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 Setup ........................................................................................................5
  1-1 The Main Menu ........................................................................................................... 7
  1-2 Advanced 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 Chipset 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
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3-7-2</td>
<td>PCH sSATA Configuration</td>
<td>58</td>
</tr>
<tr>
<td>1-3-8</td>
<td>Miscellaneous Configuration</td>
<td>60</td>
</tr>
<tr>
<td>1-3-9</td>
<td>Server ME Configuration</td>
<td>61</td>
</tr>
<tr>
<td>1-3-10</td>
<td>Runtime Error Logging</td>
<td>62</td>
</tr>
<tr>
<td>1-3-10-1</td>
<td>Whea Settings</td>
<td>63</td>
</tr>
<tr>
<td>1-3-10-2</td>
<td>Memory Error Enabling</td>
<td>64</td>
</tr>
<tr>
<td>1-3-10-3</td>
<td>PCIe Error Enabling</td>
<td>65</td>
</tr>
<tr>
<td>1-4</td>
<td>Server Management Menu</td>
<td>66</td>
</tr>
<tr>
<td>1-4-1</td>
<td>System Event Log</td>
<td>68</td>
</tr>
<tr>
<td>1-4-2</td>
<td>View FRU Information</td>
<td>69</td>
</tr>
<tr>
<td>1-4-3</td>
<td>BMC Network Configuration</td>
<td>70</td>
</tr>
<tr>
<td>1-4-4</td>
<td>IPv6 BMC Network Configuration</td>
<td>71</td>
</tr>
<tr>
<td>1-5</td>
<td>Security Menu</td>
<td>72</td>
</tr>
<tr>
<td>1-5-1</td>
<td>Secure Boot</td>
<td>73</td>
</tr>
<tr>
<td>1-5-1-1</td>
<td>Key Management</td>
<td>74</td>
</tr>
<tr>
<td>1-6</td>
<td>Boot Menu</td>
<td>76</td>
</tr>
<tr>
<td>1-6-1</td>
<td>UEFI NETWORK Drive BBS Priorities</td>
<td>78</td>
</tr>
<tr>
<td>1-6-2</td>
<td>UEFI Application Boot Priorities</td>
<td>79</td>
</tr>
<tr>
<td>1-7</td>
<td>Save &amp; Exit Menu</td>
<td>80</td>
</tr>
<tr>
<td>1-8</td>
<td>BIOS POST Codes</td>
<td>82</td>
</tr>
<tr>
<td>1-8-1</td>
<td>AMI Standard - PEI</td>
<td>82</td>
</tr>
<tr>
<td>1-8-2</td>
<td>AMI Standard - DXE</td>
<td>82</td>
</tr>
<tr>
<td>1-8-3</td>
<td>AMI Standard - ERROR</td>
<td>84</td>
</tr>
<tr>
<td>1-8-4</td>
<td>Intel UPI POST Codes</td>
<td>85</td>
</tr>
<tr>
<td>1-8-5</td>
<td>Intel UPI Error Codes</td>
<td>85</td>
</tr>
<tr>
<td>1-8-6</td>
<td>Intel MRC POST Codes</td>
<td>86</td>
</tr>
<tr>
<td>1-8-7</td>
<td>Intel MRC Error Codes</td>
<td>86</td>
</tr>
<tr>
<td>1-8-8</td>
<td>Intel PM POST Codes</td>
<td>87</td>
</tr>
<tr>
<td>1-9</td>
<td>BIOS POST Beep code (AMI standard)</td>
<td>88</td>
</tr>
<tr>
<td>1-9-1</td>
<td>PEI Beep Codes</td>
<td>88</td>
</tr>
<tr>
<td>1-9-2</td>
<td>DXE Beep Codes</td>
<td>88</td>
</tr>
<tr>
<td>1-10</td>
<td>BIOS Recovery Instruction</td>
<td>89</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Key</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;←→&gt;</td>
<td>Move the selection bar to select the screen</td>
</tr>
<tr>
<td>↑↓←→</td>
<td>Move the selection bar to select an item</td>
</tr>
<tr>
<td>↔</td>
<td>Increase the numeric value or make changes</td>
</tr>
<tr>
<td>←→</td>
<td>Decrease the numeric value or make changes</td>
</tr>
<tr>
<td>&lt;Enter&gt;</td>
<td>Execute command or enter the submenu</td>
</tr>
<tr>
<td>&lt;Esc&gt;</td>
<td>Main Menu: Exit the BIOS Setup program Submenus: Exit current submenu</td>
</tr>
<tr>
<td>&lt;F1&gt;</td>
<td>Show descriptions of general help</td>
</tr>
<tr>
<td>&lt;F3&gt;</td>
<td>Restore the previous BIOS settings for the current submenus</td>
</tr>
<tr>
<td>&lt;F9&gt;</td>
<td>Load the Optimized BIOS default settings for the current submenus</td>
</tr>
<tr>
<td>&lt;F10&gt;</td>
<td>Save all the changes and exit the BIOS Setup program</td>
</tr>
</tbody>
</table>
- 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.
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.

