR CPU memory done call back end	0xA19A
BR Init Mid entry	0xA19B
BR enable APM	0xA19C
BR Init Mid install protocol	0xA19D

BR Init Mid end	0xA19E
BR Init Late entry	0xA19F
BR Init Late install protocol	0xA1A0
BR Init Late end	0xA1A1
BR DXE install complete protocol	0xA1A2
UNB install complete PPI	0xA1A3
UNB AfterApLaunch callback entry	0xA1A4
UNB AfterApLaunch callback end	0xA1A5

5-10-3 S3 Interface Post Code

Before the S3 save code calls out to allocate a buffer	0xA1EC
After the S3 save code calls out to allocate a buffer	0xA1ED
Before the memory S3 save code calls out to allocate a buffer	0xA1EE
After the memory S3 save code calls out to allocate a buffer	0xA1EF
Before the memory code calls out to locate a buffer	0xA1F0
After the memory code calls out to locate a buffer	0xA1F1
Before the memory code calls out to locate a buffer	0xA1F2
After the memory code calls out to locate a buffer	0xA1F3
Before the memory code calls out to locate a buffer	0xA1F4
After the memory code calls out to locate a buffer	0xA1F5
Before the memory code calls out to locate a buffer	0xA1F6
After the memory code calls out to locate a buffer	0xA1F7

5-10-4 PMU Post Code

Failed PMU training	0xA1F9

5-10-5 [0xA5XX] assigned for AGESA PSP Module

// PSP V1 Modules	
PspPeiV1 entry	0xA501
PspPeiV1 exit	0xA502
MemoryDiscoveredPpiCallback entry	0xA503
MemoryDiscoveredPpiCallback exit	0xA504
PspDxeV1 entry	0xA507
PspDxeV1 exit	0xA508
PspDxeV1 PspPciEnumerationCompleteCallBack entry	0xA50A
PspDxeV1 PspPciEnumerationCompleteCallBack exit	0xA50B
PspDxeV1 ready to boot entry	0xA50C
PspDxeV1 ready to boot exit	0xA50D
PspSmmV1 entry	0xA50E
PspSmmV1 exit	0xA50F
PspSmmV1 SwSmiCallBack entry, build the S3 save area for resume	0xA510

PspSmmV1 SwSmiCallBack exit, build the S3 save area for resume	0xA511
PspSmmV1 BspSmmResumeVector entry	0xA512
PspSmmV1 BspSmmResumeVector exit	0xA513
PspSmmV1 ApSmmResumeVector entry	0xA514
PspSmmV1 ApSmmResumeVector exit	0xA515
PspP2CmboxV1 entry	0xA516
PspP2CmboxV1 exit	0xA517
// PSP V2 Modules	
PspPeiV2 entry	0xA521
PspPeiV2 exit	0xA522
PspDxeV2 entry	0xA523
PspDxeV2 exit	0xA524
PspDxeV2 PspMpServiceCallBack entry	0xA525
PspDxeV2 PspMpServiceCallBack exit	0xA526
PspDxeV2 FlashAccCallBack entry	0xA527
PspDxeV2 FlashAccCallBack exit	0xA528
PspDxeV2 ready to boot entry	0xA529
PspDxeV2 ready to boot exit	0xA52A
PspDxeV2 exit boot serivce entry	0xA52B
PspDxeV2 exit boot serivce exit	0xA52C
PspSmmV2 entry	0xA52D
PspSmmV2 exit	0xA52E
PspSmmV2 SwSmiCallBack entry, build the S3 save area for resume	0xA52F
PspSmmV2 SwSmiCallBack exit, build the S3 save area for resume	0xA530
PspSmmV2 BspSmmResumeVector entry	0xA531
PspSmmV2 BspSmmResumeVector exit	0xA532
PspSmmV2 ApSmmResumeVector entry	0xA533
PspSmmV2 ApSmmResumeVector exit	0xA534
PspP2CmboxV2 entry	0xA535
PspP2CmboxV2 exit	0xA536
TpPspRecoverApcbFail	0xA537
// PSP fTpm modules	
PspfTpmPei entry	0xA540
PspfTpmPei exit	0xA541
PspfTpmPei memory callback entry	0xA542
PspfTpmPei memory callback exit	0xA543
PspfTpmDxe entry	0xA544
PspfTpmDxe exit	0xA545
// P2C mailbox Handling [0xA59X]	
PspP2Cmbox Command SpiGetAttrib Handling entry	0xA591

