



Полное руководство пользователя

BIOS Gen3

Тринити

2026-07-27

серверы.тринити.рф

Оглавление

1. Введение.....	3
2. Введение.....	4
2.1. Общие стандарты.....	4
2.2. Терминология.....	5
3. Обзор проекта.....	6
3.1. Блок-схема системы.....	6
3.2. Сводка.....	7
3.3. Перемычки.....	8
4. Системная информация.....	9
4.1. Информация о процессоре.....	9
4.2. Информация о памяти.....	11
4.3. Информация о встроенном SATA.....	14
4.4. Информация о BMC.....	18
5. Общие функции.....	19
5.1. Установка системной даты.....	19
5.2. Установка пароля администратора и пользователя.....	21
5.3. Установка режима загрузки BIOS.....	23
6. Настройки BIOS.....	25
6.1. Main.....	25
6.2. Advanced.....	28
6.3. Platform Configuration.....	72
6.4. Socket Configuration.....	102
6.5. Server Mgmt.....	136
6.6. Security.....	144
6.7. Boot.....	147
6.8. Save & Exit.....	149
7. Обновление BIOS.....	151
7.1. Прошивка BIOS в UEFI Shell.....	151
7.2. Прошивка BIOS в Windows.....	152
7.3. Прошивка BIOS в Linux.....	153
8. Контрольные точки.....	154
8.1. Фазы прошивки UEFI Framework.....	154
8.2. Контрольные точки AMI.....	155

1. Версии

Ревизия	Дата	Описание	Автор

2. Введение

Данное руководство применимо к серверу Luxshare-ICT Hamburg (процессоры серии Intel Ice Lake).

2.1. Общие стандарты

Ссылка	Название документа	Номер документа
01	UEFI Specification	Version 2.7, May,2017
02	Advanced Configuration and Power Interface Specification	Version 5.0, Nov,2011
03	PCI Express® Base Specification	Vision 4.0, Sep,2017
04	System Management BIOS (SMBIOS) Reference Specification	Version 3.0.0, Feb,2015
05	Intelligent Platform Management Interface Specification	Version 2.0., Jun,2004

Таблица 0-1 Справочные документы общих стандартов

2.2. Терминология

Термин	Описание
ACPI	Advanced Configuration and Power Interface
BBS	BIOS Boot Specification
DIMM	Dual Inline Memory Module
SMBIOS	System Management BIOS
SMBIOS	System Management Interrupt
SPD	Serial Presence Detect

Таблица 0-2 Терминология

3. Обзор проекта

3.1. Блок-схема системы



Рисунок 0-1 Блок-схема системы

3.2. Сводка

Компонент	Тип
Процессор	Intel ICX CPU
ВМС	Aspeed AST2500
Память	RDIMM, 3DS-RDIMM, LRDIMM, 3DS-LRDIMM и Crow Pass DIMM 8каналов/сокет DDR4, 2 DIMM/канал Макс. частота: 3200MT/s @1DPC, 2933MT/s @2DPC)
Поддержка ОС	Linux: Ubuntu, CentOS
BIOS	AMI AptioV Core Base (UEFI)
Flash ROM	MX25Lxxx/32MB

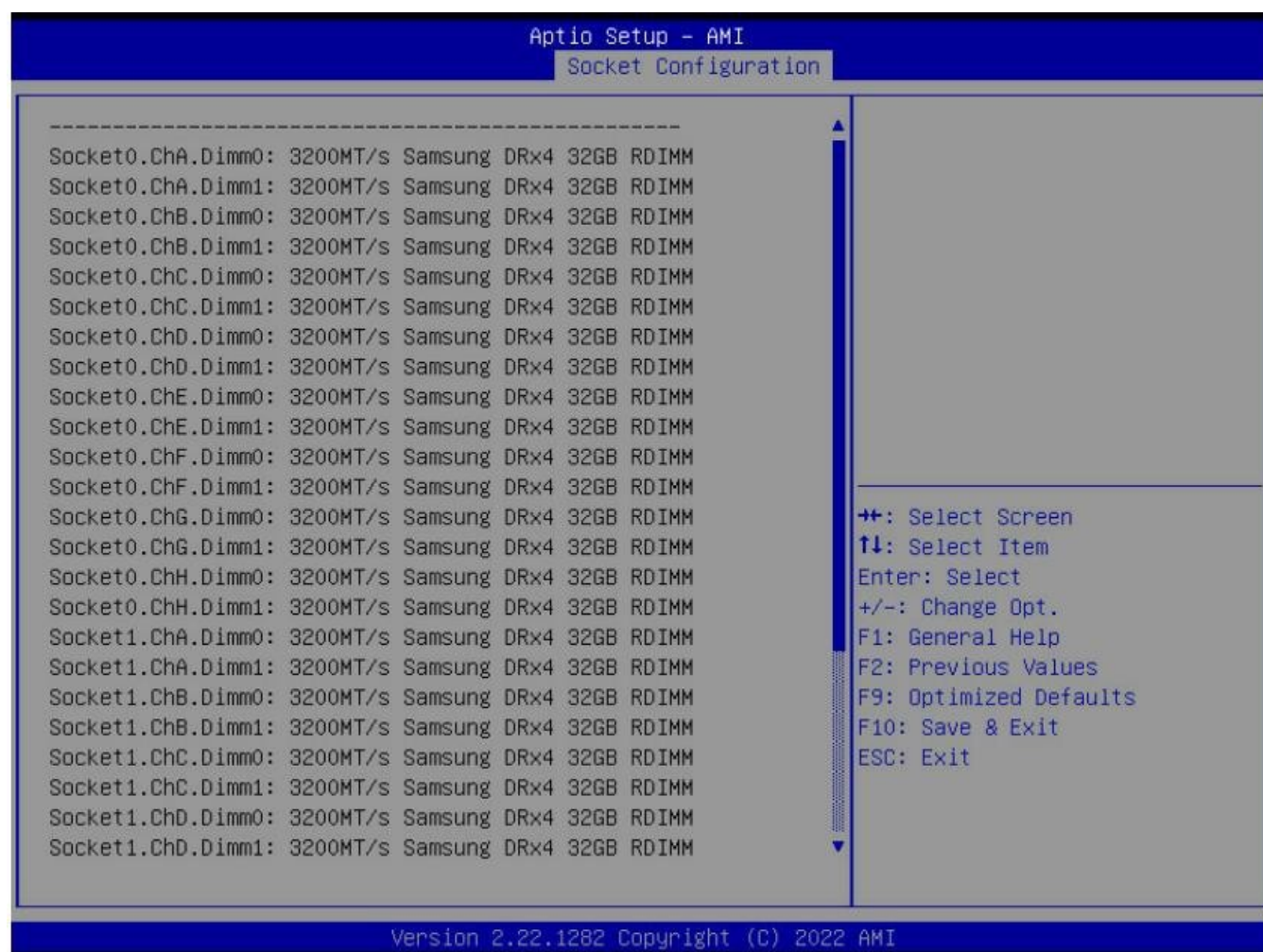


Таблица 0-1 Сводка

3.3. Переключки

J15	Программный триггер NMI
J16	Режим производства
J17	Очистка пароля
J27	Режим восстановления BIOS
J32	Режим восстановления ME
J53	Очистка CMOS

Таблица 0-2 Переключки

4. Системная информация

Отображение системной информации в настройках BIOS.

