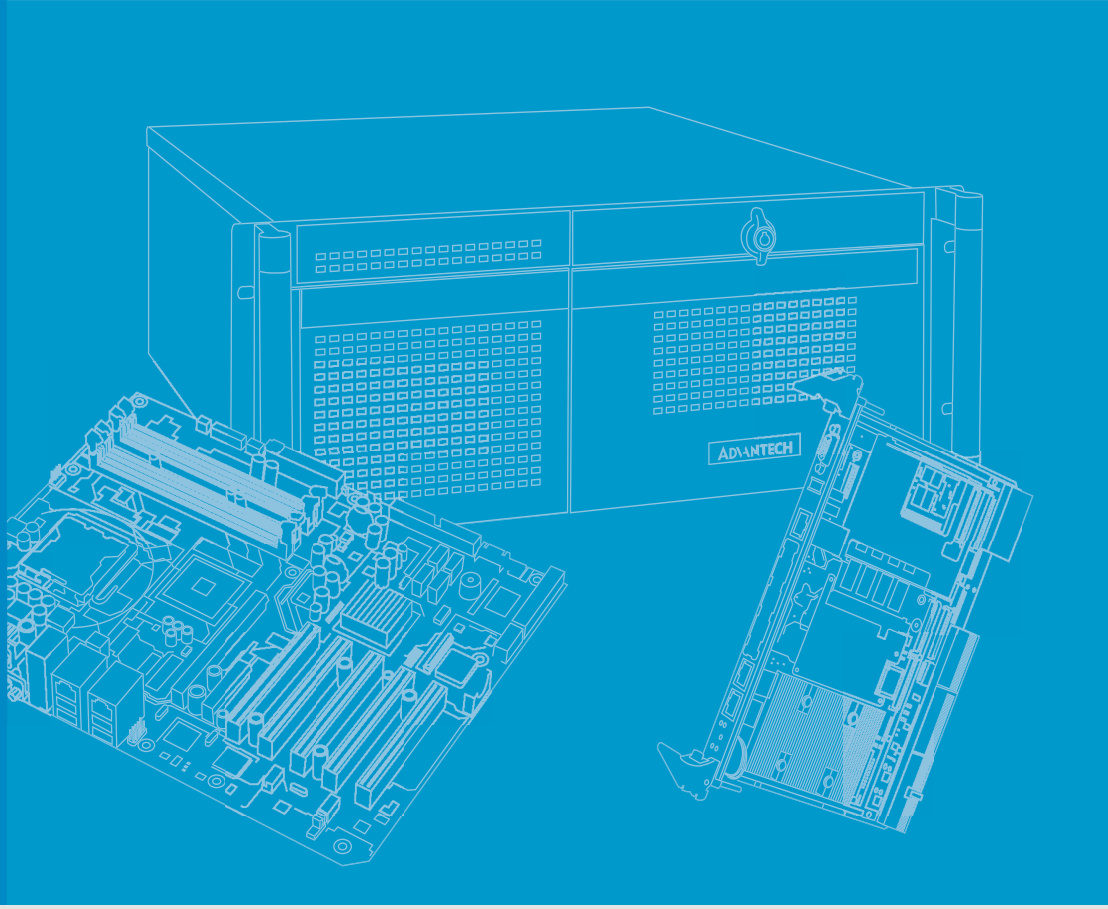

User Manual

MIC-8303C

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

For more information about this and other Advantech products, please visit our website at:

http://www.advantech.com/

For technical support and service, please visit our support website at:

http://support.advantech.com

Part No. Edition 1

Printed in China January 2017

Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandise authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications.

FCC Class A

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

Technical Support and Assistance

1. Visit the Advantech web site at http://support.advantech.com where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions in which there is a chance of personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data.*

Note! *Notes provide optional additional information.*

Safety Instructions

1. Please read these safety instructions carefully.
2. Please keep this User's Manual for later reference.
3. Please disconnect this equipment from AC outlet before cleaning. Use a damp cloth. Don't use liquid or sprayed detergent for cleaning. Use moist sheet or cloth for cleaning.
4. For pluggable equipment, the socket-outlet shall near the equipment and shall be easily accessible.
5. Please keep this equipment from humidity.
6. Lay this equipment on a reliable surface when installing. A drop or fall could cause injury.
7. The openings on the enclosure are for air convection hence protecting the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source when connecting the equipment to the power outlet.
9. Place the power cord such a way that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for long time, disconnect the equipment from mains to avoid being damaged by transient over-voltage.
12. Never pour any liquid into ventilation openings; this could cause fire or electrical shock.
13. Never open the equipment. For safety reasons, only qualified service personnel should open the equipment.
14. If one of the following situations arises, get the equipment checked by service personnel:
    - The power cord or plug is damaged.
    - Liquid has penetrated into the equipment.
    - The equipment has been exposed to moisture.
    - The equipment does not work well, or you cannot get it to work according to the user's manual.
    - The equipment has been dropped and damaged.
    - The equipment has obvious signs of breakage.
15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -40° C (-40° F) OR ABOVE 85° C (185° F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
16. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.
17. The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).
18. RESTRICTED ACCESS AREA: The equipment should only be installed in a Restricted Access Area.

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Contents

Chapter 1

Product Overview

1.1 MIC-8303C Overview

Advantech's MIC-8303C is a dual systems (per system per processor) micro-server blade, which is based on Intel Xeon D integrated platform, fitting into the market for the server market prioritizing efficiency and networking. Xeon D, also known as Broadwell-DE, combines up to sixteen high performance Broadwell cores and the PCH onto a single die, reduces both down to 14 nm for power consumption/die area and offers an array of server features normally found with the Xeon line. This is being labeled as the first proper Intel Xeon SoC platform.

The MIC-8303C is a dual CPU blade with up to 16 cores and 32 threads of processing power, fast PCI Express Gen3 lanes running at up to 8Gbps. With four DDR4 DIMMs per socket in a two channel design running up to 2133MT/s, can also support memory densities up to 128GB. Each CPU supports one USB 3.0 ports to the front, one mini USB console port for Management Interface, and the fabric connection is implemented by Braodwell-DE CPU to get two 10GBASE-KR connections.

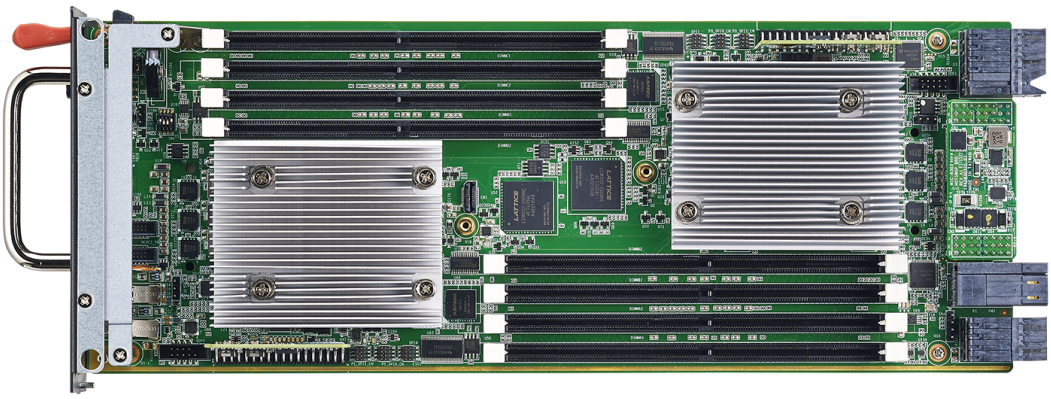

Figure 1.1 MIC-8303C

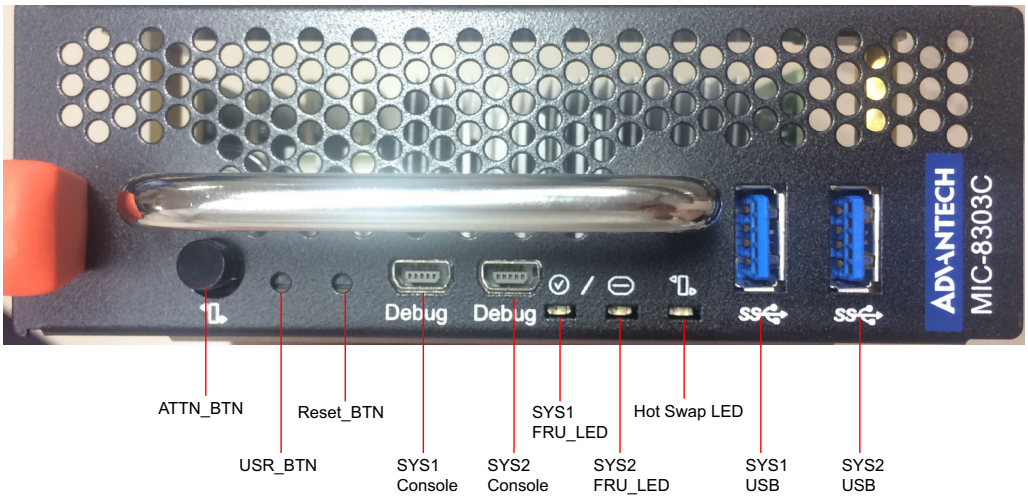

Figure 1.2 MIC-8303C Front Panel Layout

1.2 MIC-8303C Block Diagram

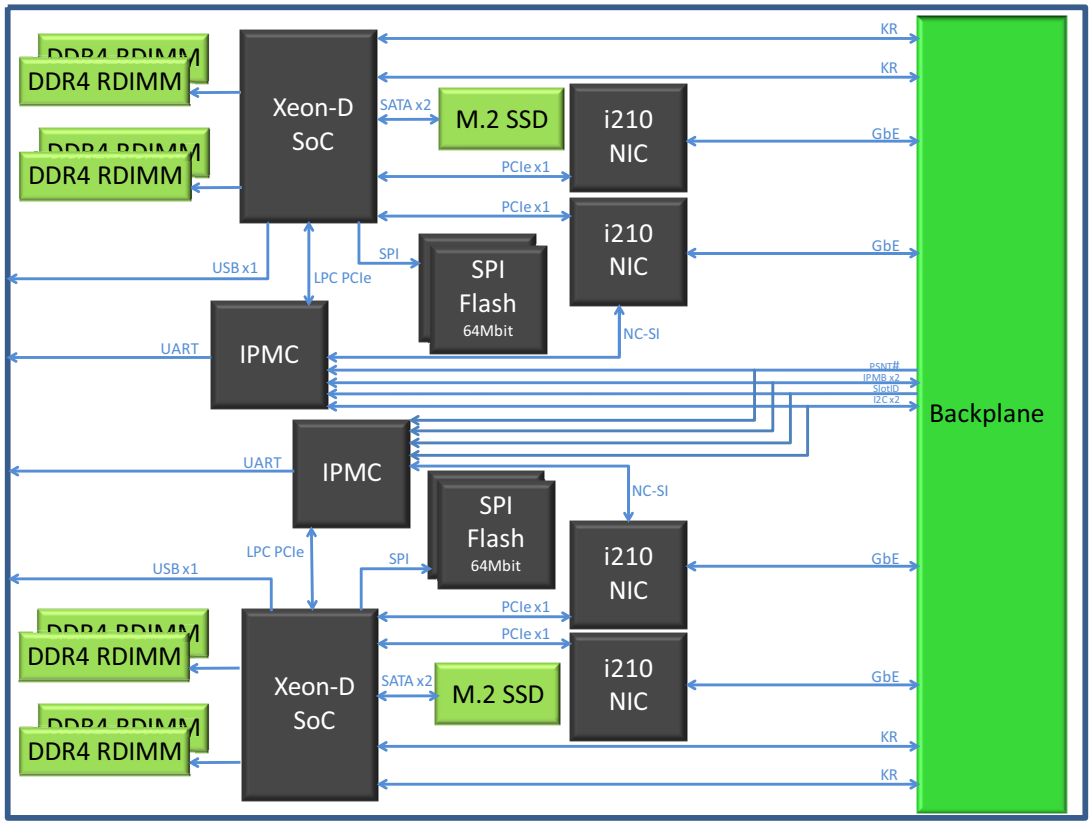

Figure 1.3 MIC-8303C Block Diagram

1.3 LED Behavior

Table 1.1: LED Behavior of MIC-8303C

LED	Category	Color	Description
Hot Swap LED	Handle	Blue	Handle LED for hot-swap indication
SYS 1 FRU LED	OOS	Red	On: Out of service Off: Normal Blinking: Bootloader active / update in progress
	Health	Green	FW status indicator On: FW active, payload active Off: FW inactive Blinking: FW active, payload inactive
SYS 2 FRU LED	OOS	Red	On: Out of service Off: Normal Blinking: Bootloader active / update in progress
	Health	Green	FW status indicator On: FW active, payload active Off: FW inactive Blinking: FW active, payload inactive

Chapter 2

Installation

2.1 Insert into Chassis

Please remove the filler panel before installing node blade. Node blades support hot-swap, it is not required to turn off the chassis power before installing the board.

To insert node blade into the PAC-6009 chassis:

1. To ensure that the node blade will function properly in the chassis, set the jumpers at “off”, which allows the board to function under normal mode. See Table 2.1 for MIC-8303C SW2, SW3 and SW4setting.

Table 2.1: MIC-8303C SW2, SW3 and SW4 Jumper Setting

SW2 IPMC CFG(CPU0)			
Default	Normal operation	1 Off	
SW3 IPMC CFG(CPU1)			
Default	Normal operation	1 Off	
SW4 IPMC CFG			
Default	Normal operation	1 Off 2 Off 3 Off 4 Off	

Note! ▬ represents the key.

2. Align the PCB edge to the card guide rail.
3. Carefully slide the node blade into the system until the connector contacts into the backplane. Make sure (1) the front panel alignment pin falls into the receptacle, (2) the orange latch spring is tightly locked.
4. Following is the sequence of the handle and Health Status LED:
   - Blue (Hot Swap LED) solid, green (Health Status LED) off
   - Board inserted to the final position I:
     Blue blinking (activation request to ShMC), green blinking (FW active)
   - Board inserted to the final position II:
     Blue off (ShMC granted activation), green blinking (FW active)
   - Board inserted to the final position III:
     Blue off (ShMC granted activation), green solid (ShMC allows the ATCA blade to turn on thepayload power)
5. In case of a failure, the red LED will be lit.