PspP2Cmbox Command SpiSetAttrib Handling entry	0xA592
PspP2Cmbox Command SpiGetBlockSize Handling entry	0xA593
PspP2Cmbox Command SpiReadFV Handling entry	0xA594
PspP2Cmbox Command SpiWriteFV Handling entry	0xA595
PspP2Cmbox Command SpiEraseFV Handling entry	0xA596
PspP2Cmbox Command Handling exit	0xA59E
PspP2Cmbox Command Handling Fail exit	0xA59F
// C2P mailbox Handling	
PSP C2P mailbox entry base [0xA5BX | Cmd]	0xA5B0
Before send C2P command MboxBiosCmdDramInfo	0xA5B1
Before send C2P command MboxBiosCmdSmmInfo	0xA5B2
Before send C2P command MboxBiosCmdSleep SxInfo	0xA5B3
Before send C2P command MboxBiosCmdRsmInfo	0xA5B4
Before send C2P command MboxBiosCmdQueryCap	0xA5B5
Before send C2P command MboxBiosCmdBootDone	0xA5B6
Before send C2P command MboxBiosCmdClearS3Sts	0xA5B7
Before send C2P command MboxBiosCmdS3DataInfo	0xA5B8
Before send C2P command MboxBiosCmdNop	0xA5B9
Before send C2P command MboxBiosCmdHSTIQuery	0xA5C4
Before send C2P command MboxBiosCmdClrSmmLock	0xA5C7
Before send C2P command MboxBiosCmdPcieInfo	0xA5C8
Before send C2P command MboxBiosCmdGetVersion	0xA5C9
PSP C2P mailbox exit base [0xA5DX | Cmd]	0xA5D0
Wait C2P command MboxBiosCmdDramInfo finished	0xA5D1
Wait C2P command MboxBiosCmdSmmInfo finished	0xA5D2
Wait C2P command MboxBiosCmdSleep SxInfo finished	0xA5D3
Wait C2P command MboxBiosCmdRsmInfo finished	0xA5D4
Wait C2P command MboxBiosCmdQueryCap finished	0xA5D5
Wait C2P command MboxBiosCmdBootDone finished	0xA5D6
Wait C2P command MboxBiosCmdClearS3Sts finished	0xA5D7
Wait C2P command MboxBiosCmdS3DataInfo finished	0xA5D8
Wait C2P command MboxBiosCmdNop finished	0xA5D9
Wait C2P command MboxBiosCmdHSTIQuery finished	0xA5E4
Wait C2P command MboxBiosCmdClrSmmLock finished	0xA5C7
Wait C2P command MboxBiosCmdPcieInfo finished	0xA5C8
Wait C2P command MboxBiosCmdGetVersion finished	0xA5C9
// fTPM command Handling [0xA5FX]	
PspfTpm send TPM command entry	0xA5F0
PspfTpm send TPM command exit	0xA5F1
PspfTpm receive TPM command entry	0xA5F2
PspfTpm receive TPM command exit	0xA5F3

5-10-6 [0xA9XX, 0xAAXX] assigned for AGESA NBIO Module

// NbioBase	
AmdNbioBase PEIM driver entry	0xA900
AmdNbioBase PEIM driver exit	0xA901
AmdNbioBase DXE driver entry	0xA902
AmdNbioBase DXE driver exit	0xA903
// PCIe	
AmdNbioPcie PEIM driver entry	0xA904
AmdNbioPcie PEIM driver exit	0xA905
AmdNbioPcie DXE driver entry	0xA906
AmdNbioPcie DXE driver exit	0xA907
// GFX	
AmdNbioGfx PEIM driver entry	0xA908
AmdNbioGfx PEIM driver exit	0xA909
AmdNbioGfx DXE driver entry	0xA90A
AmdNbioGfx DXE driver exit	0xA90B
// IOMMU	
AmdNbioIommu DXE driver entry	0xA90C
AmdNbioIommu DXE driver exit	0xA90D
// ALIB	
AmdNbioALIB DXE driver entry	0xA90E
AmdNbioALIB DXE driver exit	0xA90F
// SMU	
AmdSmuV8 PEIM driver entry	0xA910
AmdSmuV8 PEIM driver exit	0xA911
AmdSmuV8 DXE driver entry	0xA912
AmdSmuV8 DXE driver exit	0xA913
AmdSmuV9 PEIM driver entry	0xA914
AmdSmuV9 PEIM driver exit	0xA915
AmdSmuV9 DXE driver entry	0xA916
AmdSmuV9 DXE driver exit	0xA917
AmdSmuV10 PEIM driver entry	0xA918
AmdSmuV10 PEIM driver exit	0xA919
AmdSmuV10 DXE driver entry	0xA91A
AmdSmuV10 DXE driver exit	0xA91B
// IOMMU PEIM	
AmdNbioIommu PEIM driver entry	0xA920
AmdNbioIommu PEIM driver exit	0xA921
// APCB DXE	
APCB DXE Entry	0xA922
APCB DXE Exit	0xA923