4.1. Информация о процессоре

```

Aptio Setup - AMI
Main Advanced Platform Configuration Socket Configuration Server Mgmt Security Boot >
/-----/
|> PCH Configuration                               |Displays and provides option |
|> Miscellaneous Configuration                     |to change the PCH Settings |
|> Server ME Configuration                         |                           |
|> Runtime Error Logging                           |                           |
|-----|
|Setup Warning:                                    |                           |
|Setting items on this Screen to incorrect values  |                           |
|may cause system to malfunction!                  |                           |
|-----|
|><: Select Screen                                |                           |
|^v: Select Item                                  |                           |
|Enter: Select                                    |                           |
|+/-: Change Opt.                                |                           |
|F1: General Help                                |                           |
|F2: Previous Values                             |                           |
|F9: Optimized Defaults                          |                           |
|F10: Save & Exit                                |                           |
|ESC: Exit                                       |                           |
|-----|
Version 2.22.1282 Copyright (C) 2021 AMI

```

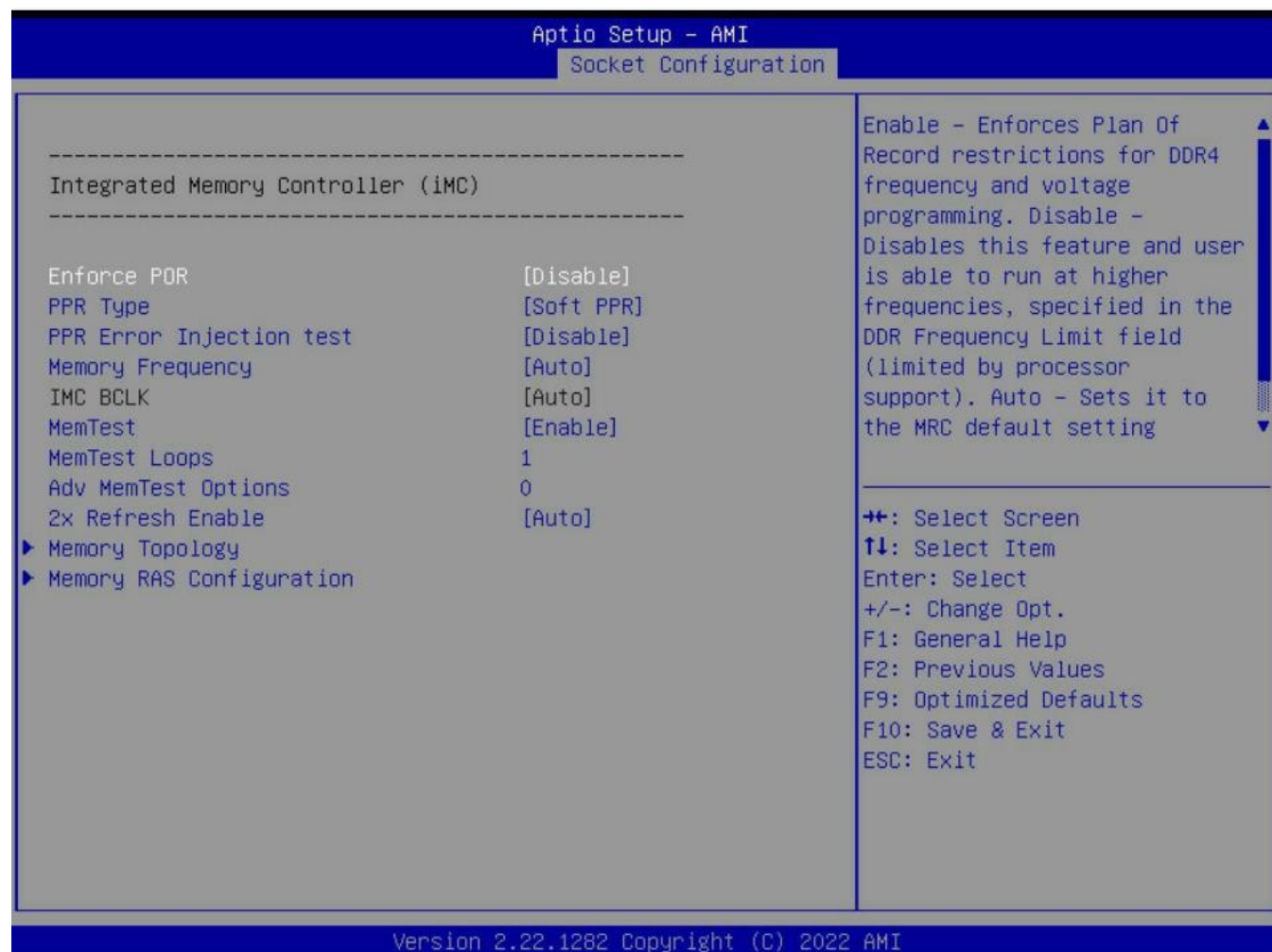
Загрузитесь в настройки BIOS, перейдите в **Socket Configuration->Processor Configuration**.



Рисунок 0-1 Конфигурация процессора

4.2. Информация о памяти

Загрузитесь в настройки BIOS, перейдите в **Socket Configuration->Memory Configuration**.



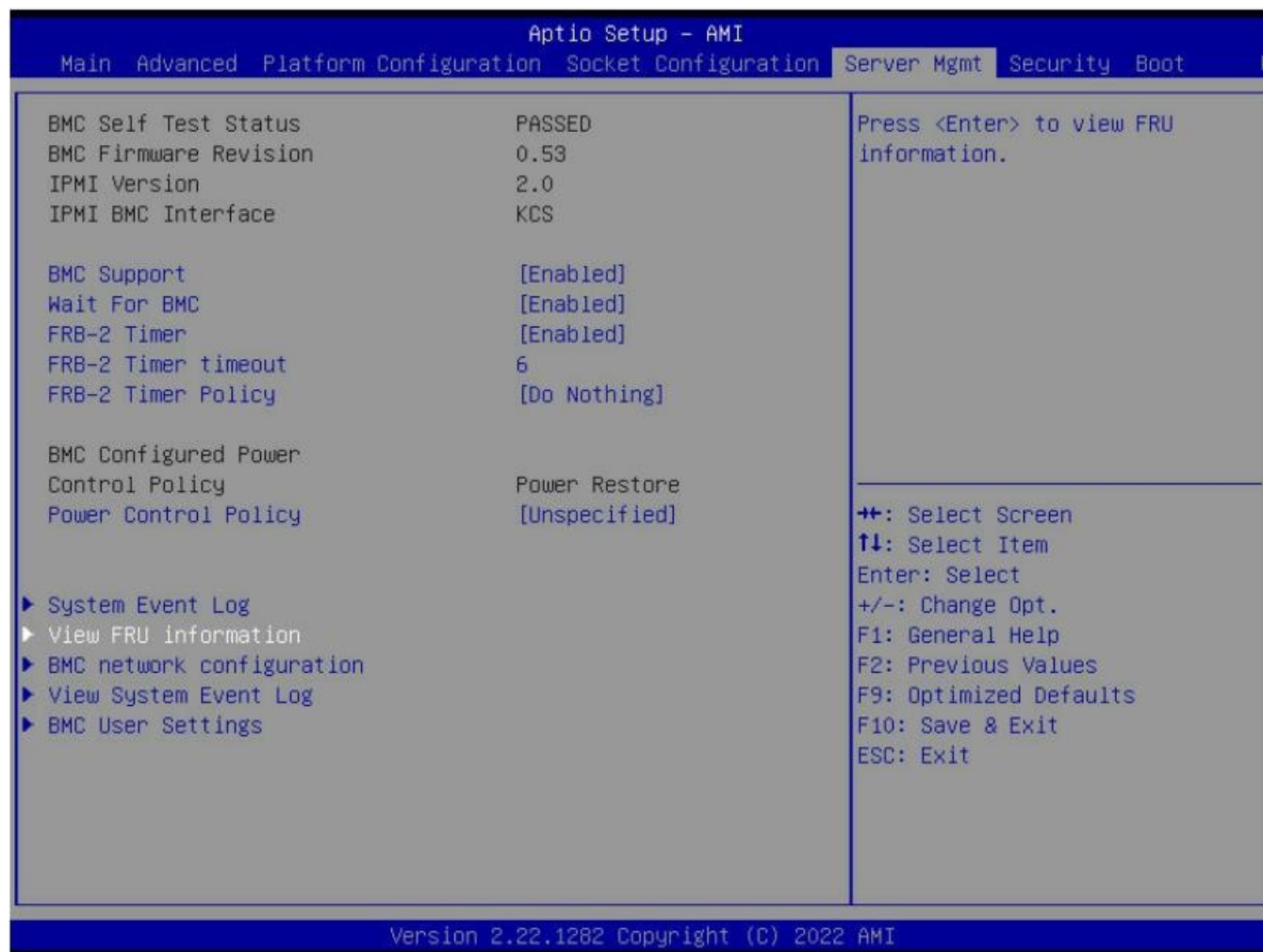


Рисунок 0-2 Конфигурация памяти

Выберите **Memory Topology** для просмотра всей информации о памяти.