To extract node blade from the PAC-6009 chassis:

1. Push the Attention button.
2. Node blade will start deactivation (shut down OS), and blink the blue LED (Hot Swap LED).
3. When the blue LED is constantly lit, it is safe to extract the node blade.

4. Press the orange latch spring to unlatch node blade.

Caution!

- *Only ONE Node blade is allowed to be extracted at one time.*
- *DO NOT leave the slot empty when extracting the board, the alternative board or a dummy card MUST be inserted immediately for safety purpose.*
- *Do not force the node blade into the back plane when the mating process does not seem smooth or when there seems to be some mechanical interference during the insertion process.*

2.2 Install DDR4

To install the DDR4 STD DIMM on node blade:

1. Insert the DDR4 STD DIMM memory to the DIMM slot. Press the DDR4 STD DIMM downwards until two side latches well lock the DIMM.

To uninstall the DDR4 STD DIMM from node blade:

1. Press two side latches downwards until DDR4 STD DIMM memory unlock.

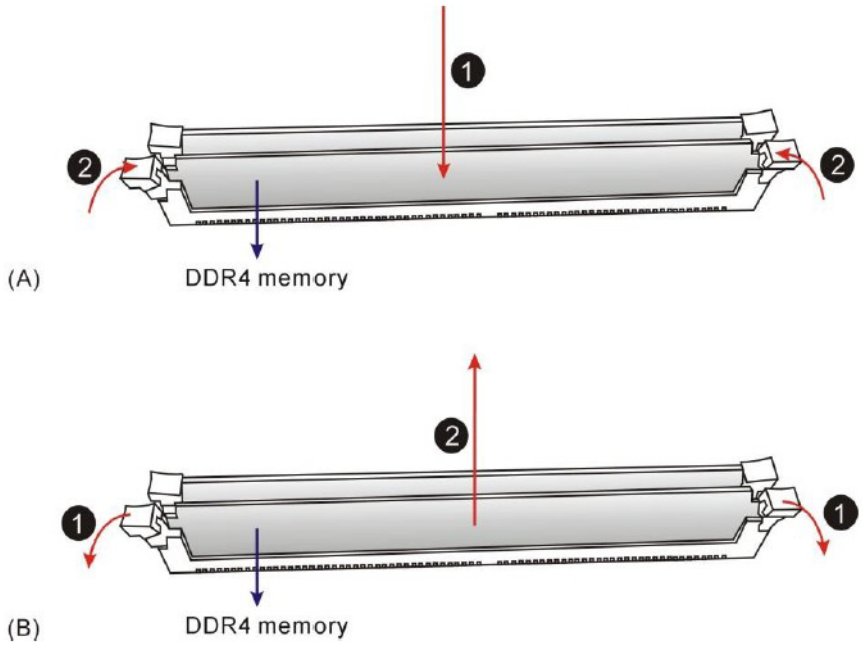

Figure 2.1 Install DDR4 Memory (B) Uninstall DDR Memory

2.3 Install 2242 M.2 SSD

Single M.2 Solid State Drive (SSD) modules are available to be installed on the MIC-8303C and dual for MIC-8303C(1). For installing the storage module, please follow the bellowing procedures.

1. Insert the m-SATA SSD with an angle of approximate 33° in the slot. Press the m-SATA SSD downwards.
2. Install and fasten the fixing screw.

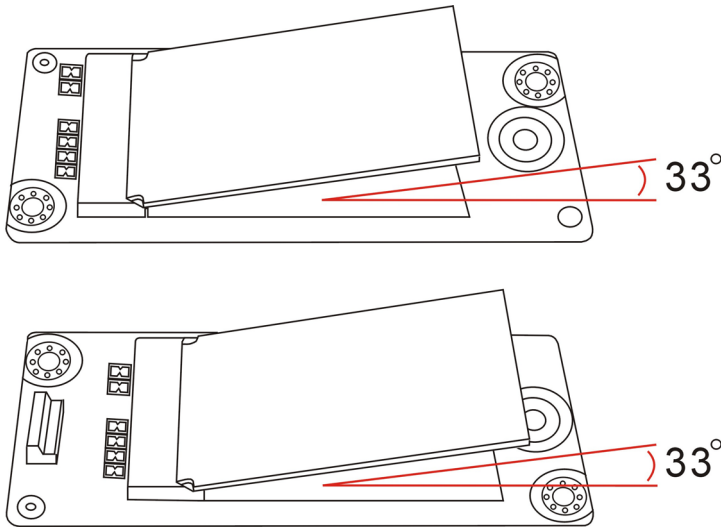

Figure 2.2 Top Side of M.2 Board (B) Bottom Side of M.2 Board

Note! *MIC-8303C has two 2242 M.2 SSD slot, which are located on top and bottom of the M.2 board.*

Chapter 3

AMI APTIO BIOS Setup

3.1 Introduction

This section describes the AMI APTIO BIOS, UEFI compliant, which has been specifically adapted to the MIC-8303C. With the AMI APTIO BIOS Setup program, users can modify BIOS settings and control the special features of the MIC-8303C. The setup program uses a number of menus for making changes and turning special features on or off. This chapter describes the basic navigation of the MIC-8303C setup screens.

3.2 Entering Setup

Turn on the computer, and there should be a “version” code displayed that shows the BIOS supporting the CPU. If there is no number assigned to the patch code, please contact an Advantech application engineer to obtain an up-to-date patch code file. This will ensure that the CPU’s system status is valid. Press <DEL> or <F2> and users will immediately be allowed to enter Setup.

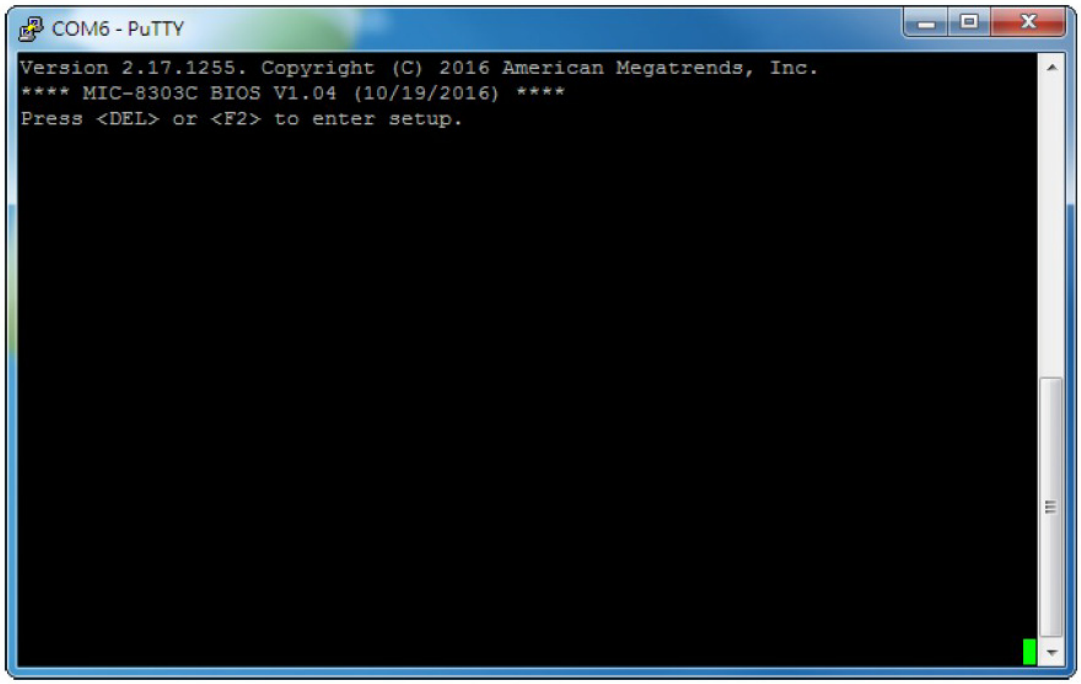

Figure 3.1 Press <DEL> or <F2> to Run Setup

3.3 Main Setup

When users first enter the BIOS Setup Utility, users will enter the Main setup screen. Users can always return to the Main setup screen by selecting the Main tab. Two main setup options are described in this section. The main BIOS setup screen is shown as below.

The main BIOS setup menu screen has two main frames. The left frame displays all the options that can be configured, the default setting is in bold. The right frame displays the key legend. Above the key legend is an area reserved for a text message.

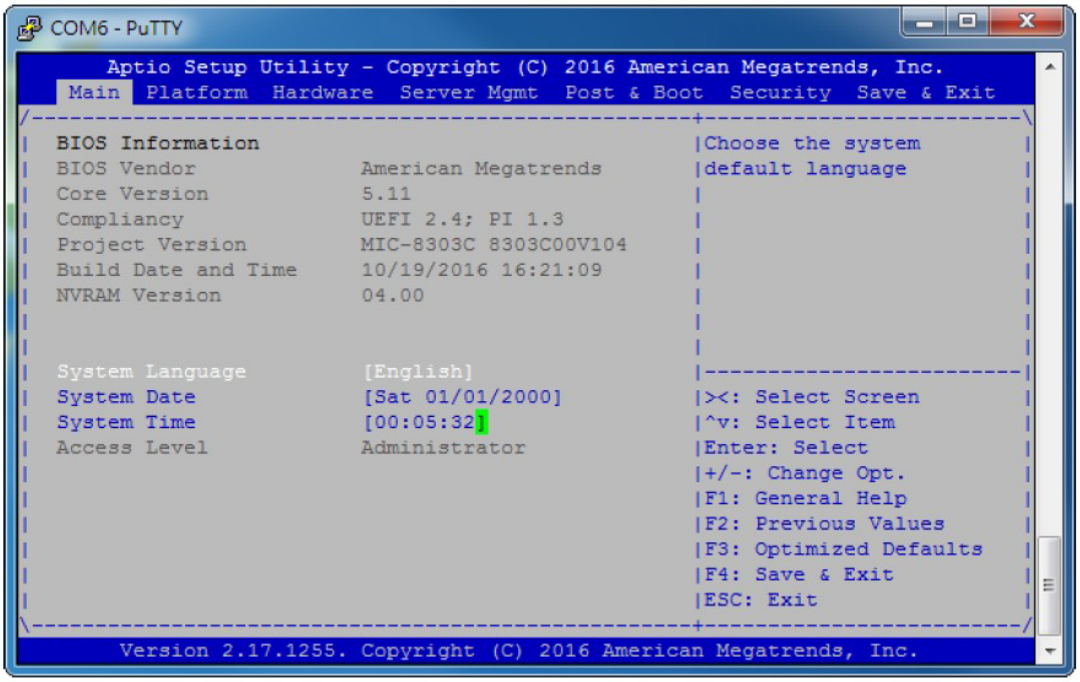

Figure 3.2 Main Page Setup Snapshot

Table 3.1: BIOS Menu: Main

Feature	Option	Description	Help text
BIOS Vendor	American Megatrends	BIOS Vendor	N/A
Core Version	X.YYY	Display the BIOS Core version	N/A
Compliancy	UEFI X.Y PI W.Z	Display the UEFI Platform Initialization version.	N/A
Project Version	MIC-8303C 8303C00V1XX	Display BIOS version	N/A
Build Date and Time	mm/dd/yyyy hh:mm:ss	Display BIOS build date & time.	N/A
NVRAM Version	XX.YY	Display NVRAM version	N/A
System Language	English	Display BIOS support language.	N/A
System Date	MM/DD/YYYY	Set the system date.	Use [+] or [-] to configure system date.
System Time	HH:MM:SS	Set the system time.	Use [+] or [-] to configure system time.
Access Level	Administrator User	Display currently access level	N/A

3.3.1 System Language

Use this option to change the system language. Highlight System Language by using the <Arrow> keys. Press <Enter> into the sub menu to select the proper language for further setup and maintenance.

3.3.2 System Date / System Time

Use this option to change the system date and time. Highlight System Date or System Timeby using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time is entered in HH:MM:SS format.

3.4 Platform Setup

Select the Platform tab from the MIC-8303C setup screen to enter the Platform setup screen. Users can select any of the items in the left frame of the screen, such as Serial Console, to go to the sub menu for that item. Users can display the Platform-setup option by highlighting it using the <Arrow> keys. All Platform setup options are described in this section. The Platform setup screen is shown as below. The sub menus are described in the following pages.

