# **BIOS Setup**

(For Purley Platform)

User's Guide

Rev.1.0

# **Copyright**

© 2017 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, visit our website at:

# http://b2b.gigabyte.com

You are a professional?

Get an access to our complete source of sales, marketing & technical materials at:

# http://reseller.b2b.gigabyte.com



# Table of Contents

Chapter 1	BIOS Se	tup	5
	1-1 Th	e Main Menu	7
	1-2 Ad	vanced Menu	10
	1-2-1	iSCSI Configuration	11
	1-2-2	Intel(R) Virtual RAID on CPU	12
	1-2-3	Intel(R) Ethernet Connection X722	13
	1-2-3-1	NIC Configuration	16
	1-2-4	Trusted Computing	17
	1-2-5	Serial Port Console Redirection	18
	1-2-5-1	COM1/COM2 Serial Over LAN/Legacy/Serial Port for Out-of-Band EMS	
		Console Redirection Settings	19
	1-2-6	SIO Configuration	22
	1-2-7	PCI Subsystem Settings	25
	1-2-8	Network Stack	26
	1-2-9	CSM Configuration	27
	1-2-10	Post Report Configuration	29
	1-2-11	NVMe Configuration	30
	1-2-12	USB Configuration	31
	1-2-13	Chipset Configuration	32
	1-3 Ch	ipset Setup Menu	33
	1-3-1	Processor Configuration	34
	1-3-1-1	Pre-Socket Configuration	36
	1-3-2	Common RefCode Configuration	38
	1-3-3	UPI Configuration	39
	1-3-4	Memory Configuration	41
	1-3-4-1	Memory Topology	43
	1-3-4-2	Memory RAS Configuration	44
	1-3-5	IIO Configuration	45
	1-3-5-1	Intel® VT for Directed I/O (VT-d)	46
	1-3-5-2	Inter® VMD Technology	47
	1-3-6	Advanced Power Management Configuration	48
	1-3-6-1	CPU P State Control	49
	1-3-6-2	Hardware PM State Control	50
	1-3-6-3	CPU C State Control	51
	1-3-6-4	Package C State Control	52
	1-3-6-5	CPU-Advanced PM Tuning	53
	1-3-7	PCH Configuration	55
	1-3-7-1	PCH SATA Configuration	56

1-3-7-	2 PCH sSATA Configuration	58
1-3-8	Miscellaneous Configuration	60
1-3-9	Server ME Configuration	61
1-3-10	Runtime Error Logging	62
1-3-10	-1 Whea Settings	63
1-3-10	-2Memory Error Enabling	64
1-3-10	-3PCle Error Enabling	65
1-4 Se	erver Management Menu	
1-4-1	System Event Log	68
1-4-2	View FRU Information	69
1-4-3	BMC Network Configuration	70
1-4-4	IPv6 BMC Network Configuration	71
1-5 Se	ecurity Menu	72
1-5-1	Secure Boot	73
1-5-1-	1 Key Management	74
1-6 Bo	oot Menu	76
1-6-1	UEFI NETWORK Drive BBS Priorities	78
1-6-2	UEFI Application Boot Priorities	79
1-7 Sa	ave & Exit Menu	80
1-8 BI	OS POST Codes	82
1-8-1 Al	/I Standard - PEI	82
1-8-2	AMI Standard - DXE	82
1-8-3	AMI Standard - ERROR	84
1-8-4	Intel UPI POST Codes	85
1-8-5	Intel UPI Error Codes	85
1-8-6	Intel MRC POST Codes	86
1-8-7	Intel MRC Error Codes	86
1-8-8	Intel PM POST Codes	87
1-8-8	Intel PM POST Codes	87
1-9 BI	OS POST Beep code (AMI standard)	
1-9-1	PEI Beep Codes	88
1-9-2	DXE Beep Codes	88
1-10 BI	OS Recovery Instruction	

# 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 <F2> 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></enter>	Execute command or enter the submenu
<esc> Main Menu: Exit the BIOS Setup program</esc>		Main Menu: Exit the BIOS Setup program
		Submenus: Exit current submenu
	<f1></f1>	Show descriptions of general help
	<f3></f3>	Restore the previous BIOS settings for the current submenus
	<f9></f9>	Load the Optimized BIOS default settings for the current submenus
	<f10></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.)

# 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.)

# 1-1 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.

Aptio Setup Main Advanced Chipset	Utility – Copyright (C) 2017 American Meg Server Mgmt Security Boot Save & Exit	atrends, Inc.
Project Name Project Version Build Date and Time	MD71-HB0-00 F03 06/22/2017 19:04:38	
BMC Information BMC Firmware Version	01.12	
Processor Information CPU 0 Brand String CPU 1 Brand String Max CPU Speed CPU Signature	Intel(R) Xeon(R) Gold 614 Intel(R) Xeon(R) Gold 614 2300 MHz 50654	
Processor Core Microcode Patch	36 02000022	→+: Select Screen ↑↓: Select Item
Platform Information Processor PCH RC Revision	SKX HO LBG QS/PRQ - 2 - S1 137.R08	Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values
Memory Information Total Memory Memory Frequency	8192 MB 2133 MHz	F10: Save & Exit ESC: Exit
Onboard LAN Information	₹	

Processor Information		▲ Set the Time, Use Tab to
CPU 0 Brand String	Intel(R) Xeon(R) Gold 614	. switch between Time
CPU 1 Brand String	Intel(R) Xeon(R) Gold 614	. elements.
Max CPU Speed	2300 MHz	
CPU Signature	50654	
Processor Core	36	
Microcode Patch	02000022	
Platform Information		
Processor	SKX HO	
PCH	LBG QS/PRQ - 2 - S1	
RC Revision	137.R08	
Memory Information		++: Select Screen
Total Memory	8192 MB	<b>↑↓</b> : Select Item
Memory Frequency	2133 MHz	Enter: Select
		+/-: Change Opt.
Onboard LAN Information		F1: General Help
LAN1 MAC Address	1C-1B-0D-E6-02-12	F3: Previous Values
LAN2 MAC Address	1C-1B-0D-E6-02-13	F9: Optimized Defaults
LAN3 MAC Address	1C-1B-0D-E6-02-14	F10: Save & Exit
LAN4 MAC Address	1C-1B-0D-E6-02-15	ESC: Exit
System Date	[Mon 07/17/2017]	
	[15:07:02]	*

## ∽ 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<sup>(Note)</sup>
- ∽ BMC Firmware Version<sup>(Note)</sup>

Displays BMC firmware version information.

∽ Processor Information

# $\backsim$ CPU Brand String/Max CPU Speed/CPU Signature/Processors Core/Microcode Patch

Displays the technical specifications for the installed processor.

- ∽ Platform Information
- ∽ Processor/PCH/RC Revision

Displays the information for the installed platform.

- ∽ Memory Information
- ∽ Total Memory<sup>(Note)</sup>

Displays the total memory size of the installed memory.

∽ Memory Frequency<sup>(Note)</sup>

Displays the frequency information of the installed memory.

∽ Onboard LAN Information

# C LAN MAC Address(Note)

Displays LAN MAC address information.