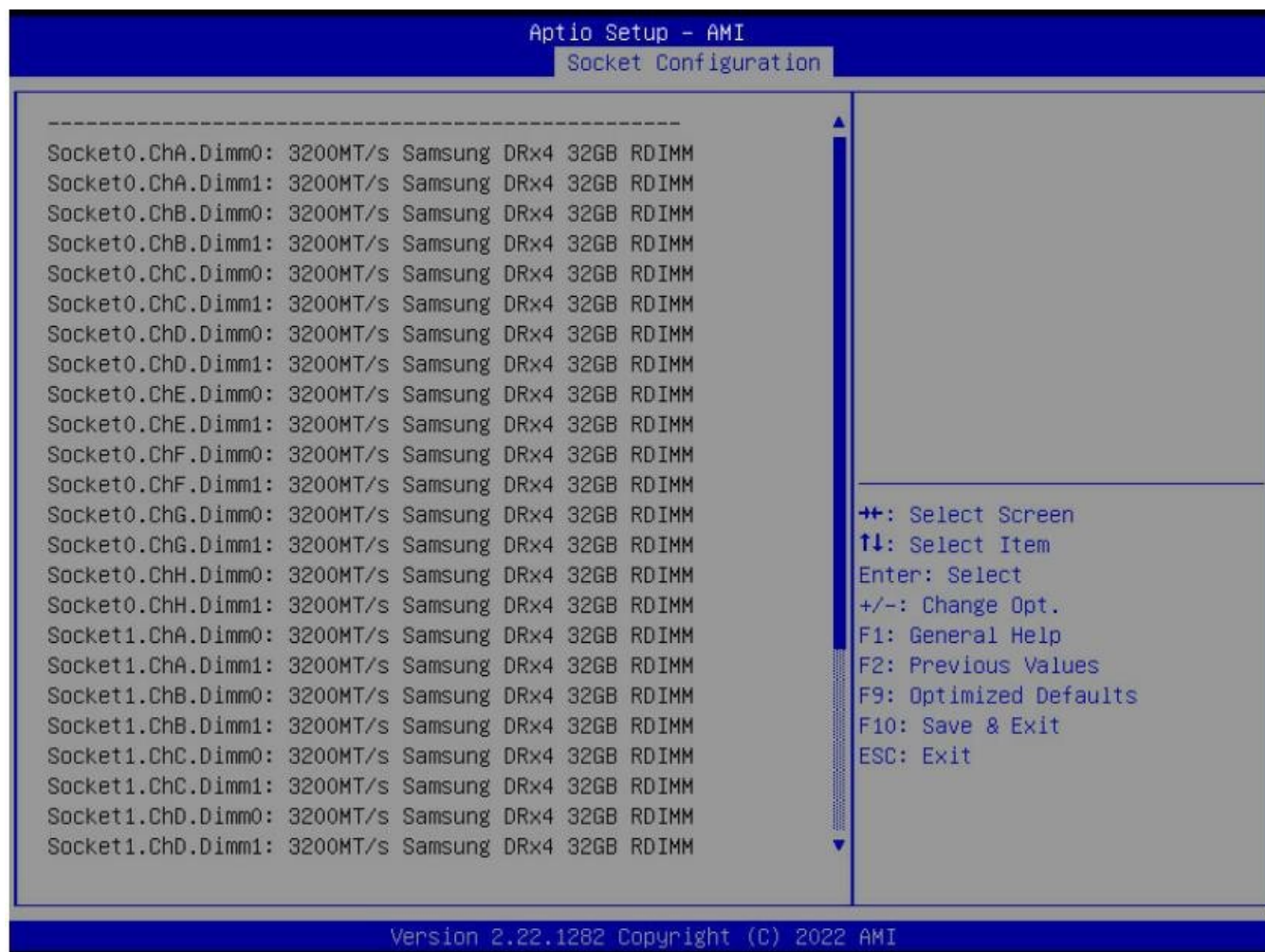
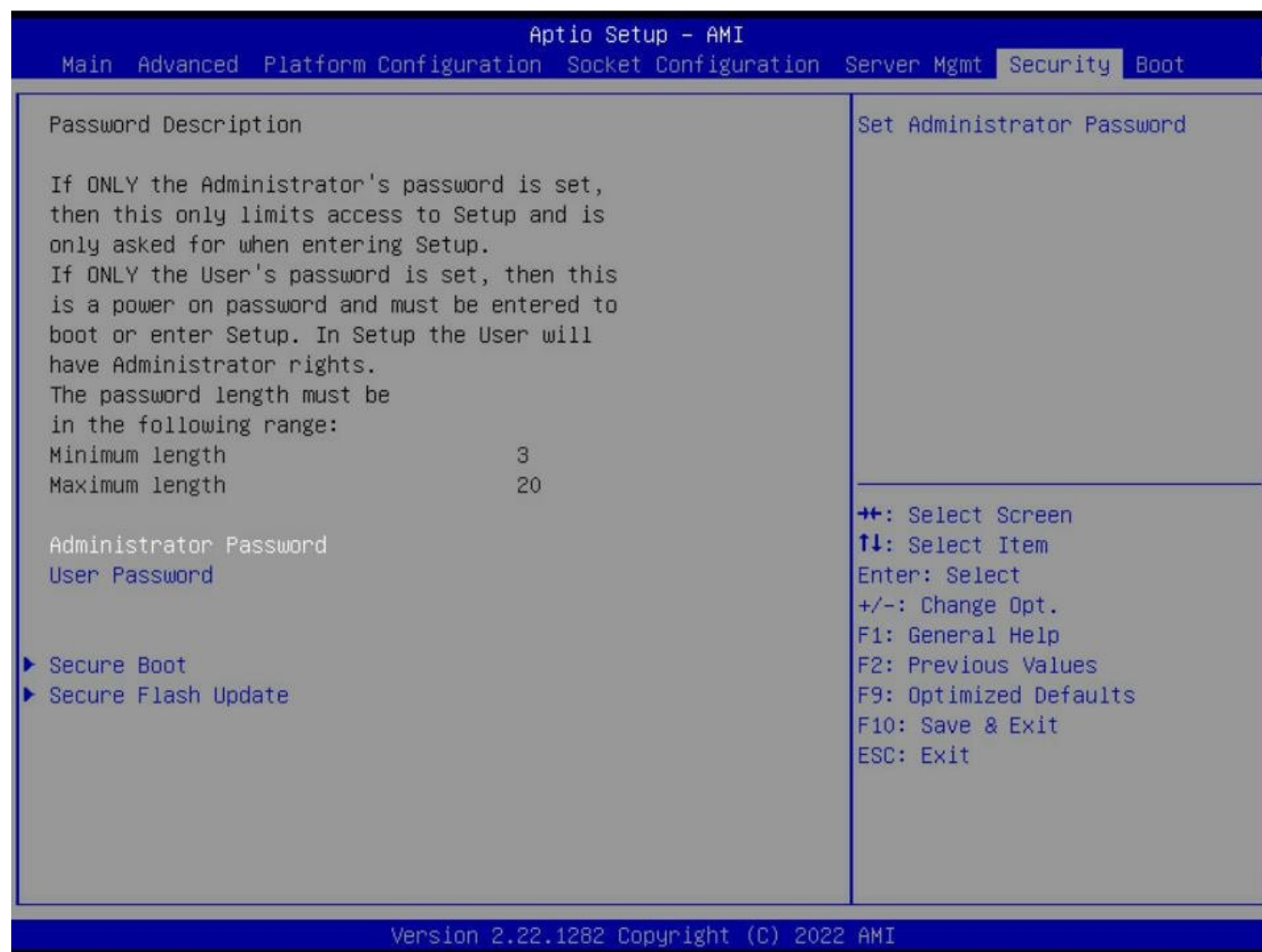


Рисунок 0-3 Топология памяти

4.3. Информация о встроенном SATA



Загрузитесь в настройки BIOS, перейдите в **Platform Configuration -> PCH Configuration**.