Processor Information
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\(^{(Note)}\)
Displays the total memory size of the installed memory.

Memory Frequency\(^{(Note)}\)
Displays the frequency information of the installed memory.
Onboard LAN Information

- 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.

(Note) Functions available on selected models.
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.
**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

Press [Enter] to manage Intel® Virtual RAID on the CPU.
1-2-3  Intel(R) Ethernet Connection X722

**NIC Configuration**

- **BIOS**: 0
- **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**: 37D2
- **PCI Address**: 1A:00:01
- **Link Status**: [Disconnected]
- **MAC Address**: 10:1B:00:0E:02:13
- **Virtual MAC Address**: 00:00:00:00:00:00

Click to configure the network device port.

++: Select Screen
11: 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.

**UEFI Driver**

Displays the technical specifications for the Network Interface Controller.
- Adapter PBA
  Displays the technical specifications for the Network Interface Controller.
- Device Name
  Displays the technical specifications for the Network Interface Controller.
- Chip Type
  Displays the technical specifications for the Network Interface Controller.
- PCI Device ID
  Displays the technical specifications for the Network Interface Controller.
- PCI Address
  Displays the technical specifications for the Network Interface Controller.
- Link Status
  Displays the technical specifications for the Network Interface Controller.
- MAC Address
  Displays the technical specifications for the Network Interface Controller.
- Virtual MAC Address
  Displays the technical specifications for the Network Interface Controller.
1-2-3-1 NIC Configuration

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>[Auto Negotiated]</th>
</tr>
</thead>
</table>

| Wake On LAN | [Enabled] |

- **Link Speed**
  Allows for automatic link speed adjustment. Default setting is **Auto Negotiated**.

- **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

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

COM1/COM2 Serial Over LAN Console Redirection
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
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.
## BIOS Setup

### Console Redirection Settings

#### COM1

<table>
<thead>
<tr>
<th>Terminal Type</th>
<th>[ANSI]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>115200</td>
</tr>
<tr>
<td>Data Bits</td>
<td>[8]</td>
</tr>
<tr>
<td>Parity</td>
<td>[None]</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>[1]</td>
</tr>
<tr>
<td>Flow Control</td>
<td>[None]</td>
</tr>
<tr>
<td>VT-UTF8 Combo Key Support</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Recorder Mode</td>
<td>[Disabled]</td>
</tr>
<tr>
<td>Resolution 100x31</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Legacy OS Redirection Resolution</td>
<td>[80x24]</td>
</tr>
<tr>
<td>Putty KeyPad</td>
<td>[VT100]</td>
</tr>
<tr>
<td>Redirection After BIOS POST</td>
<td>[Always Enable]</td>
</tr>
</tbody>
</table>

Emulation: ANSI Extended ASCII char set. VT100:
ASCII char set. VT100+: extends VT100 to support color, function keys, etc.
VT-UTF8: uses UTF8 encoding to map unicode chars onto 1 or more bytes.