∽ System Date

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

System Time

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

# 1-2 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.

Aptio Setup Utility – Copyright (C) 2017 American Meg Main Advanced Chipset Server Mgmt Security Boot Save & Exit	atrends, Inc.
<ul> <li>ISCSI Configuration</li> <li>Intel(R) Virtual R&amp;ID on CPU</li> <li>Intel(R) Ethernet Connection X722 for 106BASE-T - 10:1B:0D:E</li> <li>Intel(R) Ethernet Connection X722 for 106BASE-T - 10:1B:0D:E</li> <li>Intel(R) Ethernet Connection X722 for 16bE - 10:1B:0D:E6:02:15</li> <li>Trusted Computing</li> <li>Serial Port Console Redirection</li> <li>S10 Configuration</li> <li>PCI Subsystem Settings</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NWME Configuration</li> <li>SUB Configuration</li> <li>USB Configuration</li> <li>Chipset Configuration</li> </ul>	Configure the iSESI parameters. 
Version 2 19 1268 Fonucidht (F) 2017 American Medat	mondo The

# 1-2-1 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.

# 1-2-2 Intel(R) Virtual RAID on CPU



# ∽ Intel(R) Virtual RAID on CPU

Press [Enter] to manage Interl® Virtual RAID on the CPU.

# 1-2-3 Intel(R) Ethernet Connection X722



Version 2.19.1268. Copyright (C) 2017 American Megatrends, Ind

		Click to configure the
Blink LEDs	0	network device port.
UEFI Driver	Intel(R) 40GbE 2.1.14	
Adapter PBA	303700-000	
Device Name	Intel(R) Ethernet Connect	
Chip Type	Intel X722	
PCI Device ID	3702	
PCI Address	1A:00:01	
Link Status	[Disconnected]	
MAC Address	1C:1B:0D:E6:02:13	++: Select Screen
Virtual MAC Address	00:00:00:00:00	<b>↑↓:</b> Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F3: Previous Values
		F9: Optimized Defaults
		F10: Save & Exit
		ESC: Exit



		Click to configure the
Blink LEDs	0	
JEFI Driver	Intel(R) 40GbE 2.1.14	
Adapter PBA	303700-000	
)evice Name	Intel(R) Ethernet Connect	
Chip Type	Intel X722	
PCI Device ID	37D1	
°CI Address	1A:00:03	
ink Status.	[Disconnected]	
1AC Address	1C:1B:0D:E6:02:15	++: Select Screen
/irtual MAC Address	00:00:00:00:00	<b>↑↓</b> : Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F3: Previous Values
		F9: Optimized Defaults
		F10: Save & Exit
		ESC: Exit

∽ Intel(R) Ethernet Connection X722 for 10GBASE-T

# ∽ Intel(R) Ethernet Connection X722 for 10GbE

#### ∽ NIC Configuration

Press [Enter] for configuration of advanced items of the selected network device port.

#### ☞ Blink LEDs

Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.

#### 

Displays the technical specifications for the Network Interface Controller.

Ċ	Adapter PBA
	Displays the technical specifications for the Network Interface Controller.
Ċ	Device Name
	Displays the technical specifications for the Network Interface Controller.
T	Сһір Туре
	Displays the technical specifications for the Network Interface Controller.
Ċ	PCI Device ID
	Displays the technical specifications for the Network Interface Controller.
Ċ	PCI Address
	Displays the technical specifications for the Network Interface Controller.
T	Link Status
	Displays the technical specifications for the Network Interface Controller.
Ċ	MAC Address
	Displays the technical specifications for the Network Interface Controller.
Ċ	Virtual MAC Address

Displays the technical specifications for the Network Interface Controller.

# 1-2-3-1 NIC Configuration

Aptio Setup L Advanced	Jtility – Copyright (C) 2017 America	n Megatrends, Inc.
Link Speed Hake On LAN	[Auto Negotiated] [Enabled]	Enables power on of the system via LAN. Note that configuring Make on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.
		+: Select Screen 11: Select Trem Enter: Select +/-: Change Opt. F1: General Help F3: Frevious Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
	0.1268. Copyright (C) 2017 American	Megatrends, Inc.

# ∽ Link Speed

Allows for automatic link speed adjustment. Default setting is Auto Negotiated.

# ⑦ Wake On LAN

Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.

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

# 1-2-4 Trusted Computing

Aptio Setup Utility Advanced	– Copyright (C) 201	7 American Megatrends,	Inc.
Configuration Security Device Support ND Security Device Found		Enables support device. Securit, protoco. interfa availab.	or Disables BIOS for security O.S. will not show y Device. TCG EFI 1 and INTIA 2e will not be le.
		++: Self 11: Self Enter: 3 +/-: Chk F1: Gen F3: Pre F9: Opt. F10: Say ESC: Ex.	sct Screen sct Item Select ange Opt. eral Help /lous Values imized Defaults e & Exit it
Version 2.19.1268.	Copyright (C) 2017	American Megatrends, In	ю.

∽ Configuration

# ∽ Security Device Support

Enable/Disable the TPM support feature. Options available: Enable/Disable. Default setting is **Enable**.

# ∽ Current Status Information

Displays current TPM status information.

# 1-2-5 Serial Port Console Redirection

Aptio Setup Utility – C Advanced	opyright (C) 2017 American Meg	atrends, Inc.
COM1 Console Redirection ▶ Console Redirection Settings		Console Redirection Enable or Disable.
COM2/Serial Over LAN Console Redirection Console Redirection Settings Legacy Console Redirection	[Disabled]	
<ul> <li>Legacy Console Redirection Settings</li> <li>Serial Port for Out-of-Band Managemen Windows Emergency Management Services</li> <li>Console Redirection</li> <li>Console Redirection Settings</li> </ul>	t∕ (EMS) [Disabled]	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Prevlous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit

## ∽ COM1/COM2 Serial Over LAN Console Redirection<sup>(Note)</sup>

Select whether to enable console redirection for 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<sup>(Note)</sup>

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 Outof-Band Management EMS Console Redirection is set to Enabled.

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

COM1 Console Redirection Settings		Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+:
Terminal Type	[ANSI]	Extends VT100 to support
Data Bito	[115200]	WT-UTER: Uses UTER
Paritu	[None]	encoding to man Unicode
Stop Bits	[1]	chars onto 1 or more bytes
Flow Control	[None]	
VT-UTF8 Combo Key Support	[Enabled]	
Recorder Mode	[Disabled]	
Resolution 100x31	[Enabled]	
Legacy US Redirection Resolution	[80x24] [VT100]	++ · Salact Screen
Redirection After BIOS POST	[Always Enable]	11: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F3: Previous Values
		F9: Uptimized Defaults
		ESC: Exit

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Advanced COM2/Serial Over LAN Emulation: ANSI: Extended Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100: Extends VT100 to support color, function keys, etc. VT-UTFB: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes. Console Redirection Settings Bits per second Data Bits [8] Parity [None] Stop Bits Flow Control [None] Flow Control VT-UTF8 Combo Key Support Recorder Mode Resolution 100x31 Legacy OS Redirection Resolution Putty KeyPad Redirection After BIOS POST [Enabled] [Disabled] [Enabled] [80x24] [VT100] ↔. Select Screen †↓: Select Item [Always Enable] Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit





# ☞ 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  ${\bf 8}$ .

# 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<sup>(Note)</sup>

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<sup>(Note)</sup>

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

# Center Legacy OS Redirection Resolution<sup>(Note)</sup>

Specifies the number of Rows and Columns supported for the Legacy OS redirection. Options available: 80x24/80x25. Default setting is 80x24.

# ∽ Putty KeyPad<sup>(Note)</sup>

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

# Redirection After BIOS POST<sup>(Note)</sup>

This item allows user to enable console redirection after O.S has loaded. Options available: Always Enable/Boot Loader. Default setting is **Always Enable**.

# ∽ Legacy Console Redirection Settings

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**.