// APCB SMM	
APCB SMM Entry	0xA924
APCB SMM Exit	0xA925
// [0xA950, 0xA99F] NBIO PPI/PROTOCOL Callback	
NbioTopologyConfigureCallback entry	0xA950
NbioTopologyConfigureCallback exit	0xA951
MemoryConfigDoneCallbackPpi entry	0xA952
MemoryConfigDoneCallbackPpi exit	0xA953
DxioInitializationCallbackPpi entry	0xA954
DxioInitializationCallbackPpi exit	0xA955
DispatchSmuV9Callback entry	0xA956
DispatchSmuV9Callback exit	0xA957
DispatchSmuV10Callback entry	0xA958
DispatchSmuV10Callback exit	0xA959
AmdPcieMiscInit Event entry	0xA95A
AmdPcieMiscInit Event exit	0xA95B
NbioBaseHookReadyToBoot Event entry	0xA95C
NbioBaseHookReadyToBoot Event exit	0xA95D
NbioBaseHookPciIO Event entry	0xA95E
NbioBaseHookPciIO Event exit	0xA95F
// [0xA980, 0xA99F] BR GNB Task	
GnbEarlyInterfaceCZ entry	0xA970
GnbEarlyInterfaceCZ exit	0xA971
PcieConfigurationInit entry	0xA972
PcieConfigurationInit exit	0xA973
GnbEarlierInterfaceCZ entry	0xA974
GnbEarlierInterfaceCZ exit	0xA975
PcieEarlyInterfaceCZ entry	0xA976
PcieEarlyInterfaceCZ exit	0xA977
PciePostEarlyInterfaceCZ entry	0xA978
PciePostEarlyInterfaceCZ exit	0xA979
GfxConfigPostInterfaceCZ entry	0xA97A
GfxConfigPostInterfaceCZ exit	0xA97B
GfxPostInterfaceCZ entry	0xA97C
GfxPostInterfaceCZ exit	0xA97D
GnbPostInterfaceCZ entry	0xA97E
GnbPostInterfaceCZ exit	0xA97F
PciePostInterfaceCZ entry	0xA980
PciePostInterfaceCZ exit	0xA981
GnbEnvInterfaceCZ entry	0xA982
GnbEnvInterfaceCZ exit	0xA983

GfxConfigEnvInterface entry	0xA984
GfxConfigEnvInterface exit	0xA985
GfxEnvInterfaceCZ entry	0xA986
GfxEnvInterfaceCZ exit	0xA987
GfxMidInterfaceCZ entry	0xA988
GfxMidInterfaceCZ exit	0xA989
GfxIntInfoTableInterfaceCZ entry	0xA98A
GfxIntInfoTableInterfaceCZ exit	0xA98B
PcieMidInterfaceCZ entry	0xA98C
PcieMidInterfaceCZ exit	0xA98D
GnbMidInterfaceCZ entry	0xA98E
GnbMidInterfaceCZ exit	0xA98F
GnbSmuMidInterfaceCZ entry	0xA990
GnbSmuMidInterfaceCZ exit	0xA991
InvokeAmdInitLate entry	0xA992
InvokeAmdInitLate exit	0xA993
GnbSmuServiceRequestV8 entry	0xA994
GnbSmuServiceRequestV8 exit	0xA995

5-10-7 [0xACXX] assigned for AGESA CCX Module

CCX IDS IDS_HOOK_CCX_AFTER_AP_LAUNCH	0xAC10
CCX PEI entry	0xAC50
CCX downcore entry	0xAC51
CCX DXE entry	0xAC55
CCX MP service callback entry	0xAC56
CCX Read To Boot callback entry	0xAC57
CCX SMM entry	0xAC5D
CCX PEI start to launch APs for S3	0xAC70
CCX PEI end of launching APs for S3	0xAC71
CCX start to launch AP	0xAC90
CCX launch AP is ended	0xAC91
CCX launch AP abort	0xAC92
CCX MP service abort	0xAC93
CCX cac weights	0xAC94
CCX PEI exit	0xACE0
CCX downcore exit	0xACE1
CCX DXE exit	0xACE5
CCX MP service callback exit	0xACE6
CCX Read To Boot callback exit	0xACE7
CCX SMM exit	0xACED