++: Select Screen
11: Select Item
Enter: Select
+/ -: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

---

#### COM2/Serial Over LAN

<table>
<thead>
<tr>
<th>Terminal Type</th>
<th>[ANSI]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>115200</td>
</tr>
<tr>
<td>Data Bits</td>
<td>[8]</td>
</tr>
<tr>
<td>Parity</td>
<td>[None]</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>[1]</td>
</tr>
<tr>
<td>Flow Control</td>
<td>[None]</td>
</tr>
<tr>
<td>VT-UTF8 Combo Key Support</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Recorder Mode</td>
<td>[Disabled]</td>
</tr>
<tr>
<td>Resolution 100x31</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Legacy OS Redirection Resolution</td>
<td>[80x24]</td>
</tr>
<tr>
<td>Putty KeyPad</td>
<td>[VT100]</td>
</tr>
<tr>
<td>Redirection After BIOS POST</td>
<td>[Always Enable]</td>
</tr>
</tbody>
</table>

Emulation: ANSI Extended ASCII char set. VT100:
ASCII char set. VT100+: extends VT100 to support color, function keys, etc.
VT-UTF8: uses UTF8 encoding to map unicode chars onto 1 or more bytes.

++: Select Screen
11: Select Item
Enter: Select
+/ -: Change Opt.
F1: General Help
F3: Previous Values
F9: 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 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
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
Enable/Disable extended terminal resolution.
Options available: Enabled/Disabled. Default setting is Enabled.

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

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

Redirection After BIOS POST
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 Emergency 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.

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

1-2-6  SIO Configuration

AMI SIO Driver Version: 65.07.03

Super IO Chip Logical Device(s) Configuration
- [Active:] Serial Port 1
- [Active:] Serial Port 2

WARNING: Logical Devices state on the left side of the control...

++: Select Screen
#1: Select Item
Enter: Select
+/ -: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit

Serial Port 1 Configuration

Use This Device: [Enabled]
Logical Device Settings:
Current: IO=3F8h; IRQ=4;
Possible: [Use Automatic Settings]

WARNING: Disabling SIO Logical Devices may have unwanted side...

++: Select Screen
#1: Select Item
Enter: Select
+/ -: Change Opt.
F1: General Help
F3: Previous Values
F9: Optimized Defaults
F10: Save & Exit
ESC: Exit
**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;
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

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

Onboard LAN #1/#2/#3/#4 I/O ROM (Note)
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.

(Note) Functions available on selected models.
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**.

- **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**.
## 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**.

### 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.

**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.

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

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.

- **USB Mass Storage Driver Support**
  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.

*(Note)* This item is present only if you attach USB devices.
### 1-2-13 Chipset Configuration

<table>
<thead>
<tr>
<th>BIOS Setup Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore AC Power Loss</td>
<td>[Last State]</td>
<td>Specifies the state when power is reapplied after a power failure (GD state).</td>
</tr>
<tr>
<td>Chassis Opened Warning</td>
<td>[Disabled]</td>
<td>Enables/disables the chassis intrusion alarm function.</td>
</tr>
</tbody>
</table>

**Restore on AC Power Loss**  *(Note)*

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 alarm function.

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

*(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.
## Processor Configuration

### Pre-Socket Configuration

Press [Enter] for configuration of advanced items.

### Processor Socket/Processor ID/Processor Frequency/Processor Max Ratio/Processor Min Ratio/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 or disables 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
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 Configuration

Core Disable Bitmap(Hex) 0

CPU Socket 1 Configuration

0: Enable all cores.
FFFFFFFF: Disable all cores
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. FFFFFFFF 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

UPI Configuration
- UPI General Configuration

UPI General Configuration
- Link Frequency Select [Auto]

UPI Status
- UPI Status Help

Key Functions:
****: Select Screen
****: 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

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.

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.
I/O Configuration

Intel® VT for Directed I/O (VT-d)
Press [Enter] for configuration of advanced items.

Intel® 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)**
  - 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.

- **ACCS 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.