# ○ 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.

# 1-2-6 SIO Configuration



Aptio Setup Utility Advanced	– Copyright (C) 2017 American Me	gatrends, Inc.
Serial Port 1 Configuration		Enable or Disable this
		Logical Device.
Logical Device Settings: Current : IO=3F8h; IRQ=4;		
Possible:	[Use Automatic Settings]	
WARNING: Disabling SIO Logical Dev	ices may have unwanted side	++: Select Screen 14: Select Item Enter: Select */-: Change Oot. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.19.1268.	Copyright (C) 2017 American Mega	trends, Inc.



# ∽ AMI SIO Driver Version

Displays the AMI SIO driver version information.

# ∽ Super IO Chip Logical Device(s) Configuration

# ☞ [\*Active\*] Serial Port 1/Serial Port 2

Press [Enter] for configuration of advanced items.

# ∽ Serial Port 1/Serial Port 2 Configuration

# ∽ Use This Device

When set to Enabled allows you to configure the Serial port 1/Serial port 2 settings. When set to Disabled, displays no configuration for the serial port.

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

# ∽ Logical Device Settings

# ∽ Current:

Displays the Serial Port 1/Serial port 2 base I/O address and IRQ.

# Possible:

Configures the Serial Port 1/Serial port 2 base I/O address and IRQ. Options available for Serial Port 1: Use Automatic Settings IO=3F8h; IRQ=4; DMA; IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; Default setting is **Use Automatic Settings**. Options available for Serial Port 2: Use Automatic Settings IO=2F8h; IRQ=3; DMA; IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; Default setting is **Use Automatic Settings**.

# 1-2-7 PCI Subsystem Settings

Aptio Setup Utility Advanced	– Copyright (C) 2017 American Me	egatrends, Inc.
PCI Bus Driver Version PCI Express Slot #1 1/0 RDM PDI Express Slot #2 1/0 RDM PDI Express Slot #4 1/0 RDM PDI Express Slot #4 1/0 RDM PDI Express Slot #6 1/0 RDM PDI Express Slot #6 1/0 RDM PDI Express Slot #6 1/0 RDM PDI Express Slot #8 1/0 RDM PDI Express Slot #8 1/0 RDM Onboard LANI 1/0 RDM Onboard LANI 1/0 RDM Onboard LANA 1/0 RDM PDI Devices Common Settings: Above 46 Decoding SR-IDV Support	A5.01.12 [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [UEFI] [UEFI] [UEFI] [Disabled] [Enabled]	Enable/Disable PCI-Express slot #1 I/O ROM. **: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
	Conuniabt (C) 2017 Amonicon Mode	taoado Tao

#### ☞ PCI Bus Driver Version

Displays the PCI Bus Driver version information.

#### PCI Express Slot #1/#2/#3/#4/#5/#6/#7/#8 I/O ROM<sup>(Note)</sup>

When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled/Disabled. Default setting is **Enabled**.

#### ∽ Onboard LAN1 Controller<sup>(Note)</sup>

Enable/Disable the onboard LAN1 devices. Options available: Enabled/Disabled. Default setting is **Enabled**.

#### Onboard LAN #1/#2/#3/#4 I/O ROM<sup>(Note)</sup>

Enable/Disable the onboard LAN devices, and initializes device expansion ROM. Options available for LAN #1: Enabled/Disabled. Default setting is **Enabled**. Options available for LAN #2/#3/#4: Disabled/UEFI/Legacy. Default setting is **UEFI**.

#### PCI Devices Common Settings

#### → Above 4G Decoding

Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled/Disabled. Default setting is **Disabled**.

#### ☞ 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 Enabled.

# 1-2-8 Network Stack



#### ONE Network stack

Enable/Disable the UEFI network stack.

Options available: Enabled/DIsabled. Default setting is Enabled.

#### ∽ Ipv4 PXE Support<sup>(Note)</sup>

Enable/Disable the Ipv4 PXE feature. Options available: Enabled/DIsabled. Default setting is **Enabled**.

#### ∽ Ipv4 HTTP Support<sup>(Note)</sup>

Enable/Disable the Ipv4 HTTP feature. Options available: Enabled/Disabled. Default setting is **Disabled**.

#### Ipv6 PXE Support<sup>(Note)</sup>

Enable/Disable the Ipv6 PXE feature. Options available: Enabled/DIsabled. Default setting is **Disabled**.

## ∽ Ipv6 HTTP Support<sup>(Note)</sup>

Enable/Disable the Ipv6 HTTP feature. Options available: Enabled/DIsabled. Default setting is **Disabled**.

#### ∽ PXE boot wait time<sup>(Note)</sup>

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

## Media detect count<sup>(Note)</sup>

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

# 1-2-9 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 configurable when CSM Support 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.

 $\label{eq:options} \mbox{Options available: Upon Request/Always. Default setting is \mbox{Upon Request}.$ 

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.

#### ☞ INT19 Endless Retry

Enable/Disable headless retry boot. Options available: Enabled/Disabled. Default setting is **Enabled**. **Please note that this item is configurable when CSM Support is set to Enabled.** 

# Option ROM execution

#### P 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.

# 1-2-10 Post Report Configuration



- ∽ Post Report Configuration
- ☞ Error Message Report
- ∽ Post Error Message

Enable/Disable the POST Error Message support. Options available: Enabled/Disabled. Default setting is **Enabled**.

# 1-2-11 NVMe Configuration



# ∽ NVMe Configuration

Displays the NVMe devices connected to the system.

# 1-2-12 USB Configuration



#### ☞ USB Configuration

#### → USB Devices:

Displays the USB devices connected to the system.

#### ∽ XHCI Hand-off

Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled/Disabled. Default setting is **Enabled**.

#### C USB Mass Storage Driver Support<sup>(Note)</sup>

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 aware OS.

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

# 1-2-13 Chipset Configuration

Aptio Setup Util: Advanced	ity – Copyright (C) 2017 Ame	rican Megatrends, Inc.
Restore AC Power Loss		Specify what state when
Chassis Opened Warning	[Disabled]	a power failure (63 state).
		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.19.126	68. Copyright (C) 2017 Ameri	can Megatrends, Inc.

## → Restore on AC Power Loss<sup>(Note)</sup>

Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Stay Off, the system remains off after power shutdown.

Options available: Last State/Stay Off/Power On. The default setting depends on the BMC setting.

## ∽ Chassis Opened Warning

Enable/Disable the chassis intrusion alter function. Options available: Enabled/Disabled. Default setting is **Disabled**.

<sup>(</sup>Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

# 1-3 Chipset Setup Menu

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



# 1-3-1 Processor Configuration

Aptio Setup Utility Chipset	∣ – Copyright (C) 2017 American	Megatrends, Inc.
Processor Configuration		Change Per-Socket Settings
Per-Socket Donfiguration     Processor Socket     Processor ID     Processor Frequency     Processor Max Ratio     Microcode Revision     L1 Cache RAM     L2 Cache RAM     L3 Cache RAM     Processor 0 Version     Processor 1 Version	Socket 0 Socket 1 00050654* 00050654 2.3006Hz   2.3006Hz 17H   17H 0AH   0AH 02000022 64KB   64KB 1024KB   1024KB 25344KB   25344KB Intel(R) Xeon(R) Gold 6 140 CPU @ 2.306Hz Intel(R) Xeon(R) Gold 6 140 CPU @ 2.306Hz	++: Select Screen 11: Select Item Enter: Select
Hyper-Threading [ALL] Enable Intel(R) TXT VMX Enable SMX Hardware Prefetcher Adjacent Cache Prefetch DCU Streamer Prefetcher DCU IP Prefetcher	(Enable) [Disable] [Enable] [Disable] [Enable] [Enable] [Enable] [Enable]	F:: General Help F3: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit

Version 2.19.1268. Copyright (C) 2017 American Megatrends, Inc



#### ∽ Processor Configuration

#### ∽ Pre-Socket Configuration

Press [Enter] for configuration of advanced items.