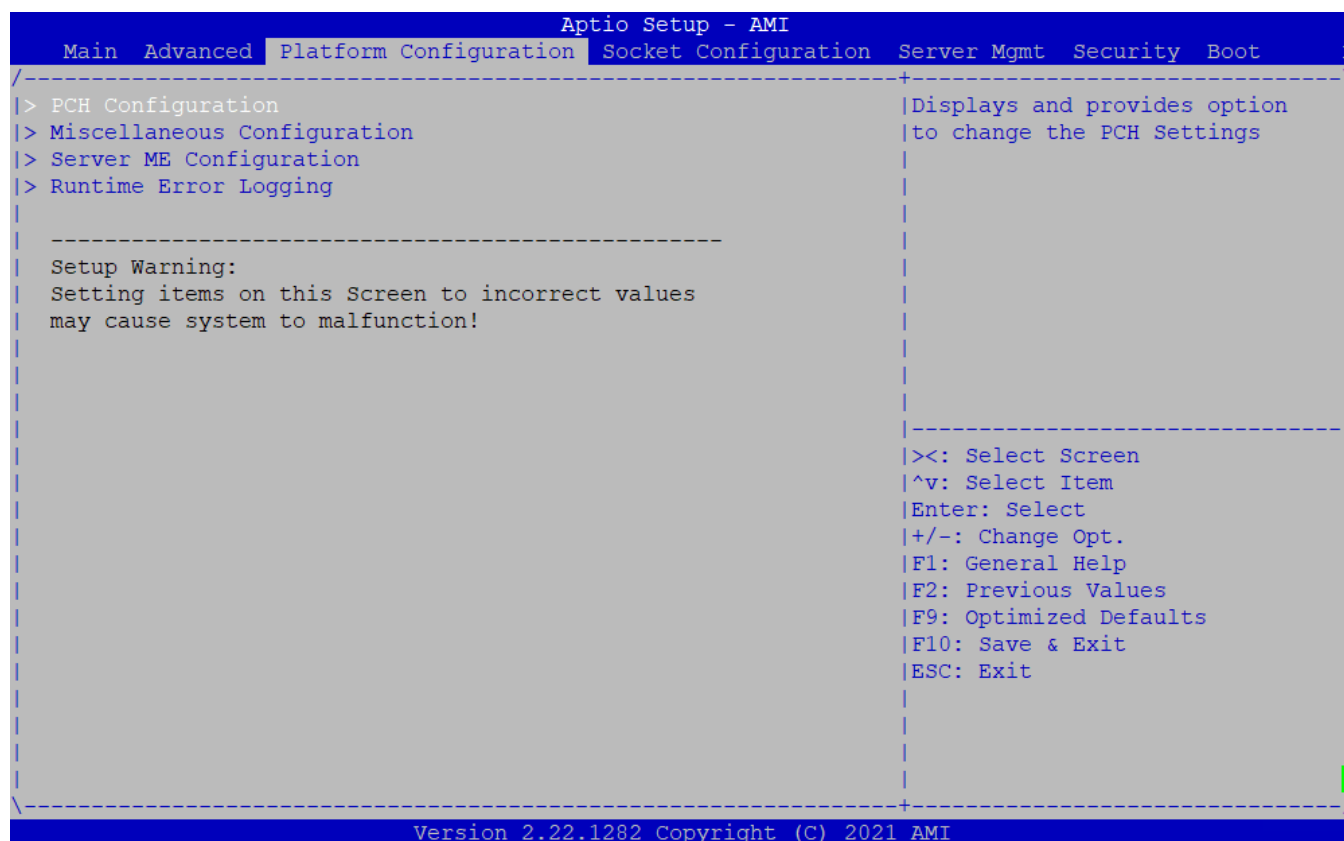


Рисунок 0-4 Конфигурация платформы

Выберите PCH SATA Configuration или PCH sSATA Configuration для просмотра всей информации о SATA или sSATA.

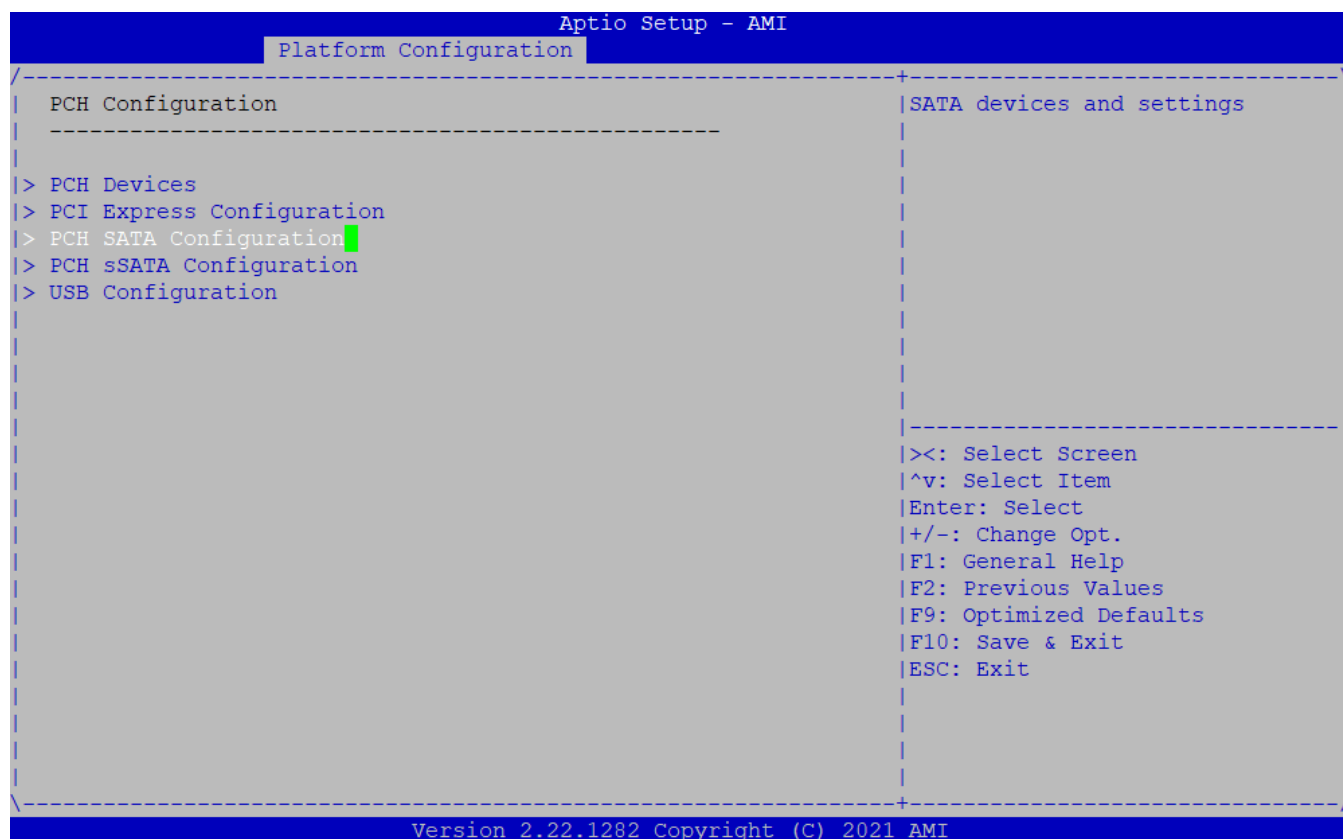
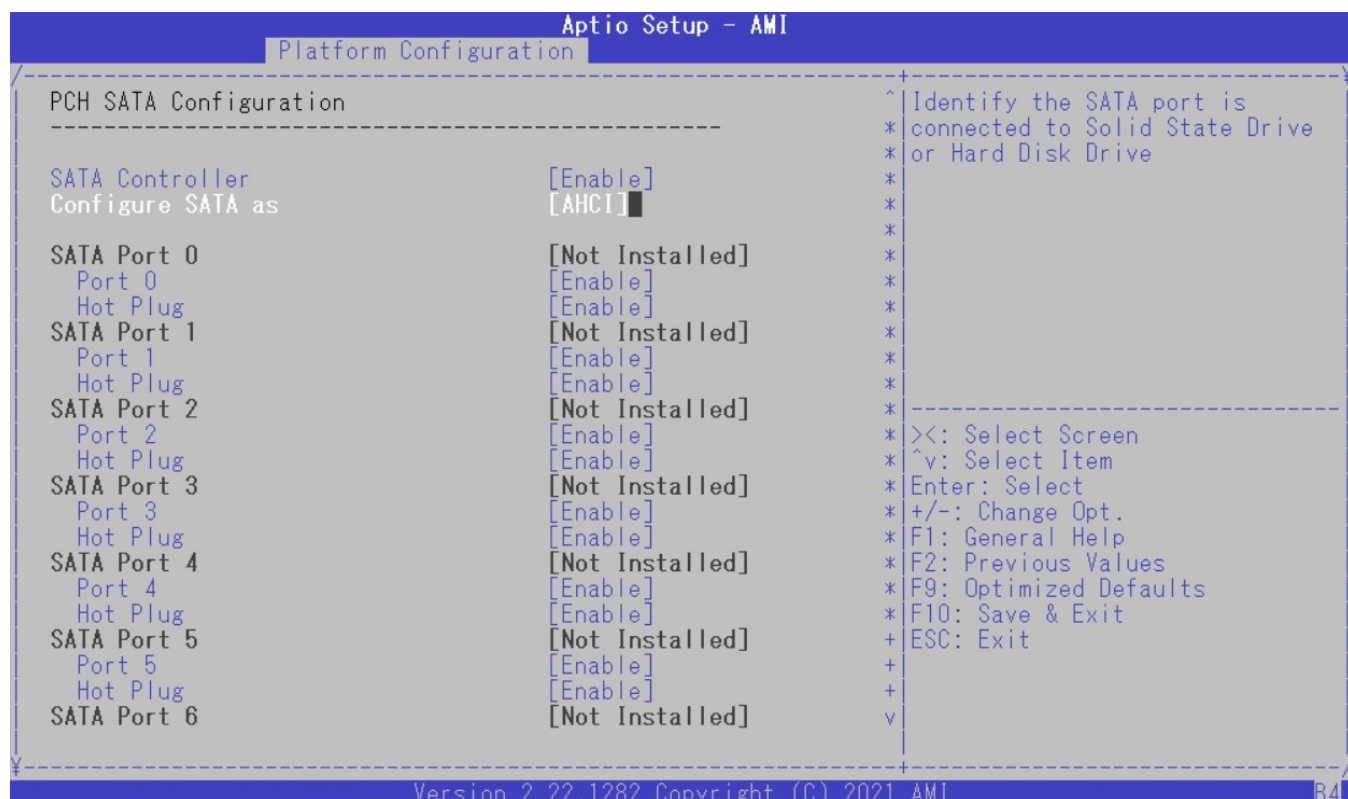