- **PassThrough DMA**
  - 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 Support (Non-Isoch)**
  - Enable/Disable Non-Isoch VT_D Engine Coherency support.
  - Options available: Enable/Disable. Default setting is Enable.
1-3-5-2 Intel® VMD Technology

먼저 Intel® VMD 기술

먼저 Intel® VMD 구성

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

- **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

Hardware P-States

<table>
<thead>
<tr>
<th>Description</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable: Hardware chooses a P-state based on OS Request (Legacy P-States)</td>
<td>Disable/Native Mode/Out of Band Mode/Native Mode with No Legacy Support.</td>
</tr>
<tr>
<td>Native Mode: Hardware chooses a P-state based on OS guidance.</td>
<td>Default setting is Native Mode.</td>
</tr>
<tr>
<td>Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance)</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>CPU C State Control</th>
<th>Autonomous Core C-State</th>
<th>CPU C6 report</th>
<th>Enhanced Halt State (C1E)</th>
<th>OS ACPI Cx</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Disable]</td>
<td>[Auto]</td>
<td>[Enable]</td>
<td>(ACPI C2)</td>
</tr>
</tbody>
</table>

**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**.

**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**.

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

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.

(Note) Advanced items prompt when this item is set to BIOS Controls EPB.
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 allowed access the RAID setup utility at boot time.

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

› Alternate Device ID on RAID (Note 1)
  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) (Note 2)
  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) (Note 2)
  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.

(Note 1) Only appears when HDD sets to RAID Mode.
(Note 2) Only supported when HDD is in AHCI or RAID Mode.
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 allowed access the RAID setup utility at boot time.
Options available: AHCI/RAID. Default setting is AHCI.

○ Alternate Device ID on RAID (Note 1)
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.

○ ssSATA Port 0/1/2/3/4/5
The category identifies ssSATA 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) (Note 2)
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) (Note 2)
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

(Note 1) Only appears when HDD sets to RAID Mode.
(Note 2) Only supported when HDD is in AHCI or RAID Mode.
1-3-8  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

- **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

Enabling/Disabling Options

SEL Components [Enabled]

Erasing Settings

Erase SEL [No]
When SEL is Full [Do Nothing]

Custom EFI Logging Options

Log EFI Status Codes [Error code]

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

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

Erase 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.

<table>
<thead>
<tr>
<th>FRU Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Manufacturer</td>
<td>GIGABYTE</td>
</tr>
<tr>
<td>System Product Name</td>
<td>MD71-HB0-00</td>
</tr>
<tr>
<td>System Version</td>
<td>0100</td>
</tr>
<tr>
<td>System Serial Number</td>
<td>01234567890123456789NB</td>
</tr>
<tr>
<td>Board Manufacturer</td>
<td>GIGABYTE</td>
</tr>
<tr>
<td>Board Product Name</td>
<td>MD71-HB0-00</td>
</tr>
<tr>
<td>Board Version</td>
<td>01234567</td>
</tr>
<tr>
<td>Board Serial Number</td>
<td>51750300004</td>
</tr>
<tr>
<td>Chassis Manufacturer</td>
<td>GIGABYTE</td>
</tr>
<tr>
<td>Chassis Product Name</td>
<td>01234567</td>
</tr>
<tr>
<td>Chassis Serial Number</td>
<td>01234567890123456789NB</td>
</tr>
</tbody>
</table>

(Note) The model name will vary depends on the product you purchased.
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 digits, 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.
**IPv6 BMC Network Configuration**

- **IPv6 BMC Lan Channel 1**
- **IPv6 BMC Lan Option**
  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.

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.

- **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** *(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.*
1-5-1-1 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.
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
  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.

- 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 sequence:
  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.
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.
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.

- **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 system 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