# Processor Socket/Processor ID/Processor Frequency/Processor Max Raito/ Processor Min Raio/Microcode Revision/L1 Cache RAM/L2 Cache RAM/L3 Cache RAM/ Processor 0/1 Version

Displays the technical specifications for the installed processor.

# ∽ Hyper-Threading [All]

The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance.

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

# ☞ Enable Intel(R) TXT

Enables ord isables the Intel Trusted Execution Technology support function. Options available: Enable/Disable. Default setting is **Disable**.

# VMX (Vanderpool Technology)

Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: Enable/Disable. Default setting is **Enable**.

# ☞ Enable SMX

 ${\mbox{Enable/Disable the Secure Mode Extensions (SMX) support function.}$ 

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

# ∽ Hardware Prefetcher

Select whether to enable the speculative prefetch unit of the processor. Options available: Enable/Disable. Default setting is **Disable**.

# Adjacent Cache Prefetch

When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enable/Disable. Default setting is **Enable**.

# ☞ DCU Streamer Prefetch

Prefetches the next L1 data line based upon multiple loads in same cache line. Options available: Enable/Disable. Default setting is **Enable**.

# DCU IP Prefetch

Prefetches the next L1 Data line based upon sequential load history. Options available: Enable/Disable. Default setting is **Enable**.

# ං Aes-Ni

Enable/Disable the AES-NI (Intel Advanced Encryption Standard New Instructions) support function. Options available: Enable/Disable. Default setting is **Enable**.

# 1-3-1-1 Pre-Socket Configuration




# ∽ CPU Socket 0/1 Configuration

Press [Enter] for configuration of advanced items.

## ∽ Core Disable Bitmap(Hex) (for CPU socket 0/1)

Number of Cores to enable. 0 means all cores. FFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.

# 1-3-2 Common RefCode Configuration



## ∽ Common RefCode Configuration

### ∽ MMIO High Base

Selects the MMIO High Base setting. Options available: 56T/40T/24T/16T/4T/1T. Default setting is 56T.

## ∽ MMIO High Granularity Size

Selects the allocation size used to assign mmioh resources. Total mmioh space can be up to 32xgranularity. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.

Options available: 1G/4G/16G/64G/256G/1024G. Default setting is 256G.

## ∽ Isoc Mode

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

## ∽ Numa (Non-Uniform Memory Access)

Enable/Disable Non-uniform Memory Access (NUMA). Options available: Enable/Disable. Default setting is **Enable**.

# 1-3-3 UPI Configuration



Aptio Setup Util Chipset	ity – Copyright (C) 2017	'American Megatrends, Inc.
UPI General Configuration		UPI Status Help
▶ UPI Status Link Frequency Select	[Auto]	
		★: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Vancian 2 19 12	69 - Copupight (C) 2017 (	menican Magataede - Tac

JPI Status		
Number of CPU Current UPI Link Frequency	2 10.4 GT/s	
		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

# ☞ UPI General Configuration

Press [Enter] to change the UPI general settings.

# ・ UPI Status

Press [Enter] to view the UPI status.

# ∽ Link Frequency Select

Selects the UPI link frequency. Options available: 9.6GB/10.4GB/Auto. Default setting is **Auto**.

# 1-3-4 Memory Configuration

Aptio Setup Utility Chipset	– Copyright (C) 2017 Am	erican Megatrends, Inc.
Chipset Integrated Memory Controller (IAC Enforce POR Memory Frequency Enable ADR Legacy ADR Mode ADR Data Save Mode Erase-Arm NVDIMMS Restore NVDIMMS Interleave NVDIMMS Interleave NVDIMMS Memory RAS Configuration	[Auto] [Auto] [Auto] [Enable] [Disable] [NVOLMS] [Enable] [Enable] [Disable]	Enable - Enforces Plan Df Record restrictions for DDR4 frequency and voltage programming. Disable - Disables this feature. Auto - Sets it to the MRC default setting: current default is Enable. +*: Select Screen 11: Select Item Enter: Select */-: Change Opt. F1: General Help F3: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit
Vapalan 0 40 4050		

## ∽ Integrated Memory Controller (iMC)

### ☞ Enforce POR

When set to Enable, the system enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. When set to Auto, the system sets it to the MRC default settings. Options available: Auto/POR/Disable. Default setting is **Enable**.

### ∽ Memory Frequency

Configures the memory frequency. Options available: Auto/2133/2400/2666. Default setting is **Auto**.

### ☞ Enable ADR

Enables the detecting and enabling of ADR. Options available: Enable/Disable. Default setting is **Enable**.

## ∽ Legacy ADR Mode

Enable/Disable the Legacy ADR Mode. Options available: Enable/Disable. Default setting is **Disable**.

## → ADR Data Save Mode

Data Save Mode for ADR, Batterybacked or Type 01 NVDIMM. Options available: Disable/Batterybacked DIMMs/NVDIMMs. Default setting is **NVDIMMs**.

### ☞ Erase-ARM NVDIMMs

Enable/Disable Erasing and Arming NVDIMMs. Options available: Enable/Disable. Default setting is **Enable**.

### Options available: Enable/Disable. Default setting

# ☞ Restore NVDIMMs

Enable/Disable Automatic restoring of NVDIMMs. Options available: Enable/Disable. Default setting is **Enable**.

## ∽ Interleave NVDIMMs

Controls if NVDIMMs are interleaved together or not. Options available: Enable/Disable. Default setting is **Disable**.

# ∽ Memory Topology

Press [Enter] for configuration of advanced items.

# ∽ Memory RAS Configuration

Press [Enter] for configuration of advanced items.

# 1-3-4-1 Memory Topology



# 1-3-4-2 Memory RAS Configuration



## Memory RAS Configuration Setup

## ా RAS Type

Displays the RAS type.

## ∽ Static Virtual Lockstep Mode

Enable/Disable the Static Virtual Lockstep mode. Options available: Disable/Enable. Default setting is **Disable**.

### ∽ Mirror Mode

Mirror Mode will set entire 1LM/2LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch. Options available: Disable/Mirror Mode 1LM/Mirror Mode 2LM. Default setting is **Disable**.

### ∽ Memory Rank Sparing

Enable/Disable Memory Rank Sparing. Options available: Disable/Enable. Default setting is **Disable**.

## ∽ Correctable Error Threshold

Correctable Error Threshold (1-32767) used for sparing, tagging, and leaky bucket. Press the <+> / <-> keys to increase or decrease the desired values.

## ☞ SDDC Plus One

Enable/Disable SDDC Pluse One. Options available: Disable/Enable. Default setting is **Disable**.

# 1-3-5 IIO Configuration



∽ IIO Configuration

# ∽ Intel® VT for Directed I/O (VT-d)

Press [Enter] for configuration of advanced items.

# ∽ Inter® VMD technology

Press [Enter] for configuration of advanced items.

# 1-3-5-1 Intel® VT for Directed I/O (VT-d)



## ∽ Intel® VT for Directed I/O (VT-d)

## ∽ Intel® VT for Directed I/O (VT-d)

Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables.

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

### → ACS Control

Enable: Programs ACS only to Chipset Pcie Root Ports Bridges. Disable: Programs ACS to all PCIe bridges. Default setting is **Enable**.

### ∽ Interrupt Remapping

Enable/Disable the interrupt remapping support function. Options available: Enable/Disable. Default setting is **Enable**.