Рисунок 0-5 Конфигурация PCH



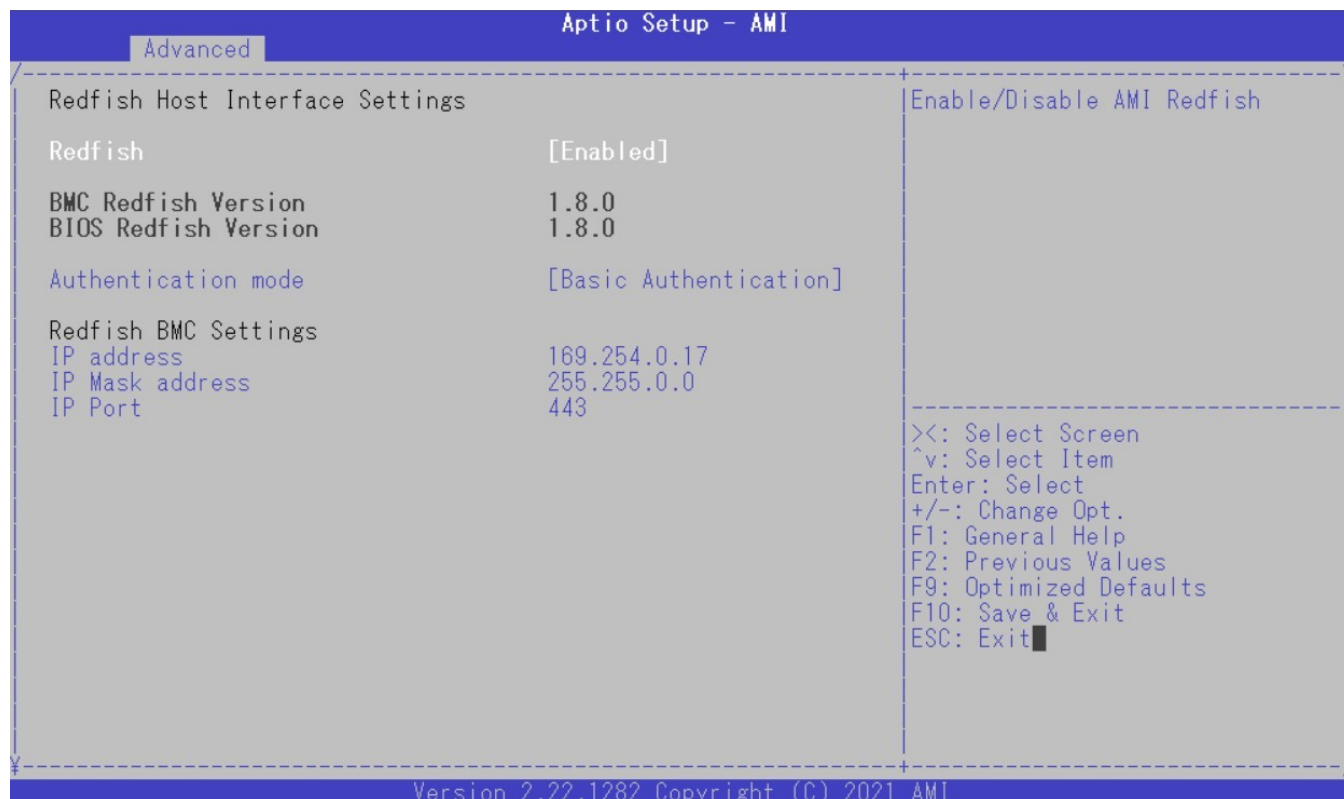


Рисунок 0-6 Конфигурация PCH SATA

4.4. Информация о BMC

Загрузитесь в настройки BIOS, перейдите в **Server Mgmt.** BIOS отобразит **BMC Self-Test Status**, **BMC Device ID**, **BMC Firmware Revision**, **IPMI Version**, **IPMI BMC Interface**.