<table>
<thead>
<tr>
<th>PEI Module</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEI_CORE_STARTED</td>
<td>0x10</td>
</tr>
<tr>
<td>PEI_CAR_CPU_INIT</td>
<td>0x11</td>
</tr>
<tr>
<td>PEI_CAR_NB_INIT</td>
<td>0x15</td>
</tr>
<tr>
<td>PEI_CAR_SB_INIT</td>
<td>0x19</td>
</tr>
<tr>
<td>PEI_MEMORY_SPD_READ</td>
<td>0x2B</td>
</tr>
<tr>
<td>PEI_MEMORY_PRESENCE_DETECT</td>
<td>0x2C</td>
</tr>
<tr>
<td>PEI_MEMORY_TIMING</td>
<td>0x2D</td>
</tr>
<tr>
<td>PEI_MEMORY_CONFIGURING</td>
<td>0x2E</td>
</tr>
<tr>
<td>PEI_MEMORY_INIT</td>
<td>0x2F</td>
</tr>
<tr>
<td>PEI_MEMORY_INSTALLED</td>
<td>0x31</td>
</tr>
<tr>
<td>PEI_CPU_INIT</td>
<td>0x32</td>
</tr>
<tr>
<td>PEI_CPU_CACHE_INIT</td>
<td>0x33</td>
</tr>
<tr>
<td>PEI_CPU_AP_INIT</td>
<td>0x34</td>
</tr>
<tr>
<td>PEI_CPU_BSP_SELECT</td>
<td>0x35</td>
</tr>
<tr>
<td>PEI_CPU_SMM_INIT</td>
<td>0x36</td>
</tr>
<tr>
<td>PEI_MEM_NB_INIT</td>
<td>0x37</td>
</tr>
<tr>
<td>PEI_MEM_SB_INIT</td>
<td>0x3B</td>
</tr>
<tr>
<td>PEI_DXE_IPL_STARTED</td>
<td>0x4F</td>
</tr>
<tr>
<td>DXE_CORE_STARTED</td>
<td>0x60</td>
</tr>
</tbody>
</table>

#### Recovery

<table>
<thead>
<tr>
<th>PEI Module</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEI_RECOVERY_AUTO</td>
<td>0xF0</td>
</tr>
<tr>
<td>PEI_RECOVERY_USER</td>
<td>0xF1</td>
</tr>
<tr>
<td>PEI_RECOVERY_STARTED</td>
<td>0xF2</td>
</tr>
<tr>
<td>PEI_RECOVERY_CAPSULE_FOUND</td>
<td>0xF3</td>
</tr>
<tr>
<td>PEI_RECOVERY_CAPSULE_LOADED</td>
<td>0xF4</td>
</tr>
</tbody>
</table>

#### S3

<table>
<thead>
<tr>
<th>PEI Module</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEI_S3_STARTED</td>
<td>0xE0</td>
</tr>
<tr>
<td>PEI_S3_BOOT_SCRIPT</td>
<td>0xE1</td>
</tr>
<tr>
<td>PEI_S3_VIDEO_REPOST</td>
<td>0xE2</td>
</tr>
<tr>
<td>PEI_S3_O S_WAKE</td>
<td>0xE3</td>
</tr>
</tbody>
</table>