### 

Enable/Disable the Non-Isoch VT\_D Engine PassThrough DMA support function. Options available: Enable/Disable. Default setting is **Enable**.

### ~ ATS

Enable/Disable Non-Isoch VT\_D Engine ATS support. Options available: Enable/Disable. Default setting is **Enable**.

### → Posted Interrupt

Enable/Disable VT\_D posted interrupt. Options available: Enable/Disable. Default setting is **Enable**.

### ∽ Coherency Suuport (Non-Isoch)

Enable/Disable Non-Isoch VT\_D Engine Coherency support. Options available: Enable/Disable. Default setting is **Enable**.

# 1-3-5-2 Inter® VMD Technology



∽ Intel® VMD technology

# ∽ Intel® VMD Configuration

Enable/Disable the Intel VMD support function. Options available: Enable/Disable. Default setting is **Disable**.

# 1-3-6 Advanced Power Management Configuration



- ∽ Advanced Power Management Configuration
- ∽ CPU P State Control

Press [Enter] for configuration of advanced items.

- Hardware PM State Control Press [Enter] to configure the Hardware P-State setting.
- → CPU C State Control

Press [Enter] for configuration of advanced items.

→ Package C State Control

Press [Enter] to configure the Package C State limit.

∽ CPU - Advanced PM Tuning

Press [Enter] for configuration of advanced items.

# 1-3-6-1 CPU P State Control

Aptic Setup Utility - Chipset	– Copyright (C) 20	17 American Megatrends, Inc.
CPU P State Control		Enable/Disable EIST
SpeedStep (Pstates) Turbo Mode	[Enable] [Enable]	(1-3(8(63)
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. Fl: General Help F3: Previous Values F9: Optimized Defaults F10: Save &amp; Exit ESC: Exit</pre>
Version 2 19 1268	Conucidat (C) 2017	American Megatrende Inc

## ∽ SpeedStep (Pstates)

Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.

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

## ∽ Turbo Mode

When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance.

When this item is disabled, the processor will not overclock any of its core.

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

# 1-3-6-2 Hardware PM State Control

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Chipset		
Hardware PM State Control Hardware P-States		Disable: Hardware chooses a P–state based on OS Request (Legacy P–States)
		Native Mode:Hardware chooses a P-state based on OS guidance Out of Band Mode:Hardware autonomously chooses a P-state (no OS guidance)
		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: OotImized Defaults F10: Save & Exit ESC: Exit
Version 2 19 1	268 - Popunight (P) 2017 Americ	an Merratoonds. The

## ∽ Hardware P-States

When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States).

In Native mode, the processor hardware chooses a P-state based on OS guidance.

In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance). Options available: Disable/Native Mode/Out of Band Mode/Native Mode with No Legacy Support. Default setting is **Native Mode**.

# 1-3-6-3 CPU C State Control

Aptio Setup Utility - Chipset	Copyright (C)	2017 American Mega	trends, Inc.
CPU C State Control Autonomous Core C-State CPU 66 report Enhanced Halt State (C1E)	(Disable) [Auto] [Enable]	1	autonomous Core C-State Control
OS ACPI C×	[ACPI C2]		
		•	↔: Select Screen 14: Select Item Enter: Select ×/-: Change Opt. 1: General Help 53: Previous Values
			9: Optimized Defaults 70: Save & Exit SSC: Exit
Version 2 19 1268 f	opunight (E) 20	17 American Megatr	ande Inc

## Autonomous Core C-State

Enable/Disable the Autonomous Core C-State Control. Options available: Enable/Disable. Default setting is **Disable**.

### → CPU C6 Report

Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced power-saving state than C1. Options available: Disable/Enable/Auto. Default setting is **Auto**.

### C Enhanced Halt State (C1E)(Note)

Core C1E auto promotion control. Takes effect after reboot. Options available: Enable/Disable. Default setting is **Enable**.

## ு OS ACPI Cx

Reports CPU C3/C6 to OS ACPI C2 or ACPI C3. Options available: ACPI C2/ACPI C3. Default setting is **ACPI C2**.

# 1-3-6-4 Package C State Control

A	ptio Setup Utility – Chipset	Copyright (C) 201	7 American Mega	trends, Inc.
Package C State	Control			Package C State limit
Package C State				+: Select Screen 1: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

# ∽ Package C-State

Configures the state for the C-State package limit. Options available: C0/C1 state/C2 state/C6(non Retention) state/C6(Retention) state/No Limit/Auto. Default setting is **Auto**.

# 1-3-6-5 CPU-Advanced PM Tuning



### ☞ Energy Perf BIAS

Enters the Energy Perf BIAS submenu.

### Power Performance Tuning<sup>(Note)</sup>

Tunes the Power Performance Configuration mode. When enabled, uses IA32\_ENERGY\_PERF\_BIAS input from the core. When disabled, uses alternate performance BIAS input from ENERGY\_PERF\_BIAS\_CONFIG.

Options available: OS Controls EPB/BIOS Controls EPB. Default setting is OS Controls EPB.

# $\frown$ ENERGY\_PERF\_BIAS\_CFG mode

Selects the Energy Performance Bias Configuration Mode. Options available: Performance/Balanced Performance/Balanced Power/Power. Default setting is **Balanced Performance**.

Please note that this item is configurable when Power Performance Tuning is set to BIOS Controls EPB.

# 1-3-7 PCH Configuration



∽ PCH Configuration

# ☞ PCH SATA Configuration

Press [Enter] for configuration of advanced items.

# ∽ PCH sSATA Configuration

Press [Enter] for configuration of advanced items.

# 1-3-7-1 PCH SATA Configuration



## ∽ PCH SATA Configuration

### ∽ SATA Controller(s)

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

### ∽ Configure SATA as

Configure on chip SATA type.

AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time.

RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allows access the RAID setup utility at boot time.

Options available: AHCI/RAID. Default setting is AHCI.

# ∽ Alternate Device ID on RAID<sup>(Note 1)</sup>

Enable/Disable Alternate Device ID on RAID mode. Options available: Enable/Disable. Default setting is **Disabled Please note that this option appears when HDD is in RAID Mode.** 

# · SATA Port 0/1/2/3/4/5/6/7

The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.

## · Port 0/1/2/3/4/5/6/7

Enable/Disable Port 0/1/2/3/4/5/6/7 device. Options available: Enable/Disable. Default setting is **Enable**.

## · Hot Plug (for Port 0/1/2/3/4/5/6/7)(Note2)

Enable/Disable HDD Hot-Plug function. Options available: Enable/Disable. Default setting is **Disable**.

# Spin Up Device (for Port 0/1/2/3/4/5/6/7)<sup>(Note2)</sup>

On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. Options available: Enable/Disable. Default setting is **Disable**.

# 1-3-7-2 PCH sSATA Configuration



Version 2.19.1268. Copyright (C) 2017 American Megatrends, Ind



Alternate Device ID on RAID	[Disable]	<ul> <li>Designates this port as</li> <li>Hot Pluggable.</li> </ul>
sSATA Port 0	[Not Installed]	
Port 0	[Enable]	
Hot Plug	[Disable]	
Spin Up Device	[Disable]	
sSATA Port 1	[Not Installed]	
Port 1	[Enable]	
Hot Plug	[Disable]	
Spin Up Device	[Disable]	
sSATA Port 2	[Not Installed]	
Port 2	[Enable]	
Hot Plug	[Disable]	
Spin Up Device	[Disable]	→+: Select Screen
sSATA Port 3	[Not Installed]	↑↓: Select Item
Port 3	[Enable]	Enter: Select
Hot Plug	[Disable]	+/-: Change Opt.
Spin Up Device	[Disable]	F1: General Help
sSATA Port 4	WDC WD4000FYYZ - 4000.7 GB	F3: Previous Values
Port 4	(Enable)	F9: Optimized Defaults
Hot Plug	[Disable]	F10: Save & Exit
Spin Up Device	[Disable]	ESC: Exit
sSATA Port 5	[Not Installed]	
Port 5	[Enable]	
		· ·

## PCH sSATA Configuration

### ☞ sSATA Controller(s)

Enable/Disable sSATA controller.