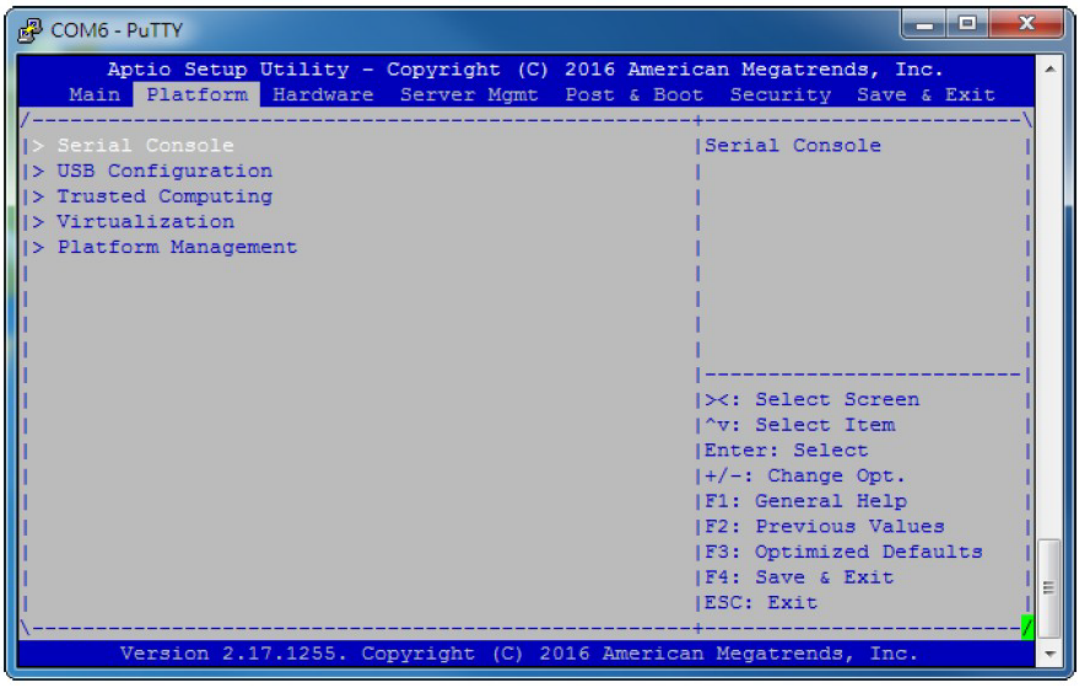

Figure 3.3 Platform Setup Snapshot

3.4.1 Serial Console

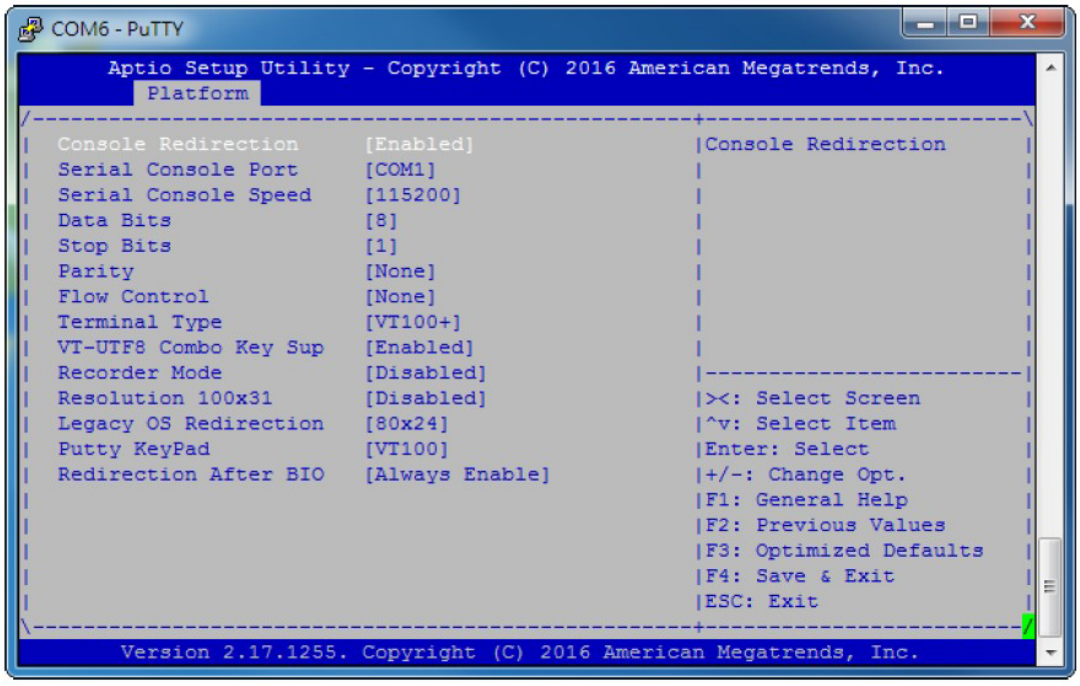

Figure 3.4 Serial Console Settings

Table 3.2: Serial Console Settings

Feature	Option	Description	Help text
Console Redirection	Enabled Disabled	Enable or disable console redirection.	Console redirection.
Serial Console Port	COM1	Configure serial port for console redirection.	Select Console port.
Bits Per Second	9600, 19200, 38400, 57600, 115200	Configure serial port Baud rate for serial port.	Select serial port Baud rate.
Data Bits	7 8	Configure the number of data bits in each transmitted or received serial character for both serial ports.	Data Bits
Stop Bits	1 2	Configure the number of stop bits transmitted and received in each serial character for both serial ports.	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.

Table 3.2: Serial Console Settings			
Parity	None Even Odd Mark Space	Configure if parity bit is generated (transmit data) or checked (receive data) between the last data word bit and stop bit of the serial data for both serial ports.	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the number of 1's in the data bits is even. Odd: parity bit is 0 if the number 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. They can be used as an additional data bit.
Flow Control	None, Hardware RTS/CTS	Configure flow control for console redirection.	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.
Terminal Type	VT100VT100+VT-UTF8 ANSI	Configure the type of console emulation used.	Terminal Type for Redirection Via AMI Debugger. 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.
VT-UTF8 Combo Key Support	Disabled Enabled	Enable or disable VT-UTF8 Combo Key	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	Disabled Enabled	Enable or disableRecorder Mode	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled Enabled	Enable or disableextended terminal resolution	Enables or disables extended terminal resolution
Legacy OS Redirection Resolution	80x24 80x25	SelectLegacy OS Redirection Resolution	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	VT100 LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS POST	Always Enable BootLoader	The Settings specify if BootLoader is selected, then Legacy console redirection is disabled before booting to Legacy OS. Default value is always Enabled which means Legacy Console Redirection is enabled for Legacy OS.	The Settings specify if BootLoader is selected, then Legacy console redirection is disabled before booting to Legacy OS. Default value is always Enabled which means Legacy Console Redirection is enabled for Legacy OS.

3.4.2 USB Configuration

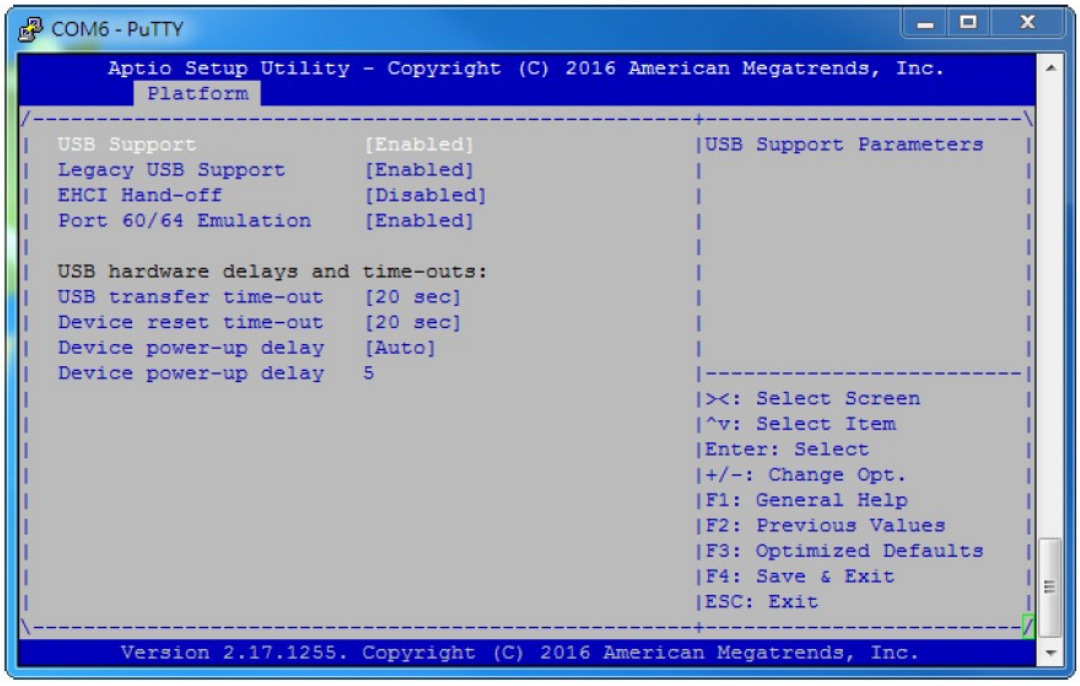

Figure 3.5 USB Configuration

Table 3.3: USB Configuration

Feature	Option	Description	Help text
USB Support	Disabled Enabled	Enable or disable USB function support	USB Support Parameters
Legacy USB Support	Enabled Disabled Auto	Enable or disable Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.	Enable Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
EHCI Hand-off	Disabled Enabled	If the OS doesn't support EHCI, BIOS will get the control.	This is a workaround for OSes without EHCI hand-off support. The EHCI ownership change should be claimed by EHCI driver.
Port 60/64 Emulation	Disabled Enabled	Enables I/O port 60h/64h emulation support.	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec	Set the time-out value for USB transfers.	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec 20 sec 30 sec 40 sec	Set the time-out value forUSB mass storage device Start Unit command.	USB mass storage device Start Unit command time-out.

Table 3.3: USB Configuration			
Device power-up delay	Auto Manual	Select device power-up delay control way.	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.
Device power-up delay in seconds	5	Set device power-up delay when “Device power-up delay” choose “Manual”	Delay range is 1..40 seconds, in one second increments

3.4.3 Trusted Computing

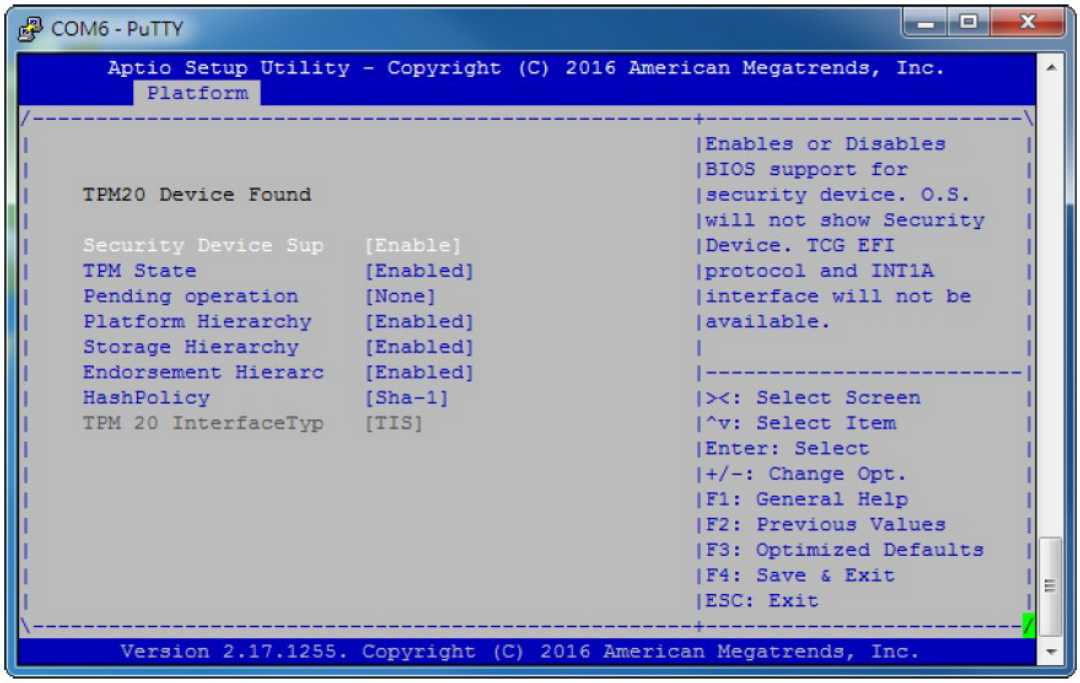

Figure 3.6 Trusted Computing

Table 3.4: Trusted Computing			
Feature	**Option**	**Description**	**Help text**
Security Device Support	Disable Enable	Enable or disable BIOS support for security device.	Enable or disable BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
TPM State	Disabled Enabled	Enable or disable TPM.	Enable or disable Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
Pending Operation	None TPM Clear	Choose TPM operation for next boot.	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Disabled Enabled	Enable or Disable Platform Hierarchy.	Enable or Disable Platform Hierarchy.

Table 3.4: Trusted Computing			
Storage Hierarchy	Disabled Enabled	Enable or Disable Storage Hierarchy.	Enable or Disable Storage Hierarchy.
Endorsement Hierarchy	Disabled Enabled	Enable or Disable Endorsement Hierarchy.	Enable or Disable Endorsement Hierarchy.
HashPolicy	Sha-1 Sha256	Select the Hash policy to use.	Select the Hash policy to use. SHA256 is most secure but might not be supported by all Operating Systems
TPM 20 Interface Type	CRB TIS	Show the Communication Interface to TPM 20 Device.	Show the Communication Interface to TPM 20 Device.

3.4.4 Virtualization

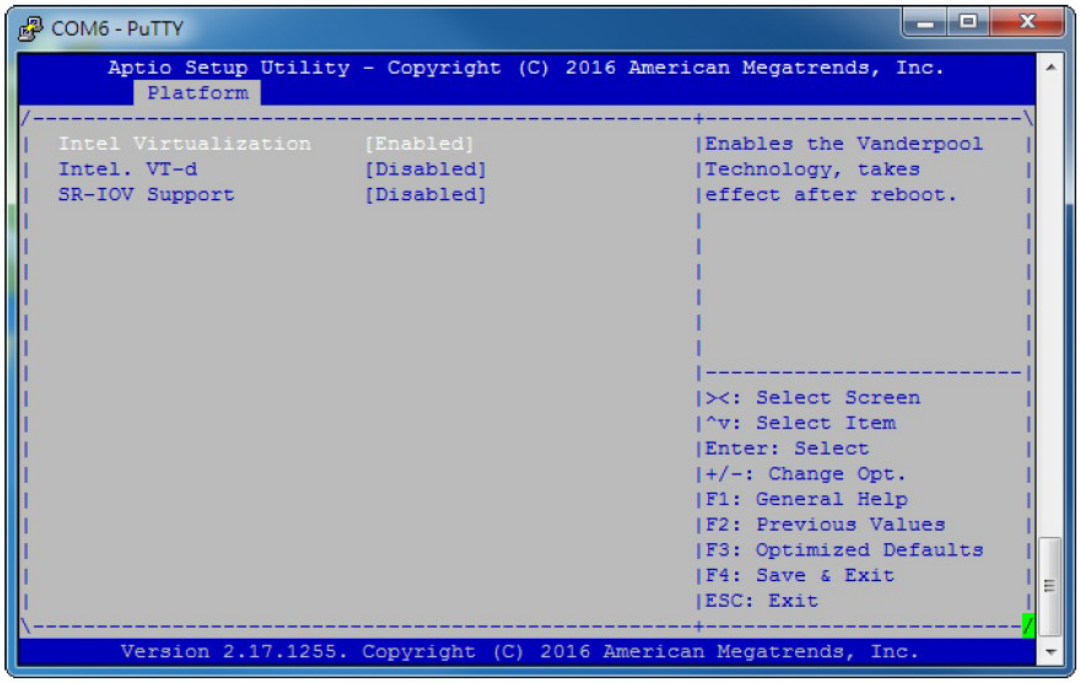

Figure 3.7 Virtualization

Table 3.5: Virtualization			
Feature	**Option**	**Description**	**Help text**
Intel Virtualization Technology	Enabled Disabled	Enable or disable BIOS support for the Vanderpool Technology	Enable the Vanderpool Technology, take effect after reboot.
Intel(R) VT-d	Enabled Disabled	Enable or disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.	Enable or disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
SR-IOV Support	Enabled Disabled	It allows a deviceto separate access to its resources among various PCIe hardware functions.	If the system has SR-IOV capable PCIe devices, this option Enables or Disables Single Root IO Virtualization Support.