### 1-8-2 AMI Standard - DXE

<table>
<thead>
<tr>
<th>DXE Module</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>DXE_CORE_STARTED</td>
<td>0x60</td>
</tr>
<tr>
<td>DXE_NVRAM_INIT</td>
<td>0x61</td>
</tr>
<tr>
<td>DXE_SBRUN_INIT</td>
<td>0x62</td>
</tr>
<tr>
<td>DXE_CPU_INIT</td>
<td>0x63</td>
</tr>
<tr>
<td>DXE_NB_HB_INIT</td>
<td>0x68</td>
</tr>
<tr>
<td>DXE_NB_INIT</td>
<td>0x69</td>
</tr>
<tr>
<td>DXE_NB_SMM_INIT</td>
<td>0x6A</td>
</tr>
<tr>
<td>Function</td>
<td>Address</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>DXE_SB_INIT</td>
<td>0x70</td>
</tr>
<tr>
<td>DXE_SB_SMM_INIT</td>
<td>0x71</td>
</tr>
<tr>
<td>DXE_SB_DEVICES_INIT</td>
<td>0x72</td>
</tr>
<tr>
<td>DXE_ACPI_INIT</td>
<td>0x78</td>
</tr>
<tr>
<td>DXE_CSM_INIT</td>
<td>0x79</td>
</tr>
<tr>
<td>DXE_BDS_STARTED</td>
<td>0x90</td>
</tr>
<tr>
<td>DXE_BDS_CONNECT_DRIVERS</td>
<td>0x91</td>
</tr>
<tr>
<td>DXE_PCI_BUS_BEGIN</td>
<td>0x92</td>
</tr>
<tr>
<td>DXE_PCI_BUS_HPC_INIT</td>
<td>0x93</td>
</tr>
<tr>
<td>DXE_PCI_BUS_ENUM</td>
<td>0x94</td>
</tr>
<tr>
<td>DXE_PCI_BUS_REQUEST_RESOURCES</td>
<td>0x95</td>
</tr>
<tr>
<td>DXE_PCI_BUS_ASSIGN_RESOURCES</td>
<td>0x96</td>
</tr>
<tr>
<td>DXE_CON_OUT_CONNECT</td>
<td>0x97</td>
</tr>
<tr>
<td>DXE_CON_IN_CONNECT</td>
<td>0x98</td>
</tr>
<tr>
<td>DXE_SIO_INIT</td>
<td>0x99</td>
</tr>
<tr>
<td>DXE_USB_BEGIN</td>
<td>0x9A</td>
</tr>
<tr>
<td>DXE_USB_RESET</td>
<td>0x9B</td>
</tr>
<tr>
<td>DXE_USB_DETECT</td>
<td>0x9C</td>
</tr>
<tr>
<td>DXE_USB_ENABLE</td>
<td>0x9D</td>
</tr>
<tr>
<td>DXE_IDE_BEGIN</td>
<td>0xA0</td>
</tr>
<tr>
<td>DXE_IDE_RESET</td>
<td>0xA1</td>
</tr>
<tr>
<td>DXE_IDE_DETECT</td>
<td>0xA2</td>
</tr>
<tr>
<td>DXE_IDE_ENABLE</td>
<td>0xA3</td>
</tr>
<tr>
<td>DXE_SCSI_BEGIN</td>
<td>0xA4</td>
</tr>
<tr>
<td>DXE_SCSI_RESET</td>
<td>0xA5</td>
</tr>
<tr>
<td>DXE_SCSI_DETECT</td>
<td>0xA6</td>
</tr>
<tr>
<td>DXE_SCSI_ENABLE</td>
<td>0xA7</td>
</tr>
<tr>
<td>DXE_SETUP_VERIFYING_PASSWORD</td>
<td>0xA8</td>
</tr>
<tr>
<td>DXE_SETUP_START</td>
<td>0xA9</td>
</tr>
<tr>
<td>DXE_SETUP_INPUT_WAIT</td>
<td>0xAB</td>
</tr>
<tr>
<td>DXE_READY_TO_BOOT</td>
<td>0xAD</td>
</tr>
<tr>
<td>DXE_LEGACY_BOOT</td>
<td>0xAE</td>
</tr>
<tr>
<td>DXE_EXIT_BOOT_SERVICES</td>
<td>0xAF</td>
</tr>
<tr>
<td>RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN</td>
<td>0xB0</td>
</tr>
<tr>
<td>RT_SET_VIRTUAL_ADDRESS_MAP_END</td>
<td>0xB1</td>
</tr>
<tr>
<td>DXE_LEGACY_OPROM_INIT</td>
<td>0xB2</td>
</tr>
<tr>
<td>DXE_RESET_SYSTEM</td>
<td>0xB3</td>
</tr>
<tr>
<td>DXE_USB_HOTPLUG</td>