5-10-8 [0xADXX] assigned for AGESA DF Module

DF PEI entry	0xAD50
DF DXE entry	0xAD55
DF Ready to Boot entry	0xAD56
DF PEI exit	0xADE0
DF DXE exit	0xADE5
DF Ready to Boot exit	0xADE6

5-10-9 [0xAFXX] assigned for AGESA FCH Module

FCH InitReset dispatch point	0xAF01
FCH InitEnv dispatch point	0xAF06
FCH InitMid dispatch point	0xAF07
FCH InitLate dispatch point	0xAF08
FCH InitS3Early dispatch point	0xAF0B
FCH InitS3Late dispatch point	0xAF0C
FCH InitS3Early dispatch finished	0xAF0D
FCH InitS3Late dispatch finished	0xAF0E
FCH Pei Entry	0xAF10
FCH Pei Exit	0xAF11
FCH MultiFch Pei Entry	0xAF12
FCH MultiFch Pei Exit	0xAF13
FCH Dxe Entry	0xAF14
FCH Dxe Exit	0xAF15
FCH MultiFch Dxe Entry	0xAF16
FCH MultiFch Dxe Exit	0xAF17
FCH Smm Entry	0xAF18
FCH Smm Exit	0xAF19
FCH Smm Dispatcher Entry	0xAF20
FCH Smm Dispatcher Exit	0xAF21
FCH InitReset HwAcpi	0xAF40
FCH InitReset AB Link	0xAF41
FCH InitReset LPC	0xAF42
FCH InitReset SPI	0xAF43
FCH InitReset eSPI	0xAF44
FCH InitReset SD	0xAF45
FCH InitReset eMMC	0xAF46
FCH InitReset SATA	0xAF47
FCH InitReset USB	0xAF48
FCH InitReset xGbE	0xAF49
FCH InitReset HwAcpiP	0xAF4F
FCH InitEnv HwAcpi	0xAF50

FCH InitEnv AB Link	0xAF51
FCH InitEnv LPC	0xAF52
FCH InitEnv SPI	0xAF53
FCH InitEnv eSPI	0xAF54
FCH InitEnv SD	0xAF55
FCH InitEnv eMMC	0xAF56
FCH InitEnv SATA	0xAF57
FCH InitEnv USB	0xAF58
FCH InitEnv xGbE	0xAF59
FCH InitEnv HwAcpiP	0xAF5F
FCH InitMid HwAcpi	0xAF60
FCH InitMid AB Link	0xAF61
FCH InitMid LPC	0xAF62
FCH InitMid SPI	0xAF63
FCH InitMid eSPI	0xAF64
FCH InitMid SD	0xAF65
FCH InitMid eMMC	0xAF66
FCH InitMid SATA	0xAF67
FCH InitMid USB	0xAF68
FCH InitMid xGbE	0xAF69
FCH InitLate HwAcpi	0xAF70
FCH InitLate AB Link	0xAF71
FCH InitLate LPC	0xAF72
FCH InitLate SPI	0xAF73
FCH InitLate eSPI	0xAF74
FCH InitLate SD	0xAF75
FCH InitLate eMMC	0xAF76
FCH InitLate SATA	0xAF77
FCH InitLate USB	0xAF78
FCH InitLate xGbE	0xAF79
End of TP range for FCH	0xAFFF
Last defined AGESA PCs	0xFFFF

5-11 BIOS POST Beep code (AMI standard)

5-11-1 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed.
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

5-11-2 DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

5-12 BIOS Recovery Instruction

The system has an embedded recovery technique. In the event that the BIOS becomes corrupt the boot block can be used to restore the BIOS to a working state. To restore your BIOS, please follow the instructions listed below:

Recovery Instruction:

1. Change xxx.ROM to amiboot.rom.
2. Copy amiboot.rom and AFUDOS.exe to USB diskette.
3. Setting BIOS Recovery jump to enabled status.
4. Boot into BIOS recovery.
5. Run Proceed with flash update.
6. BIOS update.