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

## ∽ Configure sSATA as

Configure on chip SATA type.

AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time.

RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allows access the RAID setup utility at boot time.

Options available: AHCI/RAID. Default setting is AHCI.

# ∽ Alternate Device ID on RAID<sup>(Note 1)</sup>

Enable/Disable Alternate Device ID on RAID mode. Options available: Enable/Disable. Default setting is **Disabled Please note that this option appears when HDD is in RAID Mode.** 

# ☞ sSATA Port 0/1/2/3/4/5

The category identifies sSATA hard drives that are installed in the computer. System will automatically detect HDD type.

# ∽ Port 0/1/2/3/4/5

Enable/Disable Port 0/1/2/3/4/5 device. Options available: Enable/Disable. Default setting is **Enable**.

## Hot Plug (for Port 0/1/2/3/4/5)<sup>(Note 2)</sup>

Enable/Disable HDD Hot-Plug function. Options available: Enable/Disable. Default setting is **Disable**.

# ∽ Spin Up Device (for Port 0/1/2/3/4/5)<sup>(Note 2)</sup>

On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device. Options available: Enable/Disable. Default setting is **Disabled** 

# 1-3-8 Miscellaneous Configuration



## ∽ Miscellaneous Configuration

### ∽ Active Video

Selects the active video type.

Options available: Auto/Onboard Device/PCIE Device. Default setting is Auto.

# 1-3-9 Server ME Configuration



- ∽ General ME Configuration
- Operational Firmware Version
   Displays Operational Firmware version information.
- ∽ ME Firmware Status #1/#2

Displays ME Firmware status information.

- Current State (for ME Firmware)
   Displays ME Firmware current status information.
- Error Code (for ME Firmware)
   Displays ME Firmware status error code.
- ∽ Recovery Cause (for ME Firmware)

Displays ME Firmware recovery cause.

→ PTT Support

Displays if the system supports the Intel® Platform Trust Technology.

# 1-3-10 Runtime Error Logging



## ∽ Runtime Error Logging

## ∽ System Errors

Enable/Disable system error logging function. Options available: Enable/Disable. Default setting is **Enable**.

## ∽ S/W Error Injection Support

Enable/Disable software injection error logging function. Options available: Enable/Disable. Default setting is **Disable**.

## ∽ Whea Settings

Press [Enter] for configuration of advanced items.

## ∽ Memory Error Enabling

Press [Enter] for configuration of advanced items.

### ∽ PCle Error Enabling

Press [Enter] for configuration of advanced items.

# 1-3-10-1 Whea Settings



# ☞ WHEA Support (Windows Hardware Error Architecture)

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

# 1-3-10-2 Memory Error Enabling



### ∽ Memory Error

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

## ∽ Memory Corrected Error

Enable/Disable Memory Corrected Error. Options available: Enable/Disable. Default setting is **Enable**.

### Uncorrected Error disable Memory

Enable/Disable the Memory that triggers Uncorrected Error. Options available: Enable/Disable. Default setting is **Disable**.

# 1-3-10-3 PCIe Error Enabling



### Corrected Error

Enables and escalates Correctable Errors to error pins. Options available: Enable/Disable. Default setting is **Enable**.

### ∽ Uncorrected Error

Enables and escalates Uncorrectable/Recoverable Errors to error pins. Options available: Enable/Disable. Default setting is **Enable**.

### ☞ Fatal Error Enable

Enables and escalates Fatal Errors to error pins. Options available: Enable/Disable. Default setting is **Enable**.

### ∽ SERR Propagation

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

### PERR Propagation

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

# 1-4 Server Management Menu

Aptio Setup Ut Main Advanced Chipset Se	ility – Copyright (C) 2017 Ame rver Mgmt <mark>Security Boot Sa</mark>	erican Megatrends, Inc. ve & Exit
FR8-2 Timer FR8-2 Timer Folicy OS Watchdog Timer OS Wit Timer Timeout OS Wit Timer Timeout OS Wit Timer Policy System Event Log Vieu FRU Information BHC network configuration FIPV5 BMC Network Configurat:	[Disabled] [6 minutes] [Do Nothing] [Disabled] [10 minutes] [Reset]	Enable or Disable FRB-2 timer(FOST timer) +*: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F1: Save & Kuit ESC: Exit
Vencion 2 19	1969 Popunight (P) 2017 Amon	ican Magathanda The

### ☞ FRB-2 Timer

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

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.

∽ 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.

# 1-4-1 System Event Log



## C 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**.

# Contraction 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**.

# 1-4-2 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.



# 1-4-3 BMC Network Configuration



## ∽ Select NCSI and Dedicated LAN

Switch NCSI and dedicated LAN and send KCS command. Options available: Do Nothing/Mode1 (Dedicated)/Mode2(NSCI)/Mode3 (Failover). Default setting is **Mode1 (Dedicated)**.

### Lan Channel 1

### Configuration Address source

Select to configure LAN channel parameters statically or dynamically (DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase.

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

### ∽ 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.

# 1-4-4 IPv6 BMC Network Configuration



## ∽ IPv6 BMC Lan Channel 1

## ☞ IPv6 BMC Lan Option

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

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

## → IPv6 BMC Lan IP Address/Prefix Length -> [1999::11/64]

Check if the IPv6 BMC LAN IP address matches those displayed on the screen.

# 1-5 Security Menu

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

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Main Advanced Chipset Server Mgmt <mark>Security</mark> Boot Save & Exit		
Password Description		Set Administrator Password
If ONLY the Administrato then this only limits ac only asked for when ente If ONLY the User's passus is a power on password a boot or enter Setup. In have Administrator right The password length must	r's password is set, cess to Setup and is ring Setup. ord is set, then this nd must be entered to Setup the User will S. be	
Minimum length	3	
Maximum length	20	
Administrator Password User Password ▶ Secure Boot		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
	10 1060 Conunight (C) 2017	American Magataanda Taa

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.
### 1-5-1 Secure Boot

The Secure Boot submenu is applicable when your device is installed the Windows® 8 (or above) operating system.

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Security			
System Mode Secure Boot Vendor Keys Attempt Secure I Secure Boot Mod ▶ Key Management	Boot	Setup Not Active Active [Disabled] [Custom]	Secure Boot activated when Platform Key(PK) is enrolled, System mode is User/Deployed, and CSM function is disabled
		++: Select : T4: Select Enter: Sele +/-: Change F1: General F3: Previou F9: Optimiz F10: Save a ESC: Exit	++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
	Version 2.19.12	268. Copyright (C) 2017 Ame	rican Megatrend

#### ∽ 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.

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

#### ∽ Secure Boot Mode<sup>(Note)</sup>

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.