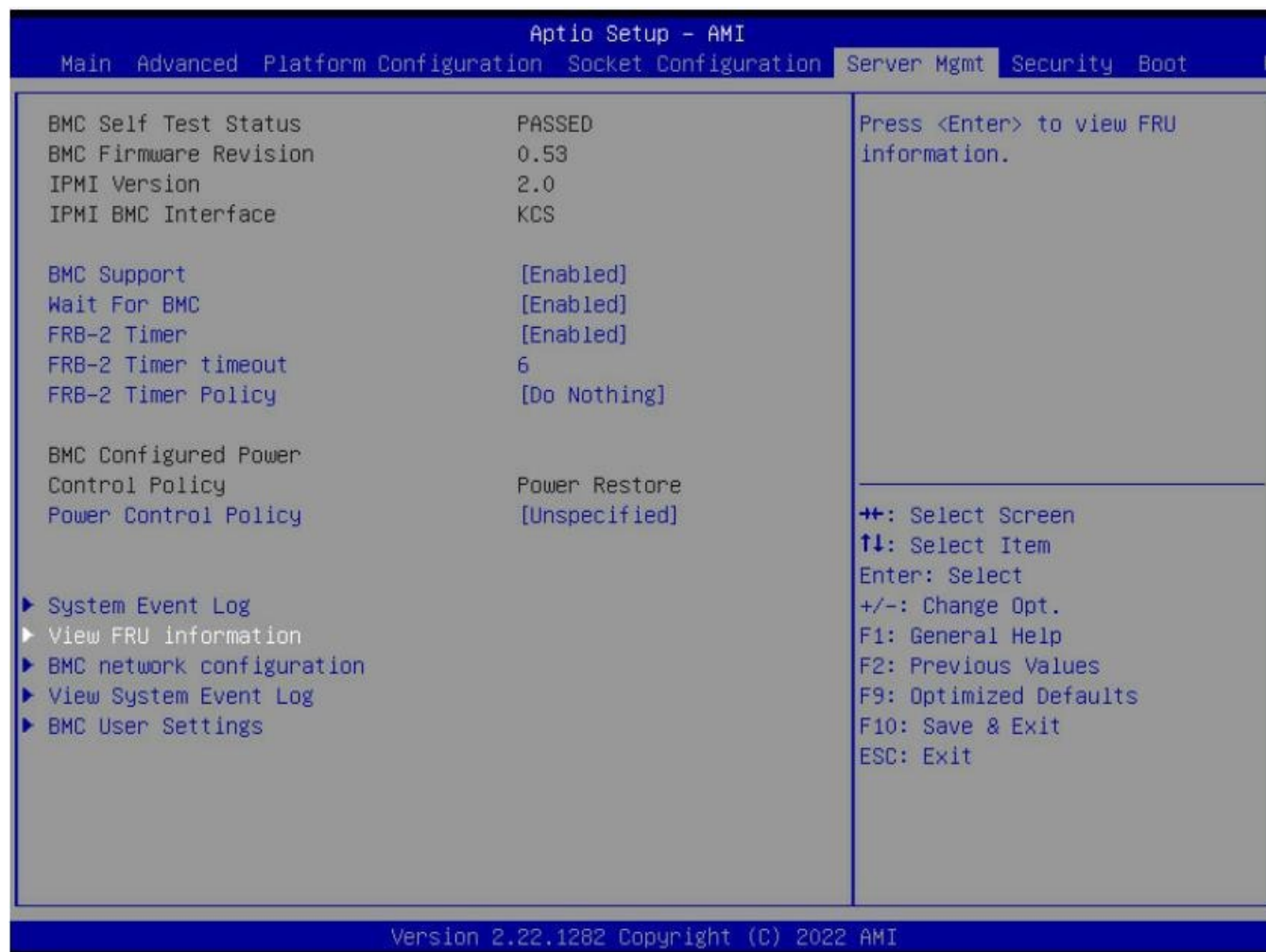


Рисунок 0-7 Информация о BMC

5. Общие функции

5.1. Установка системной даты



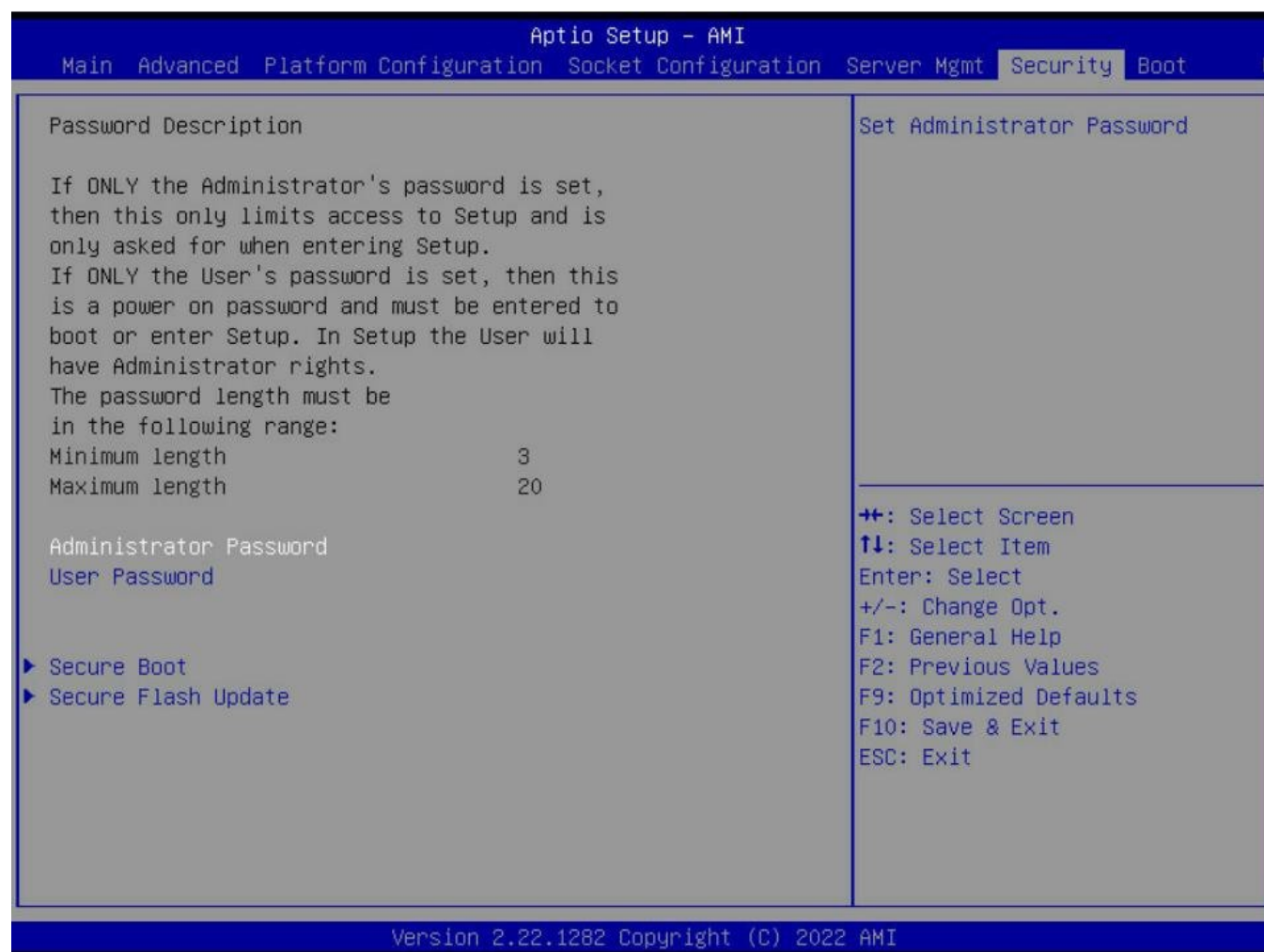
Загрузитесь в настройки BIOS, перейдите в **Main**. Выберите **System Date** и **System Time** для изменения системной даты.



Рисунок 0-8 Системная дата

5.2. Установка пароля администратора и пользователя

Загрузитесь в настройки BIOS, перейдите в **Security**. Выберите **Administrator Password** для установки пароля администратора, выберите **User Password** для установки пароля пользователя.