3.4.5 Platform Management

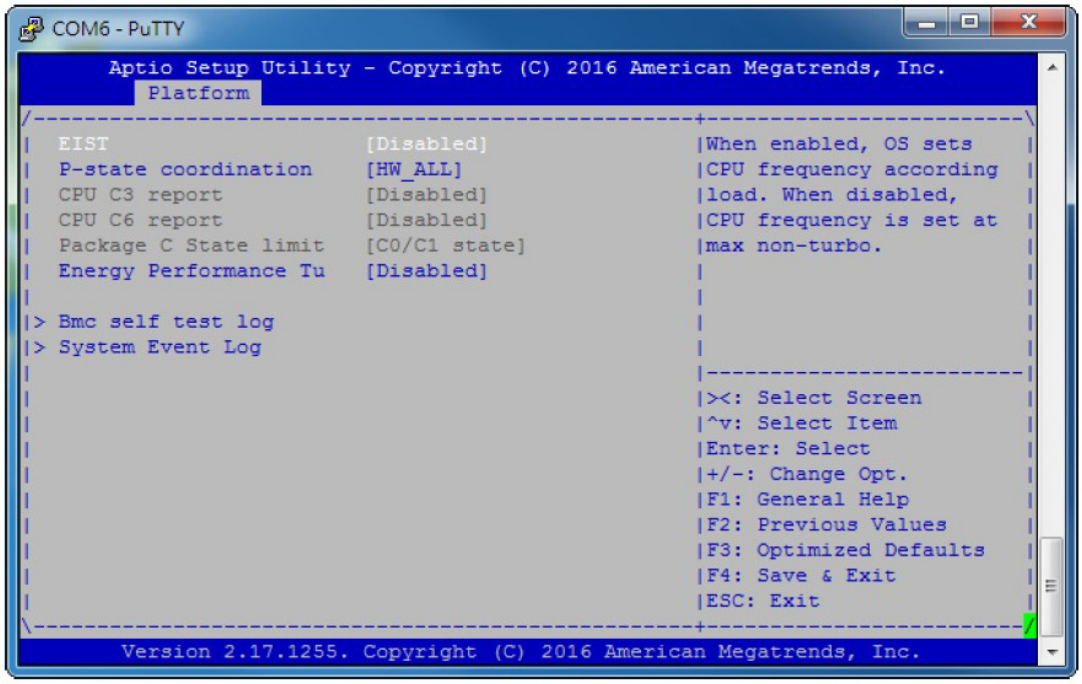

Figure 3.8 Platform Management

Table 3.6: Platform Management

Feature	Option	Description	Help text
EIST	Disabled Enabled	Enable or disable BIOS support for Enhanced Intel SpeedStep Technology	When enabled, OS sets CPU frequency according load. When disabled, CPU frequency is set at max non-turbo.
Turbo Mode	Disabled Enabled	Enable or disable processor Turbo mode.Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceed CPU defined limits.	Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceed CPU defined limits.
P-state Coordination	HW_ALL SW_ALL SW_ANY	This feature is used to change the P-State (Power-Performance State) coordination type.	HW_ALL (hardware) coordination is recommended over SW-ALL and SW_ANY (software coordination).
CPU C3 report	Disabled	Enable or disableCPU C3 report to OS	Enable/Disable CPU C3(ACPI C2) report to OS. Recommended to be disabled.
CPU C6 report	Disabled	Enable or disableCPU C6 report to OS	Enable/Disable CPU C6(ACPI C2) report to OS Recommended to be enabled.
Package C State limit	C0/C1 state	Package C State limit. The "waking-up time" will be longer if Package C state limit setting is deep C state support.	Package C State limit

Table 3.6: Platform Management			
Energy Performance Tuning	Enabled Disabled	CPU energy and performance control policy. Enabled means Power Performance controlled by OS. Disabled means Power Performance control set to “Balanced Performance Mode” by BIOS.	Selects whether BIOS or Operating System chooses energy performance bias tunning.
BMC Self- test Log	N/A	Select sub-menu.	N/A
System Event Log	N/A	Select sub-menu.	N/A

3.4.5.1 BMC Self-test Log

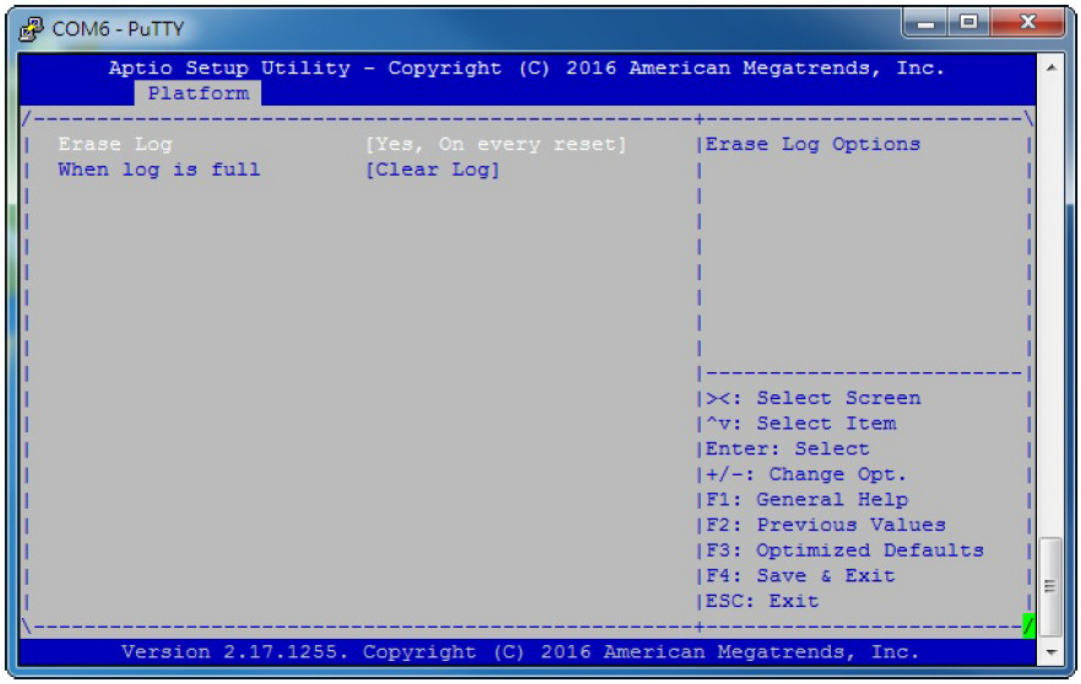

Figure 3.9 BMC Self-test Log

Table 3.7: BMC Self- test Log			
Feature	**Option**	**Description**	**Help text**
Erase Log	Yes, On every reset, No	Choose options for earsing SEL.	Erase Log Options.
When log is full	Clear Log, Do not log any more	Choose options for reactions to a full SEL.	Select the action to be taken when log is full.

3.4.5.2 System Event Log

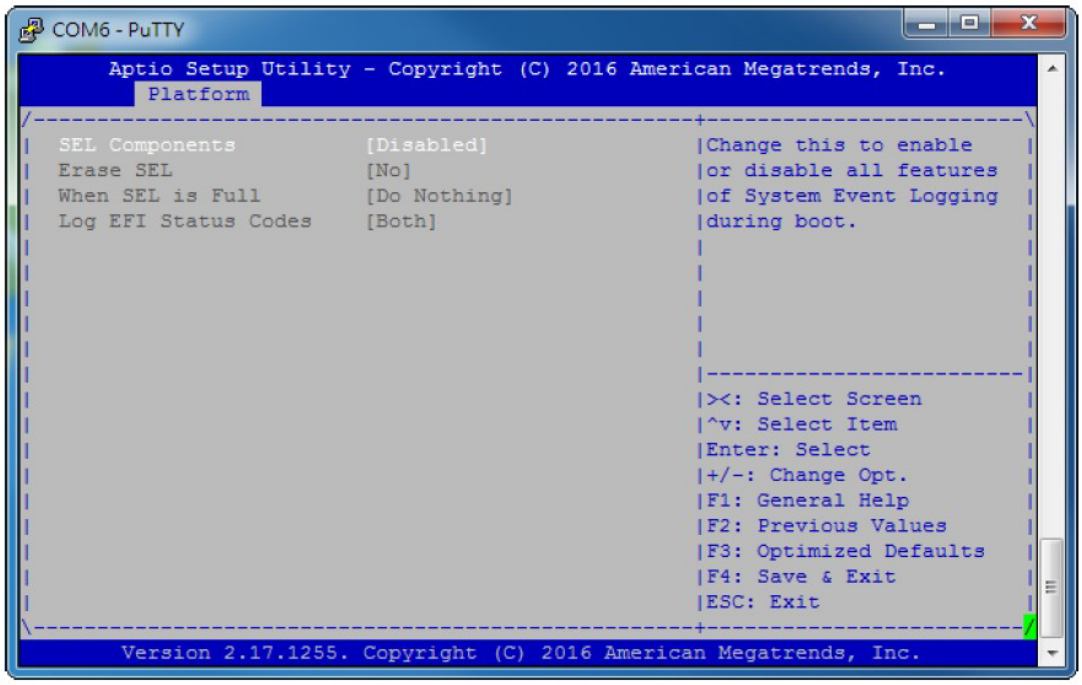

Figure 3.10 System Event Log

Table 3.8: System Event Log

Feature	Option	Description	Help text
SEL Components	Disabled Enabled	Change this to enable or disable all features of System Event Logging during boot.	Change this to enable or disable all features of System Event Logging during boot.
Erase SEL	No Yes, On next reset Yes, On every reset	Choose options for earsing SEL.	Choose options for erasing SEL.
When SEL is Full	Do Nothing Erase Immediately	Choose options for reactions to a full SEL.	Choose options for reactions to a full SEL.
Log EFI Status Codes	Disabled Both Error code Progress code	Use this item to disable the logging of EFI Status Codes or log only error code or only progress or both.	Disable the logging of EFI Status Codes for log only error code or only progress code or both.

3.5 System Event Log

Select the chipset tab from the MIC-8303C setup screen to enter the Hardware setup screen. Users can configure the parameters of CPU configuration, Northbridge and Southbridge, respectively.