### 1-5-1-1 Key Management

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. Security		
Provision Factory Defaults • Install Factory Default keys • Enroll Efi Image • Save all Secure Boot variable	(Disabled) PS	Allow to provision factory default Secure Boot keys when System is in Setup Mode
Secure Boot variable   Size + Platform Key(PK)   0 + Key Exchange Keys   0 + Authorized Signatures   0 + Forbidden Signatures   0 + Authorized TimeStamps   0 > DSRecovery Signatures   0	Keys#  Key Source 0 No Key 0 No Key 0 No Key 0 No Key 0 No Key 0 No Key 0 No Key	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit
Venelen 2 10	269 Conunight (C) 2017 Amor	ican Magathanda Inc

#### 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.

#### Control 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.

# 1-6 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 Bootup NumLock State	1 [0n]	Number of seconds to wait for setup activation key. 65535(0xFFFF) means
Boot mode select	(UEFI)	indefinite waiting.
FIXED BOOT ORDER Priorities Boot Option #1 Boot Option #2 Boot Option #3	(Herd Disk) (CD/DVD) (USB Device)	
Boot Option #4 Boot Option #5	[Network:UEFI: PXE IP4 I] [UEFI AP:UEFI: Built-in]	++: Select Screen
▶ UEFI Application Boot Prioritie:		Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

#### Boot Configuration

#### ∽ Setup Prompt Timeout

Number of seconds to wait for setup activation key. 65535 (0xFFF) 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**.

#### Quiet Boot

Enable/Disable showing the logo during POST. Options available: Enabled/Disabled. Default setting is **Enabled**.

### ∽ 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 drive.
- 2. CD-COM/DVD drive.
- 3. USB device.
- 4. Network.
- 5. UEFI.

- UEFI Network Drive BBS Priorities
  Press [Enter] to configure the boot priority.
- UEFI Application Boot Priorities
  Press [Enter] to configure the boot priority.

## 1-6-1 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.

Aptio Setup Utility	– Copyright (C) 2017 American Meg Boot	atrends, Inc.
Boot Option #1 Boot Option #2 Boot Option #3 Boot Option #4	<pre>(UEFI: PXE IP4 Intel(R)] [UEFI: PXE IP4 Intel(R)] [UEFI: PXE IP4 Intel(R)] [UEFI: PXE IP4 Intel(R)]</pre>	Sets the system boot order ++: Select Screen 14: Select Item Enter: Select +/: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F9: Optimized Defaults F9: Sptimized Select ESC: Exit
Vancian 2 19 1269	Popunight (P) 2017 Amonican Magat	popdo Tro

## 1-6-2 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.

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc. <mark>Boot</mark>		
Boot Option #1	(UEFI: Built-in EFI Shell)	Sets the system boot order ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F3: Optimized Defaults F10: Save & Exit ESC: Exit
Venetion 0 10	1969 Convertent (C) 9017 Amonicon Howa	

# 1-7 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**.

Aptio Setup Utility – Copyright (C) 2017 American Meg Main Advanced Chipset Server Mgmt Security Boot Save & Exit	atrends, Inc.
Save Options Save Changes and Exit Discard Changes and Exit	Exit system setup after saving the changes.
Save Changes and Reset Discard Changes and Reset	
Save Changes Discard Changes	
Default Options Restore Defaults	
save as User Defaults Restore User Defaults	↔: Select Screen ↑↓: Select Item
Boot Override UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 106BASE-T	Enter: Select +/-: Change Opt.
UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 10GBASE-T UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 1GbE	F1: General Help F3: Previous Values
UEFI: PXE IP4 Intel(R) Ethernet Connection X722 for 1GbE UEFI: Built-in EFI Shell	F9: Optimized Defaults F10: Save & Exit ESC: Exit

#### ∽ 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 and Reset

Restarts the system after saving the changes made. Options available: Yes/No.

#### ∽ Discard Changes and Reset

Restarts the sysetm without saving any changes. Options available: Yes/No.

#### ∽ Save Changes

Saves changes made in the BIOS setup. Options available: Yes/No.

#### Discard Changes

Discards changes made and closes 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.

### ☞ Save as User Defaults

Saves the changes made as the user default settings. Options available: Yes/No.

### ☞ Restore User Defaults

Loads the user default settings for all BIOS setup parameters. Options available: Yes/No.

#### ∽ Boot Override

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

# 1-8 BIOS POST Codes

# 1-8-1 AMI Standard - PEI

PEI_CORE_STARTED	0x10
PEI_CAR_CPU_INIT	0x11
PEI_CAR_NB_INIT	0x15
PEI_CAR_SB_INIT	0x19
PEI_MEMORY_SPD_READ	0x2B
PEI_MEMORY_PRESENCE_DETECT	0x2C
PEI_MEMORY_TIMING	0x2D
PEI_MEMORY_CONFIGURING	0x2E
PEI_MEMORY_INIT	0x2F
PEI_MEMORY_INSTALLED	0x31
PEI_CPU_INIT	0x32
PEI_CPU_CACHE_INIT	0x33
PEI_CPU_AP_INIT	0x34
PEI_CPU_BSP_SELECT	0x35
PEI_CPU_SMM_INIT	0x36
PEI_MEM_NB_INIT	0x37
PEI_MEM_SB_INIT	0x3B
PEI_DXE_IPL_STARTED	0x4F
DXE_CORE_STARTED	0x60
//Recovery	
PEI_RECOVERY_AUTO	0xF0
PEI_RECOVERY_USER	0xF1
PEI_RECOVERY_STARTED	0xF2
PEI_RECOVERY_CAPSULE_FOUND	0xF3
PEI_RECOVERY_CAPSULE_LOADED	0xF4
//S3	
PEI_S3_STARTED	0xE0
PEI_S3_BOOT_SCRIPT	0xE1
PEI_S3_VIDEO_REPOST	0xE2
PEI_S3_OS_WAKE	0xE3

## 1-8-2 AMI Standard - DXE

DXE_CORE_STARTED	0x60
DXE_NVRAM_INIT	0x61
DXE_SBRUN_INIT	0x62
DXE_CPU_INIT	0x63
DXE_NB_HB_INIT	0x68
DXE_NB_INIT	0x69
DXE_NB_SMM_INIT	0x6A

DXE_SB_INIT	0x70
DXE_SB_SMM_INIT	0x71
DXE_SB_DEVICES_INIT	0x72
DXE_ACPI_INIT	0x78
DXE_CSM_INIT	0x79
DXE_BDS_STARTED	0x90
DXE_BDS_CONNECT_DRIVERS	0x91
DXE_PCI_BUS_BEGIN	0x92
DXE_PCI_BUS_HPC_INIT	0x93
DXE_PCI_BUS_ENUM	0x94
DXE_PCI_BUS_REQUEST_RESOURCES	0x95
DXE_PCI_BUS_ASSIGN_RESOURCES	0x96
DXE_CON_OUT_CONNECT	0x97
DXE_CON_IN_CONNECT	0x98
DXE_SIO_INIT	0x99
DXE_USB_BEGIN	0x9A
DXE_USB_RESET	0x9B
DXE_USB_DETECT	0x9C
DXE_USB_ENABLE	0x9D
DXE_IDE_BEGIN	0xA0
DXE_IDE_RESET	0xA1
DXE_IDE_DETECT	0xA2
DXE_IDE_ENABLE	0xA3
DXE_SCSI_BEGIN	0xA4
DXE_SCSI_RESET	0xA5
DXE_SCSI_DETECT	0xA6
DXE_SCSI_ENABLE	0xA7
DXE_SETUP_VERIFYING_PASSWORD	0xA8
DXE_SETUP_START	0xA9
DXE_SETUP_INPUT_WAIT	0xAB
DXE_READY_TO_BOOT	0xAD
DXE_LEGACY_BOOT	0xAE
DXE_EXIT_BOOT_SERVICES	0xAF
RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN	0xB0
RT_SET_VIRTUAL_ADDRESS_MAP_END	0xB1
DXE_LEGACY_OPROM_INIT	0xB2
DXE_RESET_SYSTEM	0xB3
DXE_USB_HOTPLUG	0xB4
DXE_PCI_BUS_HOTPLUG	0xB5
DXE_NVRAM_CLEANUP	0xB6
DXE_CONFIGURATION_RESET	0xB7