<td>0xB4</td>
</tr>
<tr>
<td>DXE_PCI_BUS_HOTPLUG</td>
<td>0xB5</td>
</tr>
<tr>
<td>DXE_NVRAM_CLEANUP</td>
<td>0xB6</td>
</tr>
<tr>
<td>DXE_CONFIGURATION_RESET</td>
<td>0xB7</td>
</tr>
<tr>
<td>Error Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>0x050</td>
<td>PEI_MEMORY_INVALID_TYPE</td>
</tr>
<tr>
<td>0x050</td>
<td>PEI_MEMORY_INVALID_SPEED</td>
</tr>
<tr>
<td>0x051</td>
<td>PEI_MEMORY_SPD_FAIL</td>
</tr>
<tr>
<td>0x052</td>
<td>PEI_MEMORY_INVALID_SIZE</td>
</tr>
<tr>
<td>0x052</td>
<td>PEI_MEMORY_MISMATCH</td>
</tr>
<tr>
<td>0x053</td>
<td>PEI_MEMORY_NOT_DETECTED</td>
</tr>
<tr>
<td>0x053</td>
<td>PEI_MEMORY_NONE_USEFUL</td>
</tr>
<tr>
<td>0x054</td>
<td>PEI_MEMORY_ERROR</td>
</tr>
<tr>
<td>0x055</td>
<td>PEI_MEMORY_NOT_INSTALLED</td>
</tr>
<tr>
<td>0x056</td>
<td>PEI_CPU_INVALID_TYPE</td>
</tr>
<tr>
<td>0x056</td>
<td>PEI_CPU_INVALID_SPEED</td>
</tr>
<tr>
<td>0x057</td>
<td>PEI_CPU_MISMATCH</td>
</tr>
<tr>
<td>0x058</td>
<td>PEI_CPU_SELF_TEST_FAILED</td>
</tr>
<tr>
<td>0x058</td>
<td>PEI_CPU_CACHE_ERROR</td>
</tr>
<tr>
<td>0x059</td>
<td>PEI_CPU_MICROCODE_UPDATE_FAILED</td>
</tr>
<tr>
<td>0x059</td>
<td>PEI_CPU_NO_MICROCODE</td>
</tr>
<tr>
<td>0x05A</td>
<td>PEI_CPU_INTERNAL_ERROR</td>
</tr>
<tr>
<td>0x05A</td>
<td>PEI_CPU_ERROR</td>
</tr>
<tr>
<td>0x05B</td>
<td>PEI_RESET_NOT_AVAILABLE</td>
</tr>
<tr>
<td>0x0F8</td>
<td>PEI_RECOVERY_PPI_NOT_FOUND</td>
</tr>
<tr>
<td>0x0F9</td>
<td>PEI_RECOVERY_NO_CAPSULE</td>
</tr>
<tr>
<td>0x0FA</td>
<td>PEI_RECOVERY_INVALID_CAPSULE</td>
</tr>
<tr>
<td>0x0E8</td>
<td>PEI_MEMORY_S3_RESUME_FAILED</td>
</tr>
<tr>
<td>0x0E9</td>
<td>PEI_S3_RESUME_PPI_NOT_FOUND</td>
</tr>
<tr>
<td>0x0EA</td>
<td>PEI_S3_BOOT_SCRIPT_ERROR</td>
</tr>
<tr>
<td>0x0EB</td>
<td>PEI_S3_OS_WAKE_ERROR</td>
</tr>
<tr>
<td>0x0D0</td>
<td>DXE_CPU_ERROR</td>
</tr>
<tr>
<td>0x0D1</td>
<td>DXE_NB_ERROR</td>
</tr>
<tr>
<td>0x0D2</td>
<td>DXE_SB_ERROR</td>
</tr>
<tr>
<td>0x0D3</td>
<td>DXE_ARCH_PROTOCOL_NOT_AVAILABLE</td>
</tr>
<tr>
<td>0x0D4</td>
<td>DXE_PCI_BUS_OUT_OF_RESOURCES</td>
</tr>
<tr>
<td>0x0D5</td>
<td>DXE_LEGACY_OPROM_NO_SPACE</td>
</tr>
<tr>
<td>0x0D6</td>
<td>DXE_NO_CON_OUT</td>
</tr>
<tr>
<td>0x0D7</td>
<td>DXE_NO_CON_IN</td>
</tr>
<tr>
<td>0x0D8</td>
<td>DXE_INVALID_PASSWORD</td>
</tr>
<tr>
<td>0x0D9</td>
<td>DXE_BOOT_OPTION_LOAD_ERROR</td>
</tr>
<tr>
<td>0x0DA</td>
<td>DXE_BOOT_OPTION_FAILED</td>
</tr>
<tr>
<td>0x0DB</td>
<td>DXE_FLASH_UPDATE_FAILED</td>
</tr>
<tr>
<td>0x0DC</td>
<td>DXE_RESET_NOT_AVAILABLE</td>
</tr>
</tbody>
</table>
### 1-8-4 Intel UPI POST Codes