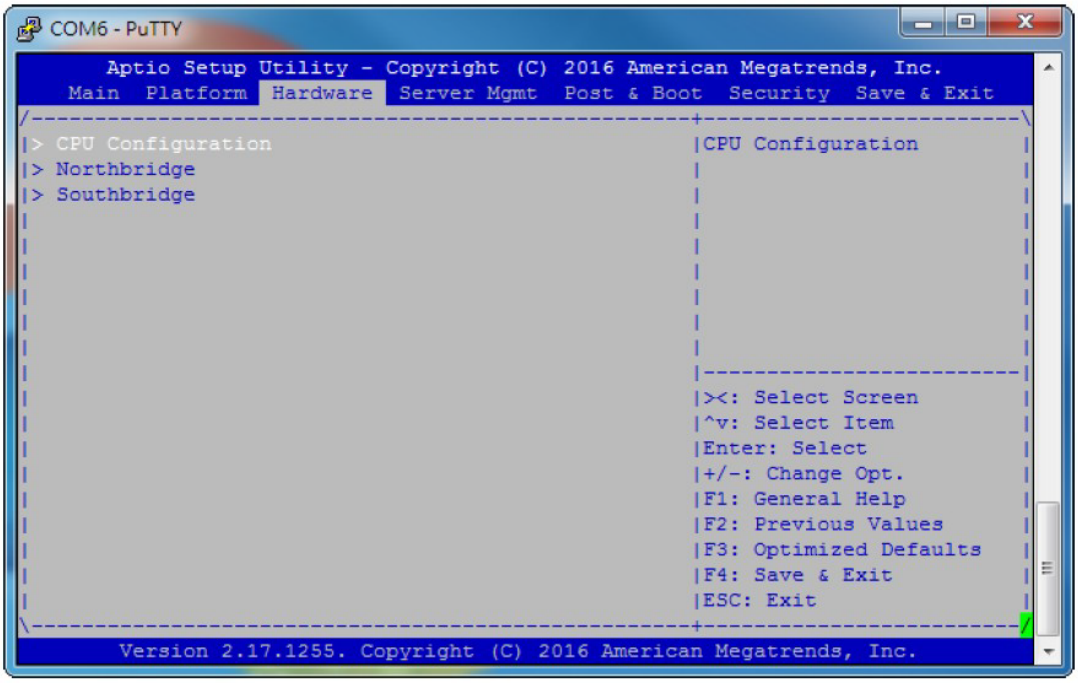

Figure 3.11 Hardware Settings

3.5.1 CPU Configuration

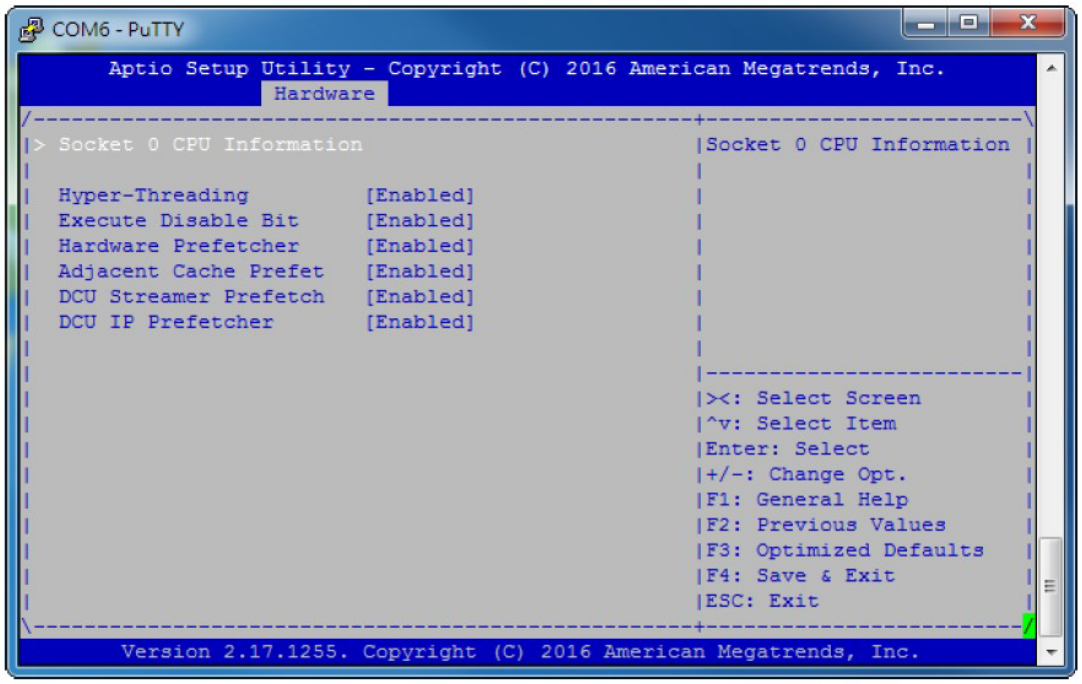

Figure 3.12 CPU configuration

Table 3.9: CPU Configuration			
Feature	**Option**	**Description**	**Help text**
Socket 0 CPU Information	N/A	Select sub-menu.	N/A
Hyper-Threading	Enabled Disabled	Enable or disable processor Hyper Threading feature.	Enable Hyper Threading (Software Method to Enable or disable Logical Processor threads.
Execute Disable Bit	Enabled Disabled	Execute Disable Bit allows the processor to classify areas in memory where application code can be executed and cannot preventing certain classes of malicious buffer overflow attacks when combined with a support-ing operating system.	When disabled, forces the XD feature flag to always return 0.
Hardware Prefetcher	Enabled Disabled	Enable or disable Hardware Prefetcher feature.	= MLC Streamer Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefetch	Enabled Disabled	Enable or disableAdjacent Cache Prefetch feature.	= MLC Spatial Prefetcher (MSR 1A4h Bit[1])
DCU Streamer Prefetcher	Enabled Disabled	Enable or disableDCU Streamer Prefetcher feature.	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).
DCU IP Prefetcher	Enabled Disabled	Enable or disableDCU IP Prefetcher feature.	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).

3.5.1.1 Socket 0 CPU Information

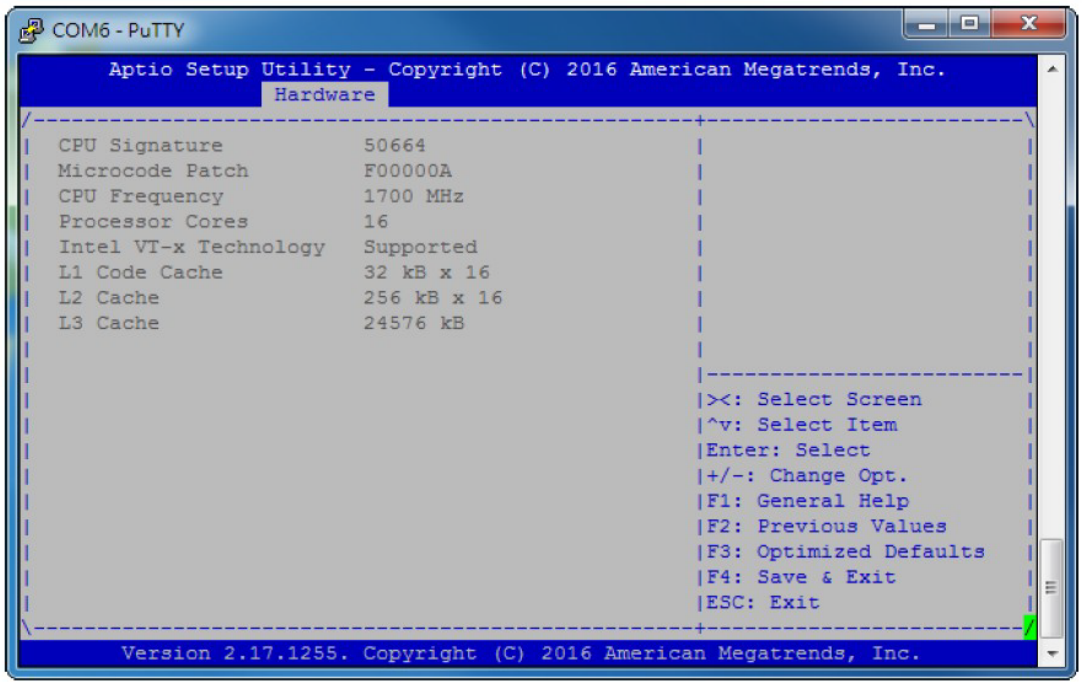

Figure 3.13 Socket 0 CPU Information

3.5.2 Northbridge

Users can setup all parameters related to the IOH function in the North Bridge page. The Broadwell-DE CPU supports QPI channel. Users can configure the related settings in the QPI configuration submenu.

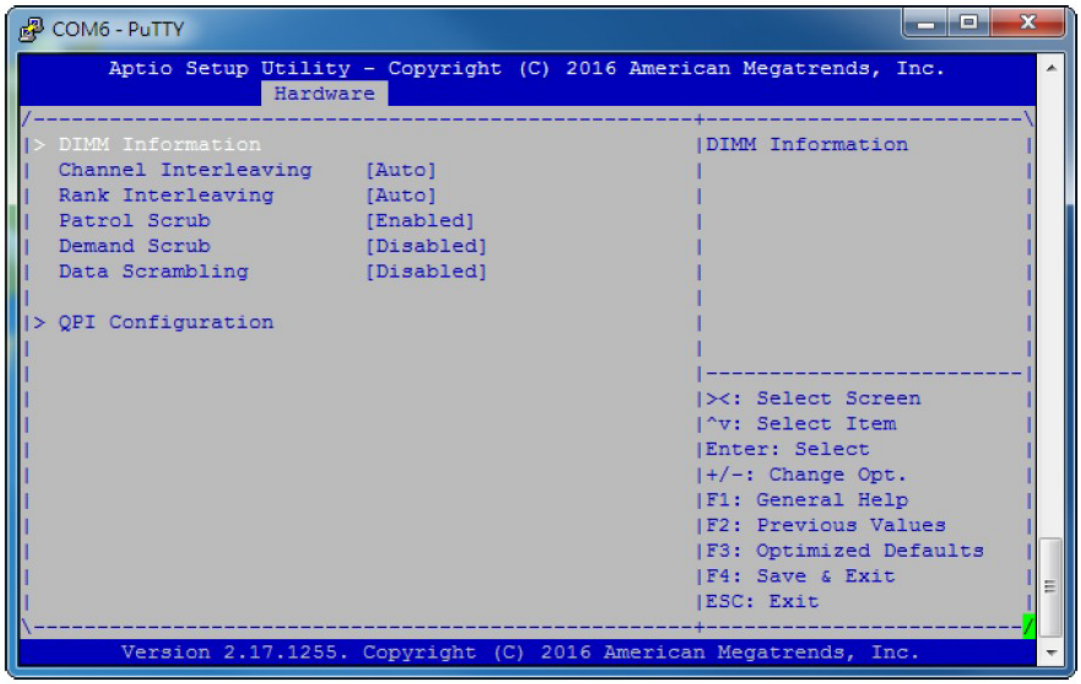

Figure 3.14 Northbridge Configuration

Table 3.10: Northbridge Configuration

Feature	Option	Description	Help text
DIMM Information	N/A	Select sub-menu	N/A
Channel Interleaving	Auto 1-way Interleave 2-way Interleave 3-way Interleave	Select Channel Interleaving setting	Select Channel Interleaving setting
Rank Interleaving	Auto 1-way Interleave 2-way Interleave 4-way Interleave 8-way Interleave	Select Rank Interleaving setting	Select Rank Interleaving setting
Patrol Scrub	Disabled Enabled	ECC patrol scrub	ECC patrol scrubenable or disable.
Demand Scrub	Disabled Enabled	ECC demand scrub	ECC demand scrub enable or disable.
Data Scrambling	Auto Disabled Enabled	Enable or disable Data Scrambling	Enable Data scrambling
QPI Configuration	N/A	Select sub-menu	N/A

3.5.2.1 DIMM Information

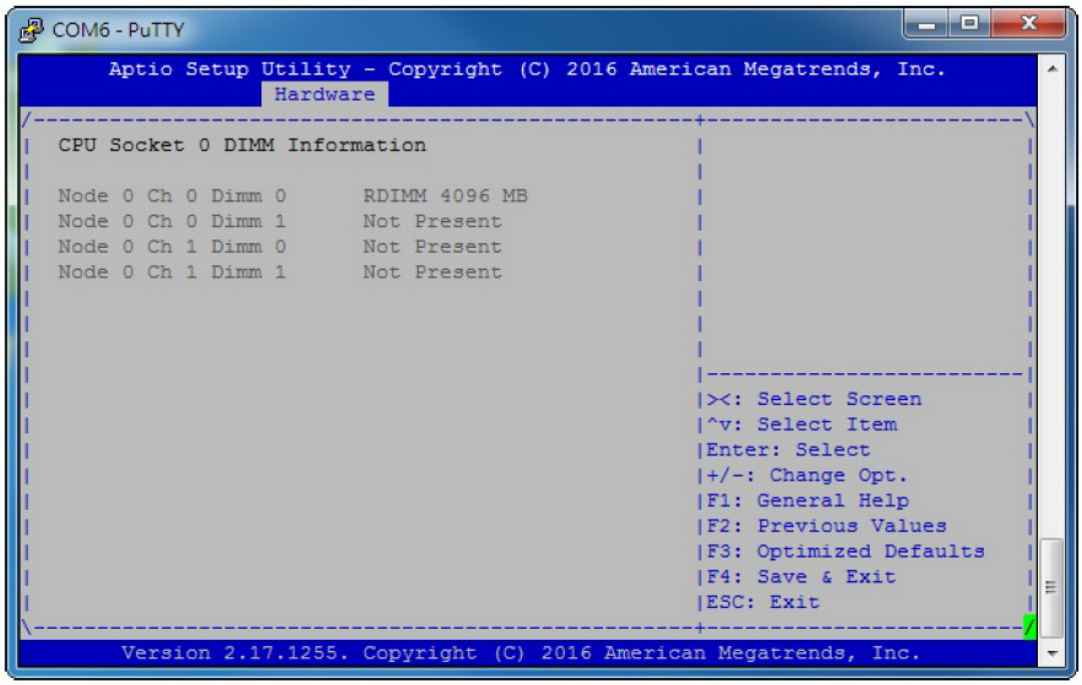

Figure 3.15 DIMM Information

3.5.2.2 QPI Configuration

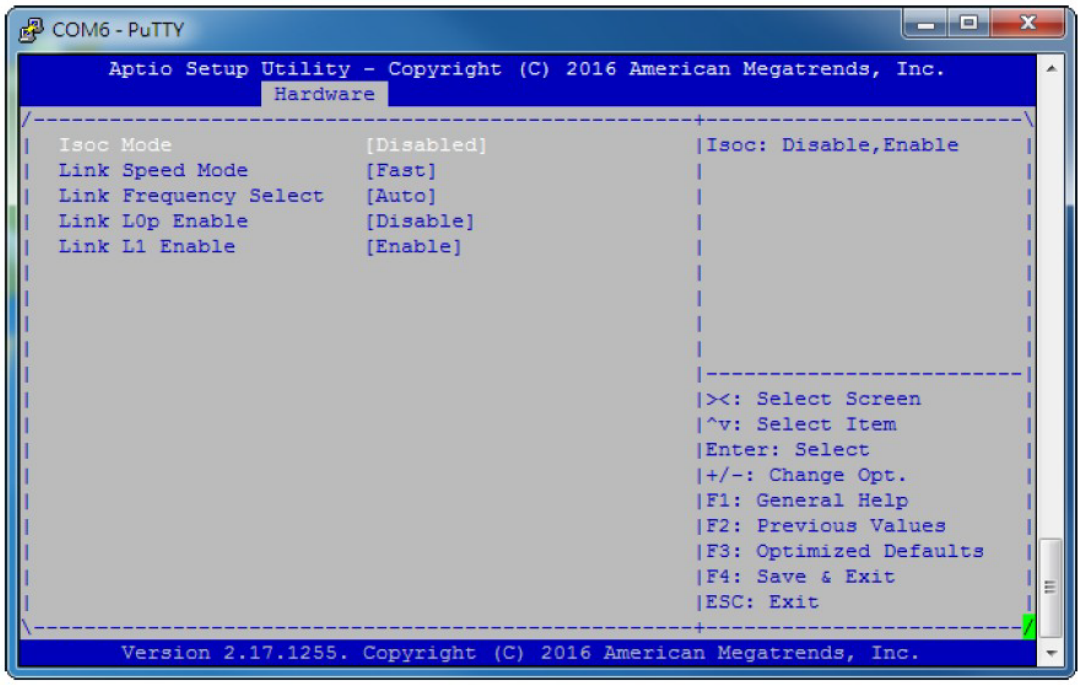

Figure 3.16 QPI Configuration

Table 3.11: QPI Configuration

Feature	Option	Description	Help text
Isoc Mode	Disabled	Enable or disable Isoc Mode	Isoc:Disable, Enable
Link Speed Mode	Slow Fast	Select the QPI link speed as either the POR speed (Fast) or default speed (Slow)	Select the QPI link speed as either the POR speed (Fast) or default speed (Slow)
Link Frequency Select	6.4GB/s, 8.0GB/s, 9.6GB/s Auto Auto Limited	Allows for selecting the QPI Link Frequency	Allows for selecting the QPI Link Frequency
Link L0p Enable	Disable Enable	Enable or disable Link L0p	Link L0p Enable:Disable,
Link L1 Enable	Disable Enable	Enable or disable Link L1	Link L1 Enable:Disable

3.5.3 Southbridge

Users can setup all parameters related to the PCH function in the South Bridge page. Also, users can configure (to enable or disable) USB port (2.0 and 3.0) supported on the MIC-8303C in this page.