## 1-8-3 AMI Standard - ERROR

PEI_MEMORY_INVALID_TYPE	0x50
PEI_MEMORY_INVALID_SPEED	0x50
PEI_MEMORY_SPD_FAIL	0x51
PEI_MEMORY_INVALID_SIZE	0x52
PEI_MEMORY_MISMATCH	0x52
PEI_MEMORY_NOT_DETECTED	0x53
PEI_MEMORY_NONE_USEFUL	0x53
PEI_MEMORY_ERROR	0x54
PEI_MEMORY_NOT_INSTALLED	0x55
PEI_CPU_INVALID_TYPE	0x56
PEI_CPU_INVALID_SPEED	0x56
PEI_CPU_MISMATCH	0x57
PEI_CPU_SELF_TEST_FAILED	0x58
PEI_CPU_CACHE_ERROR	0x58
PEI_CPU_MICROCODE_UPDATE_FAILED	0x59
PEI_CPU_NO_MICROCODE	0x59
PEI_CPU_INTERNAL_ERROR	0x5A
PEI_CPU_ERROR	0x5A
PEI_RESET_NOT_AVAILABLE	0x5B
//Recovery	
PEI_RECOVERY_PPI_NOT_FOUND	0xF8
PEI_RECOVERY_NO_CAPSULE	0xF9
PEI_RECOVERY_INVALID_CAPSULE	0xFA
//S3 Resume	
PEI_MEMORY_S3_RESUME_FAILED	0xE8
PEI_S3_RESUME_PPI_NOT_FOUND	0xE9
PEI_S3_BOOT_SCRIPT_ERROR	0xEA
PEI_S3_OS_WAKE_ERROR	0xEB
DXE_CPU_ERROR	0xD0
DXE_NB_ERROR	0xD1
DXE_SB_ERROR	0xD2
DXE_ARCH_PROTOCOL_NOT_AVAILABLE	0xD3
DXE_PCI_BUS_OUT_OF_RESOURCES	0xD4
DXE_LEGACY_OPROM_NO_SPACE	0xD5
DXE_NO_CON_OUT	0xD6
DXE_NO_CON_IN	0xD7
DXE_INVALID_PASSWORD	0xD8
DXE_BOOT_OPTION_LOAD_ERROR	0xD9
DXE_BOOT_OPTION_FAILED	0xDA
DXE_FLASH_UPDATE_FAILED	0xDB
DXE_RESET_NOT_AVAILABLE	0xDC

# 1-8-4 Intel UPI POST Codes

Initialize KTIRC inuput structure default values	0xA0
Collect info such as SBSP, Boot Mode, Reset type etc	0xA1
Setup IO SADs in SBSP to access the config space	0xA2
Setup up minimum path between SBSP & other sockets	0xA3
Add the node to the tree	
Parse the LEP of the discovered socket	
Check if the system has the supported topology	
Setup the boot path for the parent which is not	
directly connected to Legacy CPU	
Setup path from SBSP to the new found node	
Setup IO SADs in PBSP to access the config space	0xA4
System configurations that require some kind of reset	0xA5
Sync up with PBSPs	0xA6
Topology discovery and route calculation	0xA7
Program final route	0xA8
Program final IO SAD setting	0xA9
Protocol layer and other Uncore settings	0xAA
Transition links to full speed opeartion	0xAB
Phy layer settings	0xAC
Link layer settings	0xAD
Coherency Settings	0xAE
KTIRC is done	0xAF

## 1-8-5 Intel UPI Error Codes

When system BSP tries to setup path for remote sockets or sends a Boot_Go command to remote socket in SetupSbspPathToAllSockets() or SyncUpPbspForReset(). If the remote socket(s) hasn't checked-in, assert; it is a fatal condition, this error will be logged. No retry. <i>RC Behavior: System Halt</i>	0xD8
When SBSP tries to add this remote socket into system topology tree in SetupSbspPathToAllSockets(), there are some errors occur in the data structure. No retry. <i>RC Behavior: The current Socket is not added to the tree.</i> When SBSP setups the boot path for the parent which is not directly connected to Legacy CPU in SetupSbspPathToAllSockets(). The Child is not an immediate neighbor of Parent. No retry.	0xDA
SAD setup error RC Behavior: System Halt	0xDB

Unsupported topology RC Behavior: System Halt	0xDC
SBSP cannot find KPIRC TXEQ Parameters for this link in GetSocketLinkEparams(). No retry. <i>RC Behavior: System Halt</i>	0xDD

### 1-8-6 Intel MRC POST Codes

Detect DIMM population	0xB0
Set DDR frequency	0xB1
Gather remaining SPD data	0xB2
Program registers on the memory controller level	0xB3
Evaluate RAS modes and save rank information	0xB4
Program registers on the channel level	0xB5
DDRIO Initialization	0xB6
Train DDR	0xB7
Initialize CLTT/OLTT	0xB8
Hardware memory test and init	0xB9
Execute memory init	0xBA
Program memory map and interleaving	0xBB
Program RAS configuration	0xBC
Rank margin tool	0xBD
MRC is done	0xBF

# 1-8-7 Intel MRC Error Codes

No memory was detected	0xE8	
Memory test failure	0xEB	
Different dimm types are detected installed in the system	0xED	
Number of HAs found in system greater than	0xEE	
MAX_HA defined in MRC build		
Indicates a CLTT table structure error	0xEF	
Invalid VR mode, unable to set DRAM VDD	0xF0	
Failure occurred reserving memory for IOT	0xF1	
Reference code assert	0xF2	
Unsupported MC frequency set	0xF3	
Unable to get current MC frequency	0xF4	

# 1-8-8 Intel PM POST Codes

Start of PPM structure initialization	0xD0
PPM CSR programming	0xD1
PPM MSR programming	0xD2
Start of PState transition init	0xD3
PPM exit	0xD4
PPM On ready to boot event	0xD5

# 1-8-8 Intel PM POST Codes

Start of IIO early Initialization	0xE0
Pre Link training	0xE1
Start of Gen3 EQ training	0xE2
Start of PState transition init	0xE3
Gen3 parameters override	0xE4
End of IIO Early Initialization	0xE5
Start of IIO Late initialization	0xE6
PCIE port initialization	0xE7
IOAPIC initialization	0xE8
VTD initialization	0xE9
IOAT initialization	0xEA
DFX initialization	0xEB
NTB initialization	0xEC
Security Initialization	0xED
IIO late initialization	0xEE
IIO On ready to boot event	0xEF

# 1-9 BIOS POST Beep code (AMI standard)

# 1-9-1 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

## 1-9-2 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	

# 1-10 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.

Main Advanced Chinest Security	Blas Setup Genver Hant	Utility Deet Loss		a tat	100200000
ROM Inversional a loved ROM Inversion verification passed Flash Update Parameters Repet Andren Main Book Indek F fructed with flash update	DEnos Java Otrada SavaD Otrada SavaD		80: 501	iect shijs letu	to otare flash
			44 14 16 17 17 17 17 17 17 17 17 17 17 17 17 17	: Select Select Select Change Change Change Select Previou Oniologi Select Select	Screen Tree Cd. JM(2p) s Valuats d Defaults - Evilt