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

### 1-8-5 Intel UPI Error Codes

<table>
<thead>
<tr>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>0xD8</td>
</tr>
<tr>
<td>RC Behavior: System Halt</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>0xDA</td>
</tr>
<tr>
<td>RC Behavior: The current Socket is not added to the tree.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>SAD setup error</td>
<td>0xDB</td>
</tr>
<tr>
<td>RC Behavior: System Halt</td>
<td></td>
</tr>
</tbody>
</table>
### 1-8-6 Intel MRC POST Codes

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

### 1-8-7 Intel MRC Error Codes

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

Unsupported topology

**RC Behavior: System Halt**

SBSP cannot find KPIRC TXEQ Parameters for this link in GetSocketLinkEparams(). No retry.

**RC Behavior: System Halt**

### 1-8-8 Intel PM POST Codes

<table>
<thead>
<tr>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of PPM structure initialization</td>
<td>0xD0</td>
</tr>
<tr>
<td>PPM CSR programming</td>
<td>0xD1</td>
</tr>
<tr>
<td>PPM MSR programming</td>
<td>0xD2</td>
</tr>
<tr>
<td>Start of PState transition init</td>
<td>0xD3</td>
</tr>
<tr>
<td>PPM exit</td>
<td>0xD4</td>
</tr>
<tr>
<td>PPM On ready to boot event</td>
<td>0xD5</td>
</tr>
</tbody>
</table>

### 1-8-8 Intel PM POST Codes

<table>
<thead>
<tr>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of IIO early Initialization</td>
<td>0xE0</td>
</tr>
<tr>
<td>Pre Link training</td>
<td>0xE1</td>
</tr>
<tr>
<td>Start of Gen3 EQ training</td>
<td>0xE2</td>
</tr>
<tr>
<td>Start of PState transition init</td>
<td>0xE3</td>
</tr>
<tr>
<td>Gen3 parameters override</td>
<td>0xE4</td>
</tr>
<tr>
<td>End of IIO Early Initialization</td>
<td>0xE5</td>
</tr>
<tr>
<td>Start of IIO Late initialization</td>
<td>0xE6</td>
</tr>
<tr>
<td>PCIE port initialization</td>
<td>0xE7</td>
</tr>
<tr>
<td>IOAPIC initialization</td>
<td>0xE8</td>
</tr>
<tr>
<td>VTD initialization</td>
<td>0xE9</td>
</tr>
<tr>
<td>IOAT initialization</td>
<td>0xEA</td>
</tr>
<tr>
<td>DFX initialization</td>
<td>0xEB</td>
</tr>
<tr>
<td>NTB initialization</td>
<td>0xEC</td>
</tr>
<tr>
<td>Security Initialization</td>
<td>0xED</td>
</tr>
<tr>
<td>IIO late initialization</td>
<td>0xEE</td>
</tr>
<tr>
<td>IIO late initialization</td>
<td>0xEF</td>
</tr>
</tbody>
</table>
1-9 BIOS POST Beep code (AMI standard)

1-9-1 PEI Beep Codes

<table>
<thead>
<tr>
<th># of Beeps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Memory not Installed.</td>
</tr>
<tr>
<td>1</td>
<td>Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)</td>
</tr>
<tr>
<td>2</td>
<td>Recovery started</td>
</tr>
<tr>
<td>3</td>
<td>DXE IPL was not found</td>
</tr>
<tr>
<td>3</td>
<td>DXE Core Firmware Volume was not found</td>
</tr>
<tr>
<td>4</td>
<td>Recovery failed</td>
</tr>
<tr>
<td>4</td>
<td>S3 Resume failed</td>
</tr>
<tr>
<td>7</td>
<td>Reset PPI is not available</td>
</tr>
</tbody>
</table>

1-9-2 DXE Beep Codes

<table>
<thead>
<tr>
<th># of Beeps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Invalid password</td>
</tr>
<tr>
<td>4</td>
<td>Some of the Architectural Protocols are not available</td>
</tr>
<tr>
<td>5</td>
<td>No Console Output Devices are found</td>
</tr>
<tr>
<td>5</td>
<td>No Console Input Devices are found</td>
</tr>
<tr>
<td>6</td>
<td>Flash update is failed</td>
</tr>
<tr>
<td>7</td>
<td>Reset protocol is not available</td>
</tr>
<tr>
<td>8</td>
<td>Platform PCI resource requirements cannot be met</td>
</tr>
</tbody>
</table>
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.