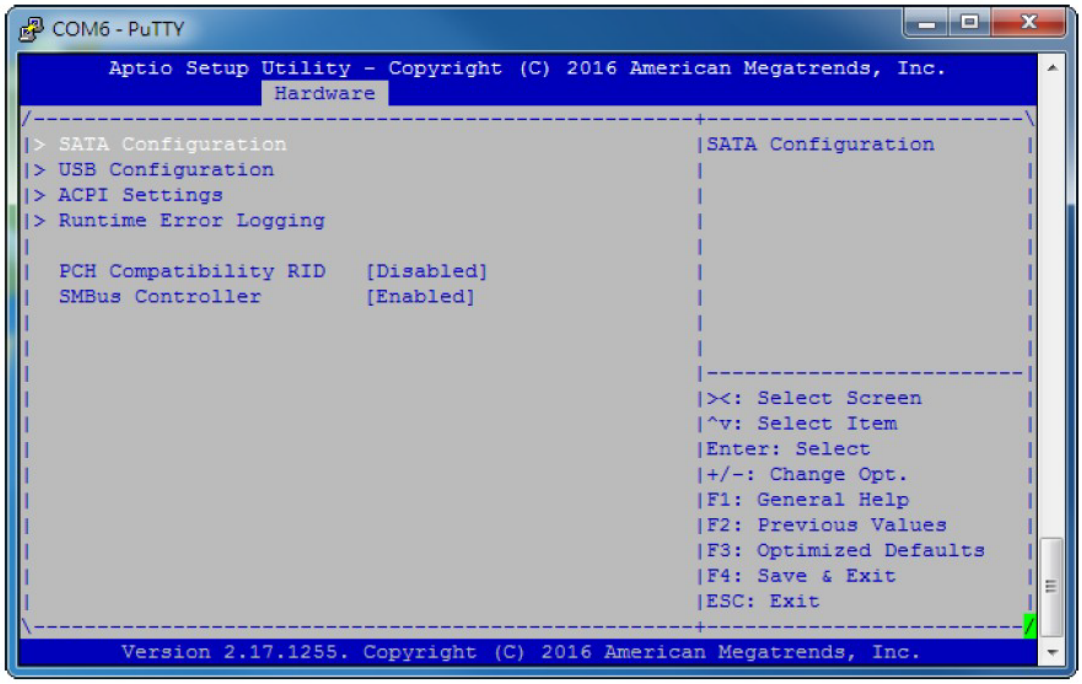

Figure 3.17 Southbridge Configuration

Table 3.12: Southbridge Configuration

Feature	Option	Description	Help text
SATA Configuration	N/A	Select sub-menu	N/A
USB Configuration	N/A	Select sub-menu	N/A
ACPI Settings	N/A	Select sub-menu	N/A
Runtime Error Logging	N/A	Select sub-menu	N/A
PCH Compatibility RID	Disabled Enabled	Enable or disable PCH Compatibility Revision ID	Enable/Disable PCH's CRID
SMBus Controller	Disabled Enabled	Enable or disableSMBus Controller	Enable/Disable SMBUS Device.

3.5.3.1 SATA Configuration

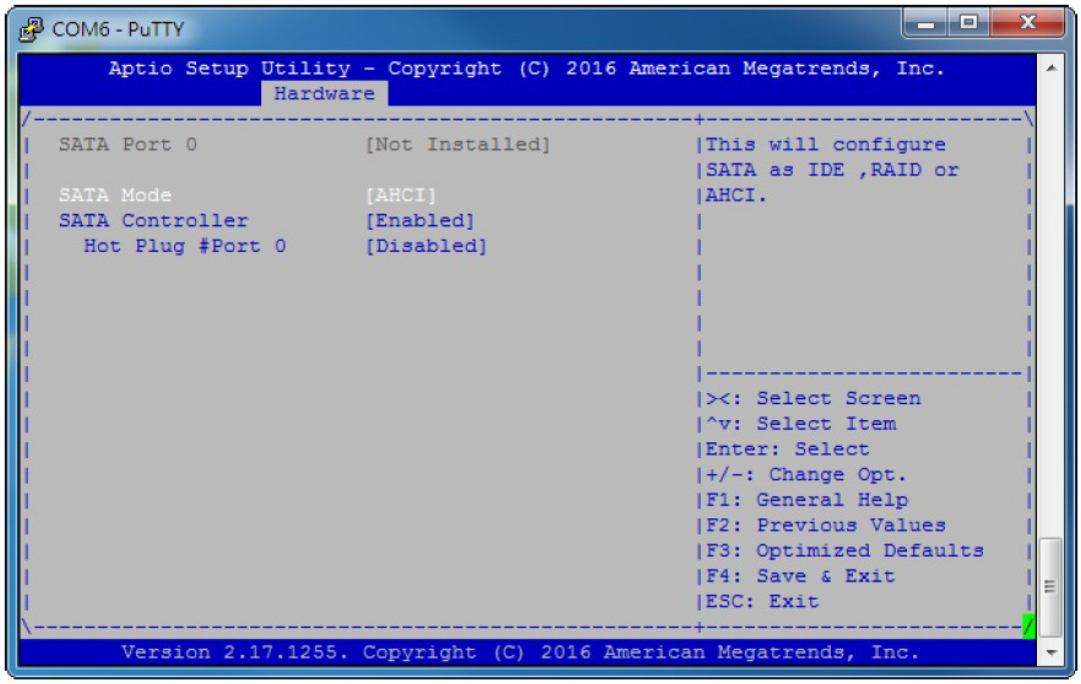

Figure 3.18 SATA Configuration

Table 3.13: SATA Configuration

Feature	Option	Description	Help text
SATA Mode	IDE AHCI	Configure SATA as IDE or AHCI.	This will configure SATA as IDE or AHCI.
SATA Controller	Disabled Enabled	Enable or Disable SATA Controller	Enable or Disable SATA Controller
Hot Plug #Port 0	Disabled Enabled	Enable or Disable hot plug function for SATA Port 0	Designates this port as Hot Pluggable.

3.5.3.2 USB Configuration

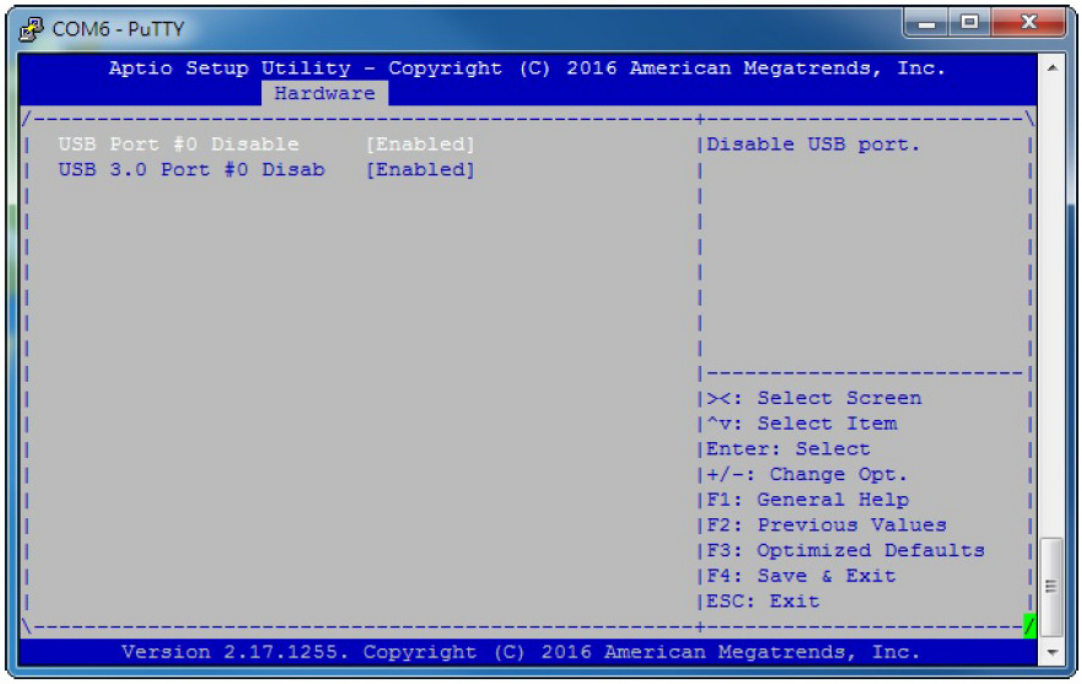

Figure 3.19 USB Configuration

Table 3.14: USB Configuration

Feature	Option	Description	Help text
USB Port #0 Disable	Enabled Disabled	Enable or disable USB Port#0	Disable USB port
USB 3.0 Port #0 Disable	Enabled Disabled	Enable or disable USB 3.0 Port#0	Disable USB port

3.5.3.3 ACPI Settings

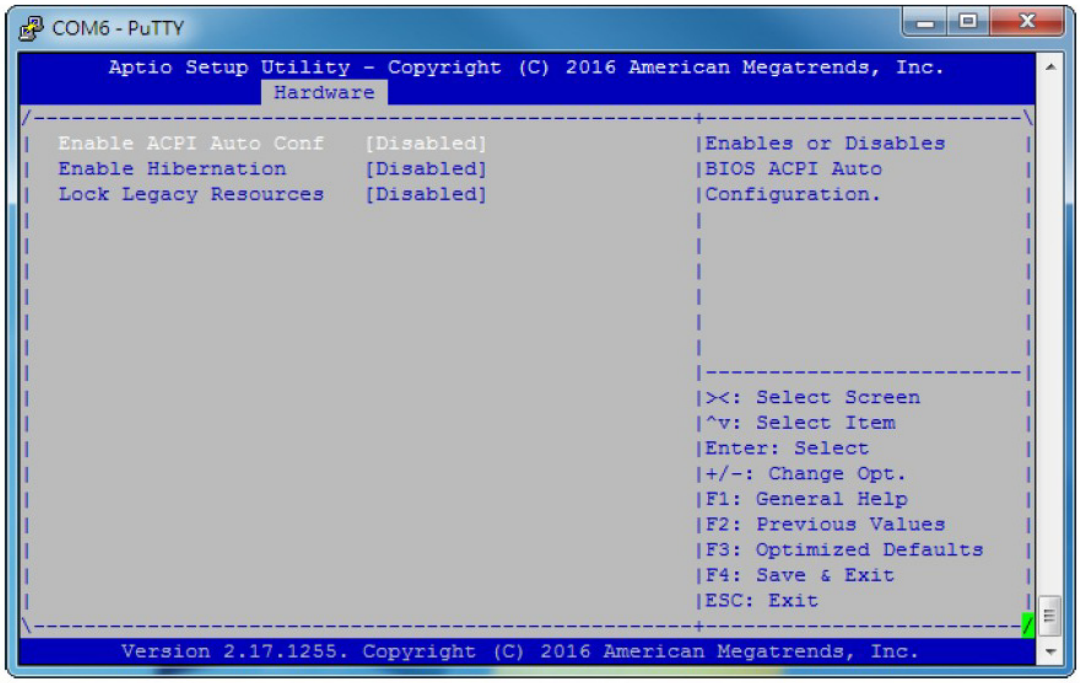

Figure 3.20 ACPI Settings

Table 3.15: ACPI Settings

Feature	Option	Description	Help text
Enable ACPI Auto Configuration	Enabled Disabled	Enable or disable BIOS ACPI Auto Configuration.	Enable or disable BIOS ACPI Auto Configuration.
Enable Hibernation	Enabled Disabled	Enable or disable Hibernation(S4)Support.	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may be not effective with some OS.
Lock Legacy Resources	Enabled Disabled	Enables or Disables Lock of Legacy Resource.	Enables or Disables Lock of Legacy Resource.

3.5.3.4 Runtime Error Logging

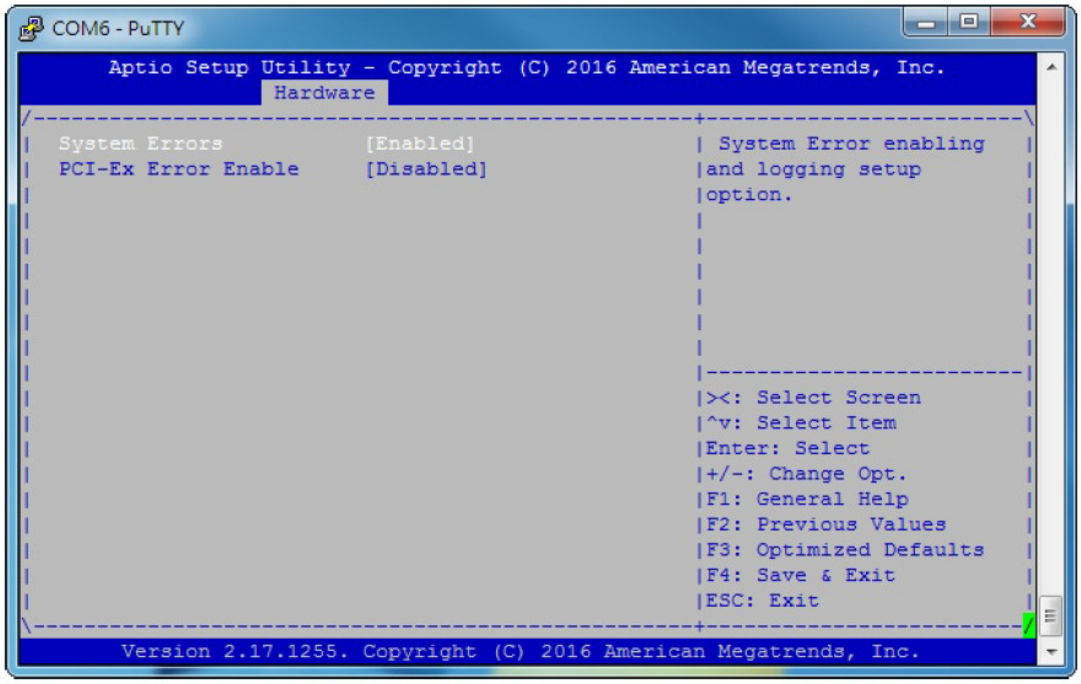

Figure 3.21 Runtime Error Logging

Table 3.16: Runtime Error Logging

Feature	Option	Description	Help text
System Errors	Disabled Enabled Auto	System Error enabling and logging setup option.	System Error enabling and logging setup option.
PCI-Ex Error Enable	Enabled Disabled	PCI-Ex Error enabling and reaction to the error.	N/A

3.6 Server Management Setup

The Server Mgmt menu supports configuring BMC related features such as OS Watchdog Timer, etc. For details of the BMC self test log and system event log, users can decide to enable the function to record the logs, erase the logs through BMC self test log submenu, or the system event log submenu.