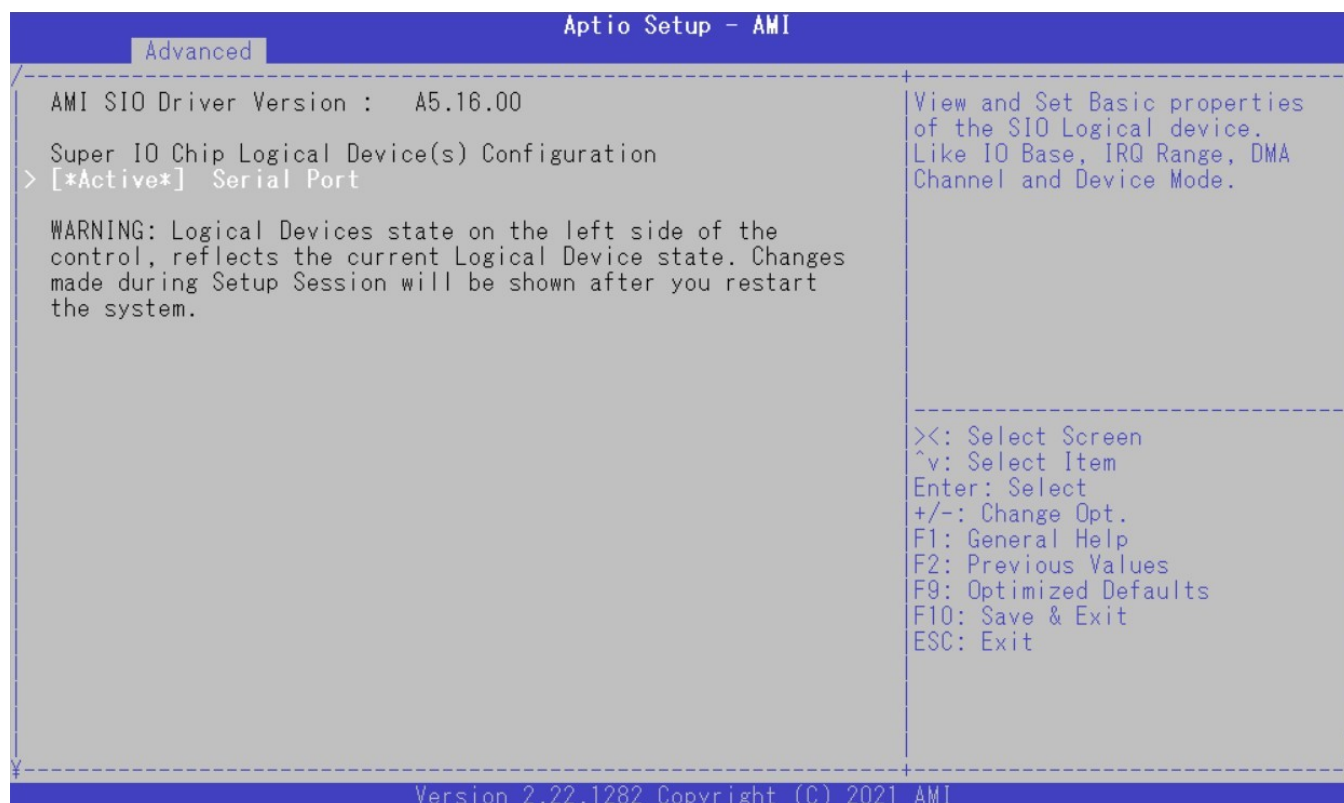
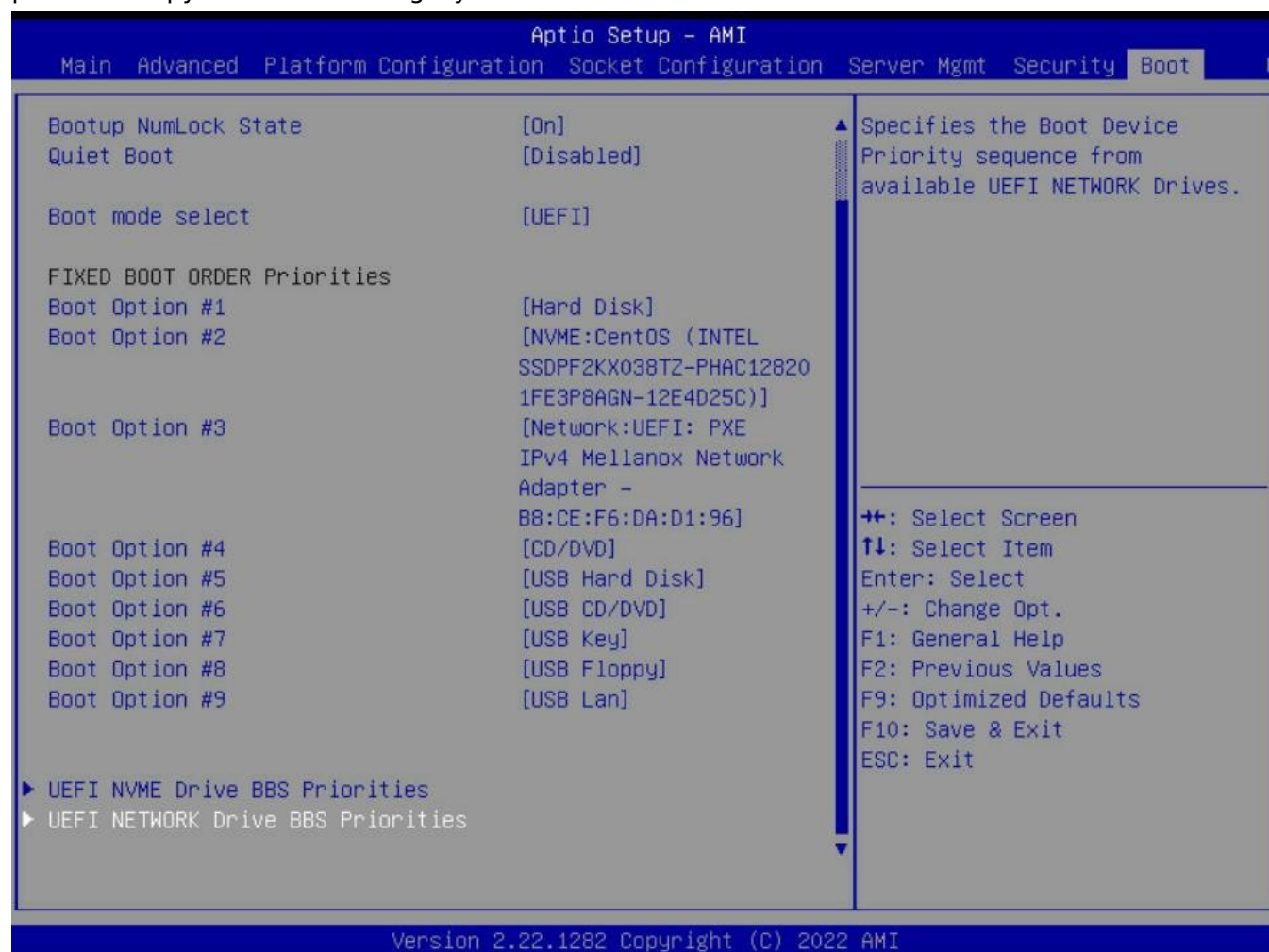


Рисунок 0-9 Пароль администратора и пользователя

5.3. Установка режима загрузки BIOS

Загрузитесь в настройки BIOS, перейдите в **Boot**. Выберите **Boot Mode Select** для установки режима загрузки: UEFI или Legacy.