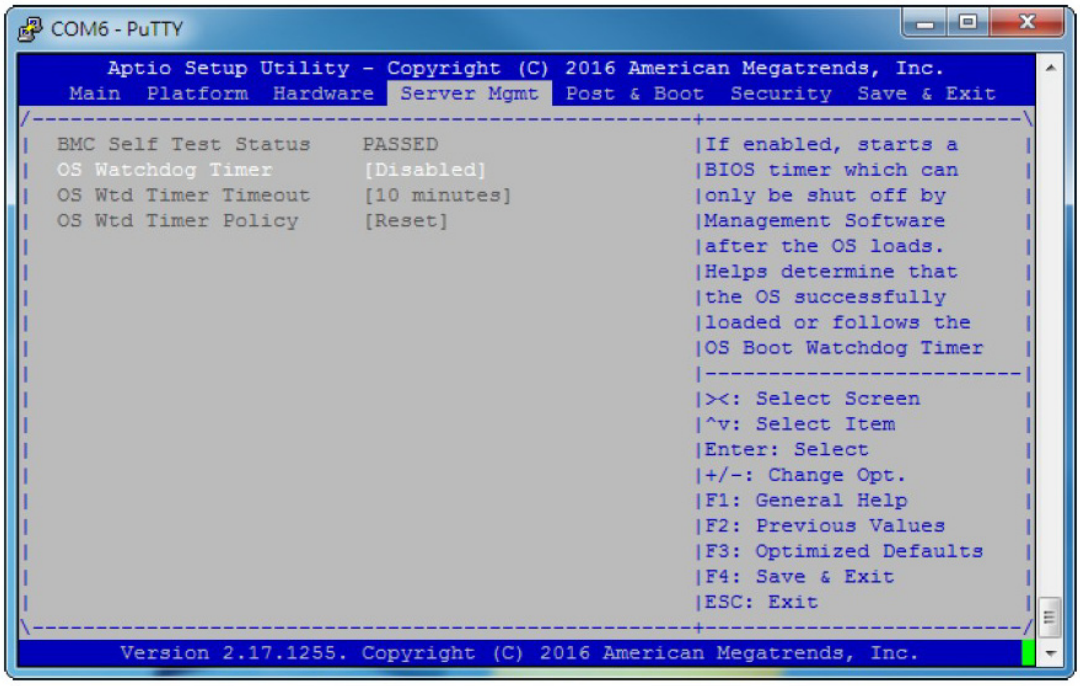

Figure 3.22 Server Management Setup

Table 3.17: Server Mgmt Configuration

Feature	Option	Description	Help text
BMC Self Test Status	N/A	Show BMC Self-Test Status	N/A
OS Watchdog Timer	Enabled Disabled	Enable or disable OS watchdog Timer	If enabled, start a BIOS timer which can only be shut off by Intel Management Software after the OS loads. Help determine that the OS successfully loaded or follow the OS Boot Watchdog Timer policy.
OS Wtd Timer Timeout	5 minutes 10 minutes 15 minutes 20 minutes	Configure the length of the OS Boot Watchdog Timer.	Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled.
OS Wtd Timer Policy	Do Nothing Reset Power Down	Configure how the system should respond if the OS Boot Watchdog Timer expires.	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.

3.7 Post and Boot Setup

The Post & Boot menu allows configuring POST behaviour and boot options.

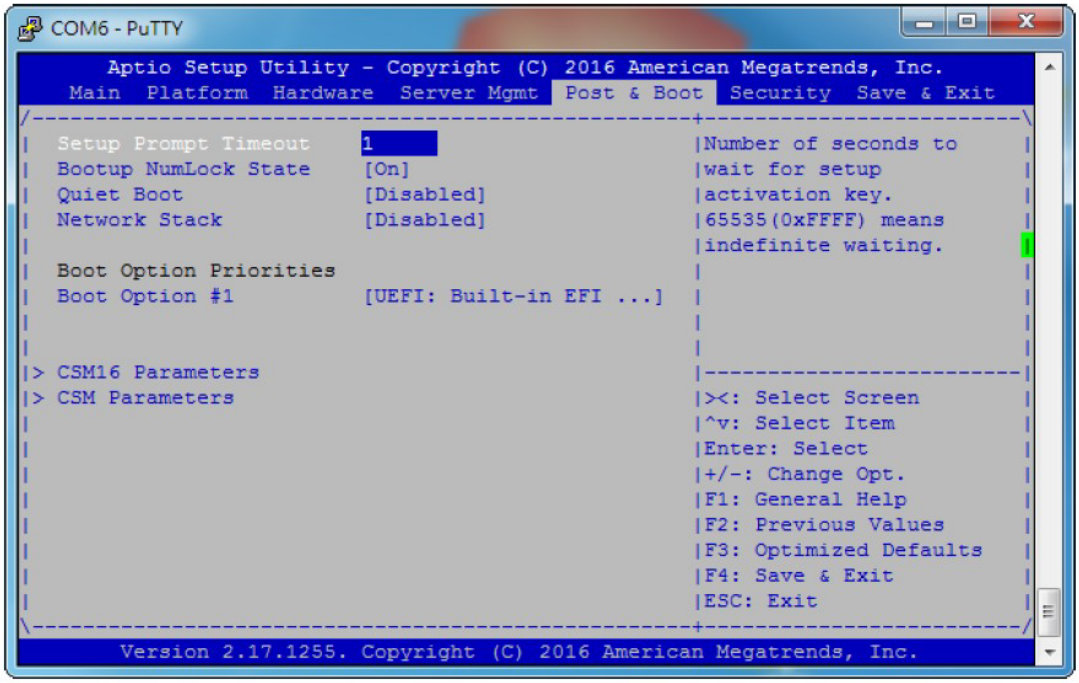

Figure 3.23 Boot Configuration

Table 3.18: Boot Configuration

Feature	Option	Description	Help text
Setup Prompt Timeout	0 to 65535 1	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	On Off	Select the keyboard NumLock state.	Select the keyboard NumLock state.
Quiet Boot	Enabled Disabled	If enabled, POST messages are not displayed on console. This might slightly speed up booting. If disabled, POS messages are displayed on console.	Enable or disable Quiet Boot option.
Network Stack	Enabled Disabled	Enable or disable UEFI Network Stack.	Enable or disable UEFI Network Stack.
Boot Option #1	XXXXXXX	Specify the priority of the available boot sources.	Specify the priority of the available boot sources.
Boot Option #2	UEFI: Built-in EFI Shell	Specify the priority of the available boot sources.	Specify the priority of the available boot sources.
Hard Drive BBS Priorities	N/A	Select sub-menu.	Set the order of the legacy devices in this group.
CSM16 Parameters	N/A	Select sub-menu.	N/A
CSM Parameters	N/A	Select sub-menu.	N/A

3.7.1 CSM16 Parameters

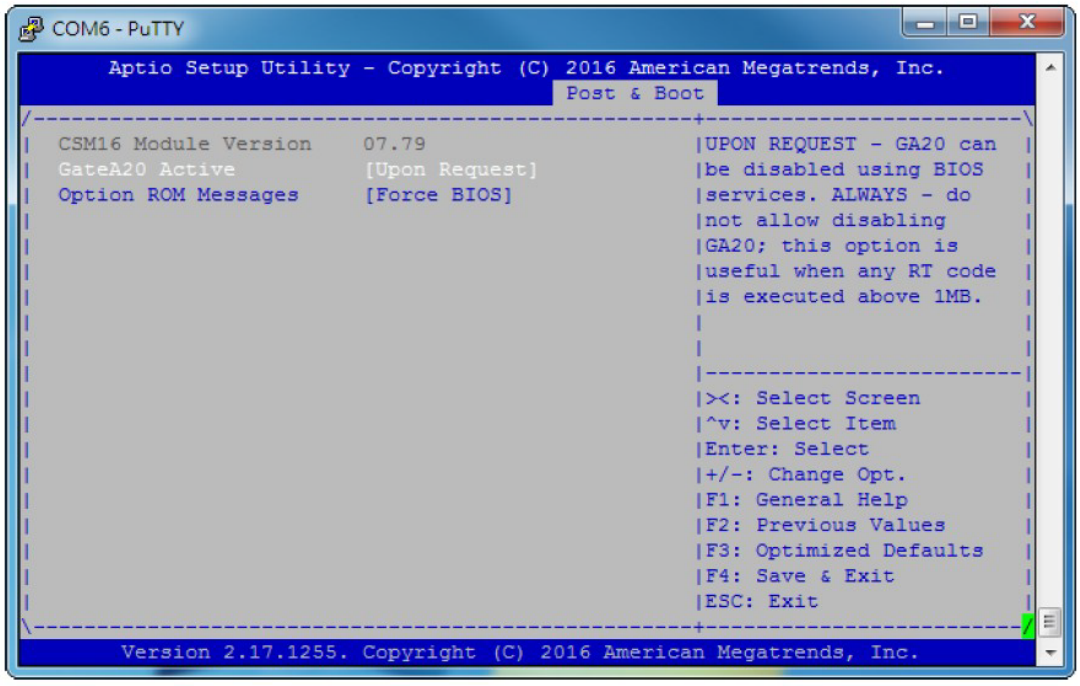

Figure 3.24 CSM16 Parameters

Table 3.19: CSM16 Parameters

Feature	Option	Description	Help text
GateA20 Active	Upon Request, Always	This function is used to enable or disable GateA20.	Upon Request – GA20 can be disabled using BIOS services. Always – do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.
Option ROM Messages	Force BIOS, Keep Current	This function is used to control the messages of the loaded PCI option ROMs.	Set display mode for Option ROM.

3.7.2 CSM Parameters

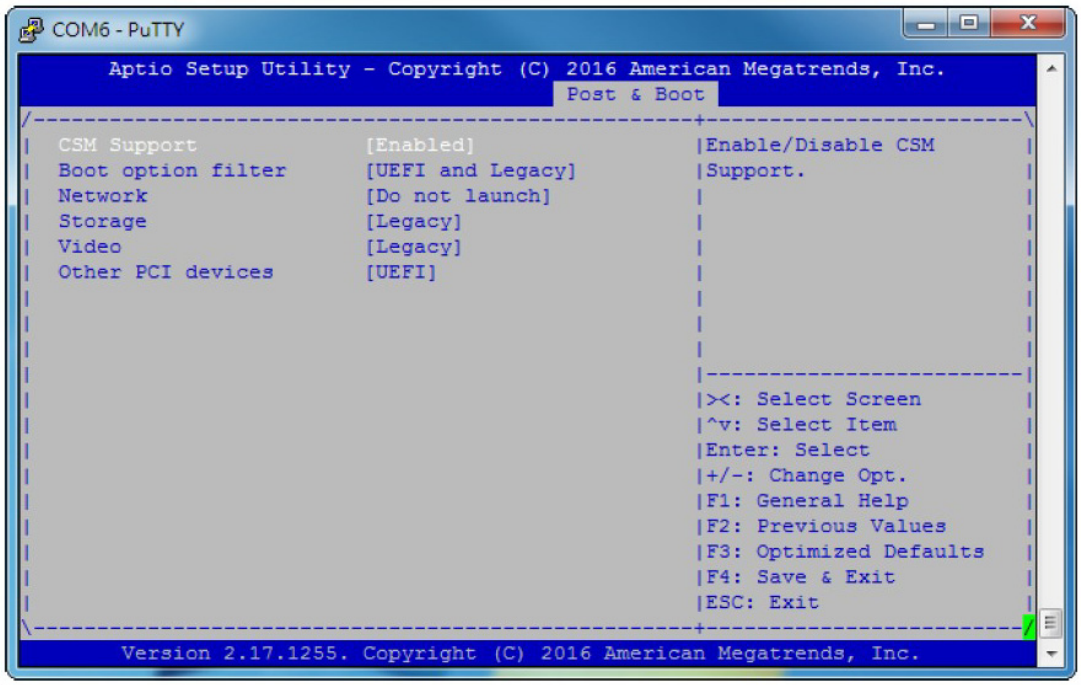

Figure 3.25 CSM Parameters

Table 3.20: CSM Parameters

Feature	Option	Description	Help text
CSM Support	Enabled Disabled	Enable/Disable CSM Support.	Enable/Disable CSM Support.
Boot option filter	UEFI and Legacy Legacy only UEFI only	This option controls Legacy/UEFI ROMs priority.	This option controls Legacy/UEFI ROMs priority.
Network	Do not Launch UEFI Legacy	Controls the execution of UEFI and Legacy PXE OpROM.	Controls the execution of UEFI and Legacy PXE OpROM.
Storage	Do not Launch UEFI Legacy	Controls the execution of UEFI and Legacy Storage OpROM.	Controls the execution of UEFI and Legacy Storage OpROM.
Video	Do not Launch UEFI Legacy	Controls the execution of UEFI and Legacy Video OpROM.	Controls the execution of UEFI and Legacy Video OpROM.
Other PCI devices	UEFI Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video.	Determines OpROM execution policy for devices other than Network, Storage, or Video.

3.8 Security Setup

The Security page allows enabling password protection and entering passwords. When logging at Administrator level, all configuration parameters can be modified.

If Administrator password is enabled and Password Check is Setup, the BIOS will prompt the user for a password before entering the setup menu.If Administrator password is enabled and Password Check is Always, the BIOS will prompt the user for a password before entering the setup menu and entering OS.If password protection is disabled, all users have administrator rights.

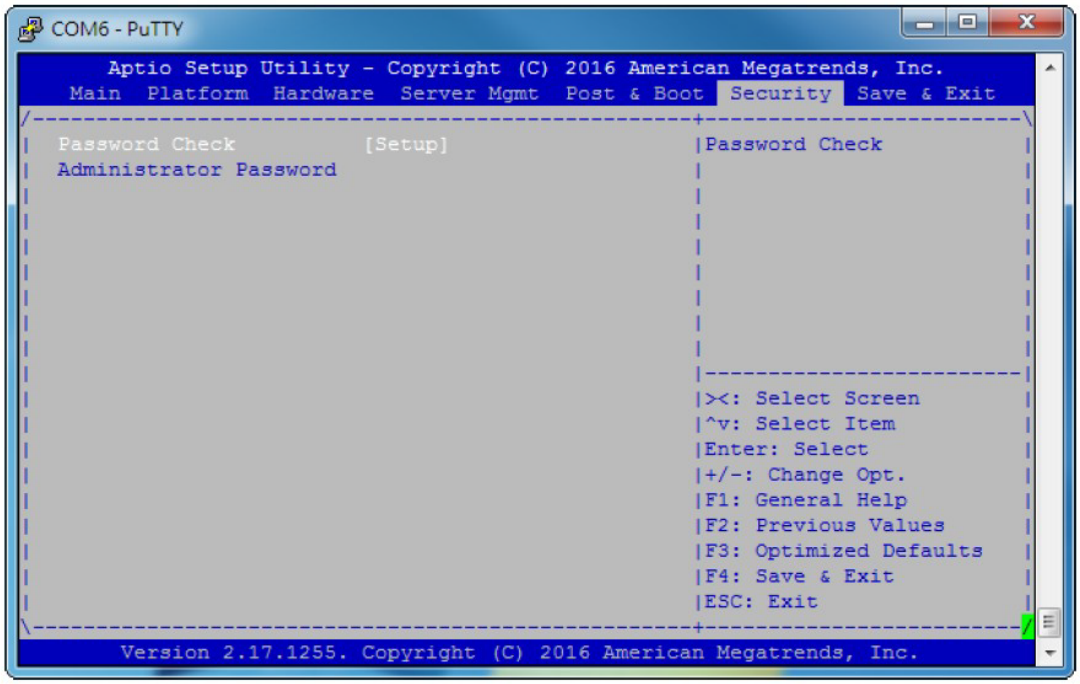

Figure 3.26 Security Configuration

Table 3.21: Security Configuration

Feature	Option	Description	Help text
Password Check	Always Setup	BIOS will prompt the user for a password before “entering the setup menu” (setup) or “entering the setup menu and entering OS” (always).	Password Check

3.9 Save and Exit Option

The Save & Exit page provides different options to exit the setup menu and to restore default values for all configuration parameters.

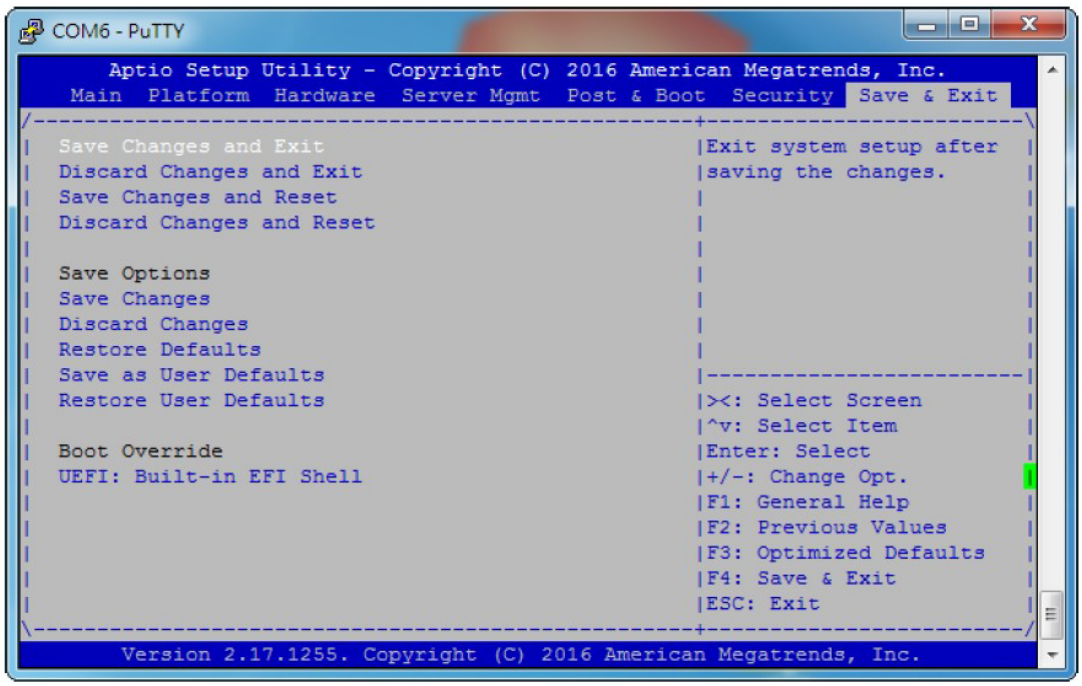

Figure 3.27 Save and Exit Configuration

Table 3.22: Save and Exit Configuration

Feature	Option	Description	Help text
Save Changes and Exit	N/A	Save modified settings into non-volatile memory and reboots the system if need.	Exit system setup after saving the changes.
Discard Changes and Exit	N/A	Discard modified settings, exit setup and continue booting the system with these old values.	Exit system setup without saving any changes.
Save Changes and Reset	N/A	Save modified settings into non-volatile memory and reboots the system.	Reset the system after saving the changes.
Discard Changes and Reset	N/A	Discard modified settings, reverts to the state when setup was entered and reboots with these old values.	Reset system setup without saving any changes.
Save Changes	N/A	Save changes of the setup option which have done so far.	Save Changes done so far to any of the setup options.
Discard Changes	N/A	Discard modifications to settings and reverts to the state when Setup was entered.	Discard Changes done so far to any of the setup options.
Restore Defaults	N/A	Load the factory default settings.	Restore/Load Default values for all the setup options.
Save as User Defaults	N/A	Save the changes done so far as User Defaults.	Save the changes done so far as User Defaults.
Restore User Defaults	N/A	Restore the User Defaults to all the setup options.	Restore the User Defaults to all the setup options.

Chapter 4

Firmware Upgrade

4.1 Chipset Software Installation Utility

4.1.1 HPM.1

The PICMG HPM.1 (Hardware Platform Management) specification defines a standard way of updating (MC) firmware components over IPMI based interfaces. Among the mechanism itself, it defines a common update file format and IPMI based commands for the update procedure.HPM.1 is the de facto standard for firmware updates in PICMG based environments.

Advanced features in HPM.1 address redundancy mechanisms, supporting both automatic and manual rollbacks, to properly support the high availability requirements in Telco platforms like AdvancedTCA.The Advantech IPMI Core supports HPM.1 updates over any of its IPMI interfaces.

As defined by the HPM.1 specification, the HPM.1 image contains a MD5 checksum over the complete image. For example the IPMITool uses this checksum to verify that the image is not corrupted.HPM.1 upgrades separate the upgrade procedure into several phases, one of this phases is the image upload, while activation is a different phase, see HPM.1 specification for the details.

4.2 HPM.1 Update Capable Components

4.2.1 Node Boards

The following table for a list of HPM.1 components is implemented on the Node blade and their respective description.

Table 4.1: Supported HPM.1 Components of Node Boards

Component	Number
IPMC Boot loader	0
IPMC Firmware	1
FPGA	2
BIOS	3
NVRAM	4

4.2.2 Bootloader Update

The bootloader HPM.1 upgrade is written to the external flash. This means there is no recovery existing for the bootloader image. It is not recommended to upgrade the bootloader in the field.U-boot always uses SPI flash 0, even if there is a copy of the bootloader in SPI flash 1, SPI flash 0 will be used for boot.

4.2.3 Firmware Update

The firmware upgrade component follows the HPM.1 specification and the upgrade and activation stage can be performed while the payload is running. In case of an update, the ShMC/IPMC is not accessible to any service while activation stage.

4.2.4 FPGA Update

The FPGA upgrade component follows the HPM.1 specification. The upgrade can be performed while the payload is running. For the activation stage, a payload part reboot and power off is required. The IPMC is not accessible to any service while activation stage.

After FPGA activation the IPMC performs a FPGA POST check, if this check fails a FPGA rollback will be initiated.

4.2.5 BIOS Update

The BIOS component requires a payload reboot or power cycle, in order to perform the activation stage. The component follows the HPM.1 standard.

4.2.6 NVRAM Update

In contrast to the other components, the NVRAM HPM.1 component provides some extended capabilities. The ShMC/IPMC can hold up to 4 NVRAM regions. Each region can be upgraded with a regular HPM.1 upgrade. The user can select the upload and activation region with issuing an OEM command to the controller.

The below figure illustrates the NVRAM section selection:

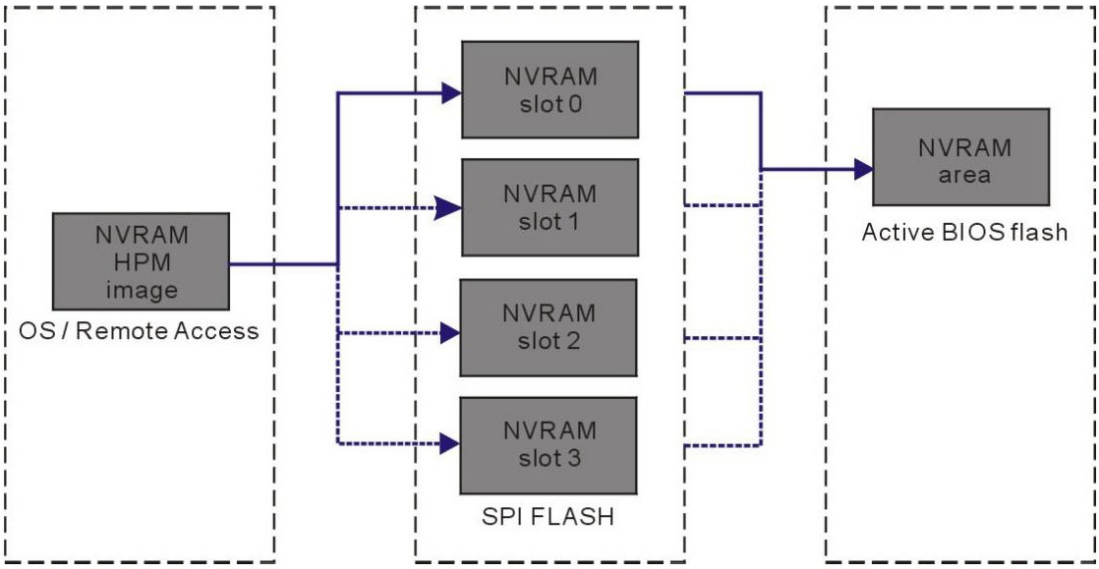

Figure 4.1 NVRAM HPM.1 Upgrade

4.3 HPM.1 Upgrade Procedure

4.3.1 Using the IPMItool

The IPMItool is an open source software which is already available in most of the Linux distributions.Besides many other IPMI commands, it supports an easy of the HPM.1 update mechanism, through different IPMI channels/interfaces. For the HPM.1 update, the “lanplus” interface is recommended as it is faster compared to payload interface (KCS).

ipmitool —I lanplus —H 192.168.1.1<ShMC or IPMC IP> —U administrator —P advantech

IPMItool call to use the lanplus interface

The Advantech IPMI firmware supports HPM.2 long messages which increases the IPMI message payload size and therefore decreases the upload time. IPMItool version >1.8.15 automatically support HPM.2 long messages on the lanplus interface.

If the network is considered safe and no unauthorized persons do have access the parameter “-C 1”can be used to force Cipher Suites 1, which is less secure but will decrease the required upload time.

4.3.2 Retrieve Currently Installed Versions

For KCS interface:

 # ipmitool hpm check

or for RMCP+ interface:

 # ipmitool -I lanplus -H 169.254.10.254 -U administrator -P advantech hpm check

PICMG HPM.1 Upgrade Agent 1.0.9:

-------Target Information-------
Device Id : 0x84
Device Revision : 0x81
Product Id : 0x8303
Manufacturer Id : 0x2839 (Unknown (0x2839))

ID	Name	Versions		
		Active	Backup	Deferred
0	8303 BL	0.30 00000000		
1	8303 IPMC	0.30 00000000	0.30 00000000	
* 2	8303FPGA	0.14 00000000	0.14 00000000	
* 3	8303 BIOS	1.02 00000000	1.02 00000000	
* 4	8303 NVRAM	4.00 00000000		

(*) Component requires Payload Cold Rese t

4.3.3 Upgrade

 # ipmitool -I lanplus -H 169.254.10.254 -U administrator -P advantech hpm upgrade esp9001_shmc_1.07.img

PICMG HPM.1 Upgrade Agent 1.0.9:

Validating firmware image integrity...OK
Performing preparation stage...
Services may be affected during upgrade. Do you wish to continue? (y/n): y <- Press ‘y’ and ‘Enter’ key
OK

Performing upgrade stage:

```
-------------------------------------------------------------------------------------------------------------
|ID       | Name              |                    Versions                          | %   |
|         |                   |   Active          |   Backup          |   File       |     |
|-------  |-------------------|-------------------|-------------------|--------------|-----|
|   0     |8303 BL            | 0.30 00000000  |0.30 00000000   |1.00 00000000|100%||
|Upload Time: 00:47                               | Image Size: 109834 bytes|
-------------------------------------------------------------------------------------------------------------
```

(*) Component requires Payload Cold Rese t

Firmware upgrade procedure success

4.3.4 Activate

 # ipmitool -I lanplus -H 169.254.10.254 -U administrator -P advantech hpm activate

PICMG HPM.1 Upgrade Agent 1.0.9:
Waiting firmware activation

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com