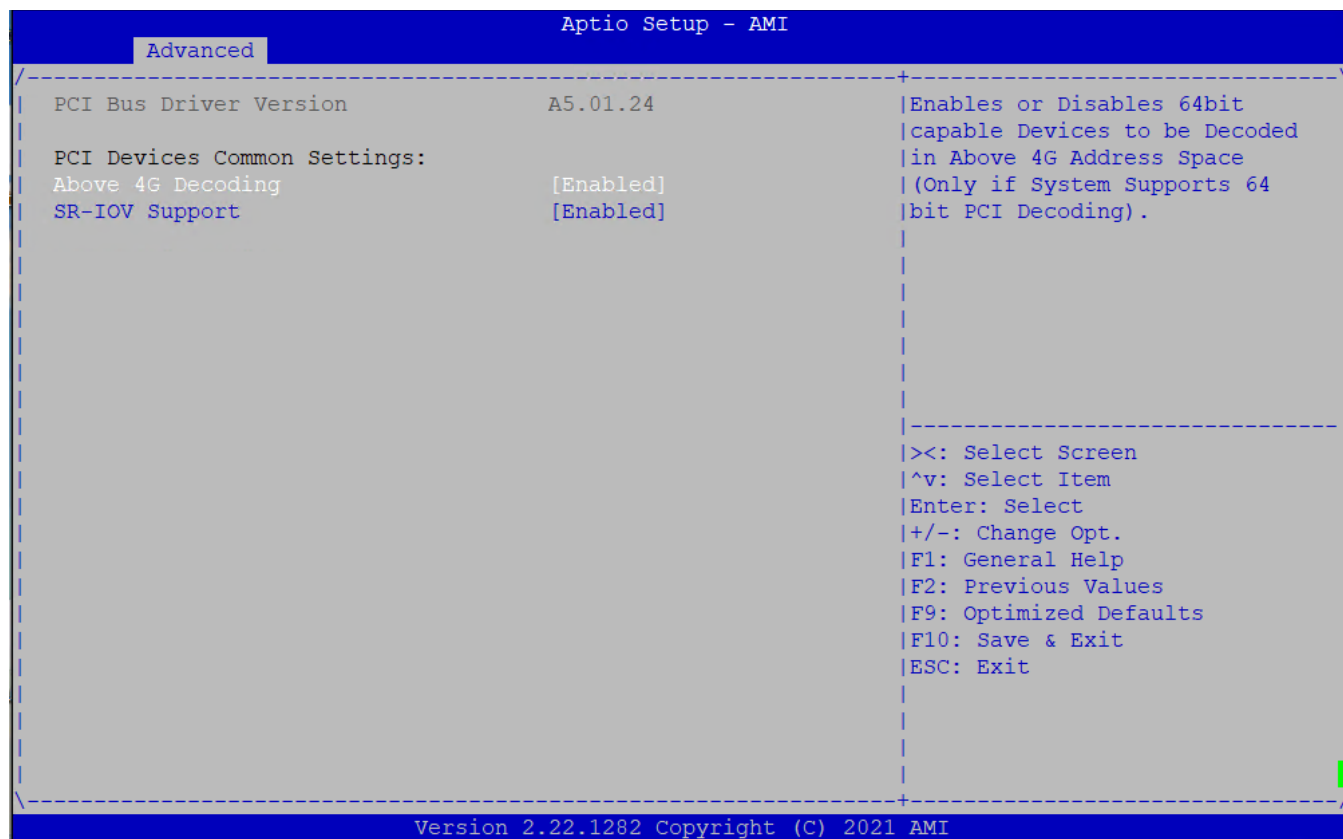


Рисунок 0-10 Режим загрузки BIOS

6. Настройки BIOS

Меню настроек BIOS в верхней части экрана BIOS содержит следующие основные разделы:
Main:

6.1. Main

Страница **Main** показана на **Рисунке 6-1**, она включает информацию о BIOS, информацию о памяти, язык системы, системную дату и время.

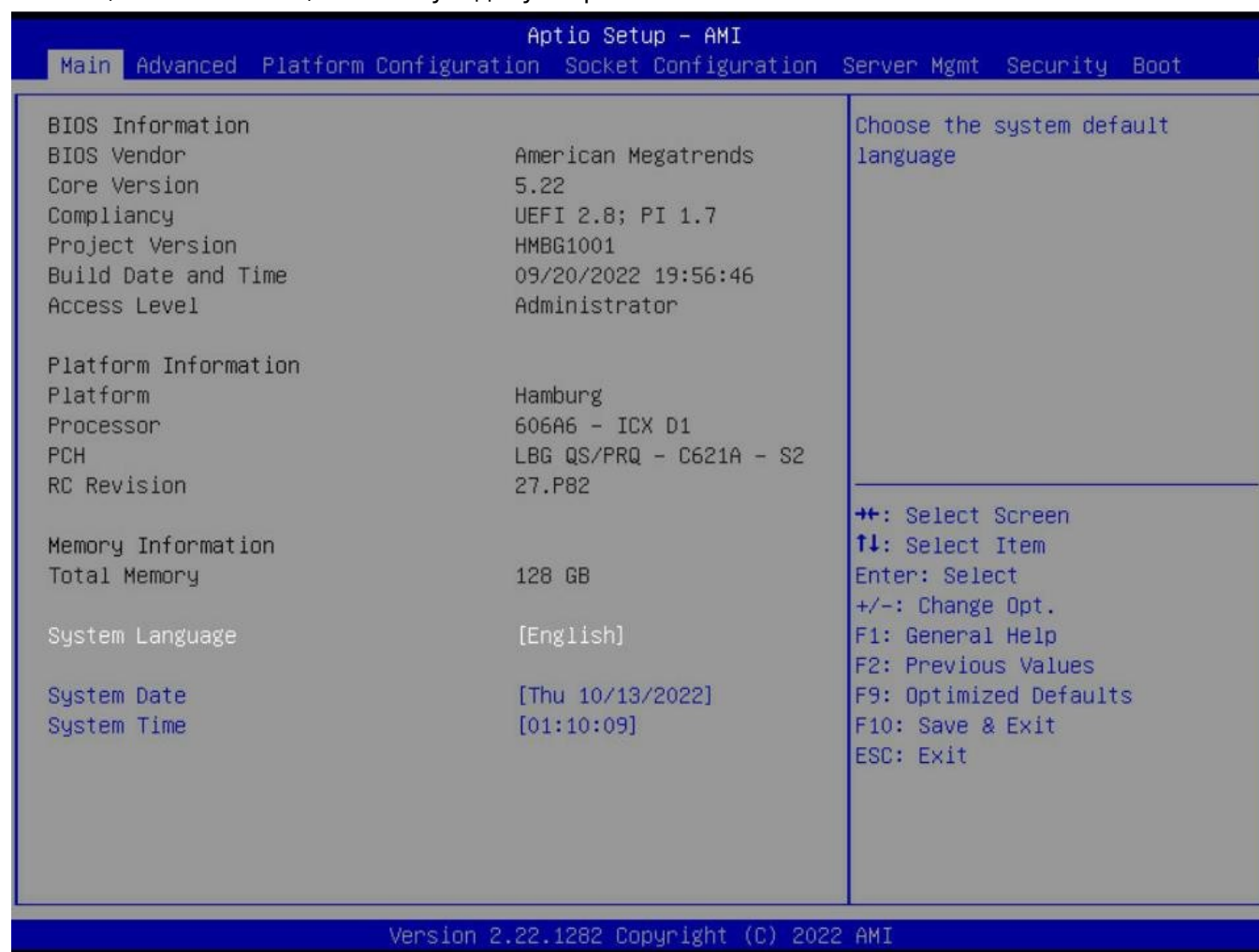


Рисунок 0-1 Main

Настройка BIOS	Опции	Описание	
BIOS Information	BIOS Information	Информация о BIOS	
BIOS Vendor	American Megatrends		
Project Version	HBDLxxyyzz	major.minor.build(x x.yy.zz)	
Build Date and Time	MM/DD/YYYY	Месяц/День/Год	

Project Version	HBDLxxyyzz	major.minor.build(x x.yy.zz)	
	HH:MM:SS	Час/Минута/Секунда	
Access Level	Administrator/ User		
Memory Information	Memory Information	Информация о памяти	
Total Memory	Read Only	Показывает общий объем памяти, установленной на материнской плате	
System Language	English	Выбор языка системы по умолчанию	
System Date (MM/DD/YYYY)	MM/DD/YYYY	Установка даты. Используйте клавишу Tab для переключения между полями даты.	
System Time (HH:MM:SS)	HH:MM:SS	Установка времени. Используйте клавишу Tab для переключения между полями времени.	

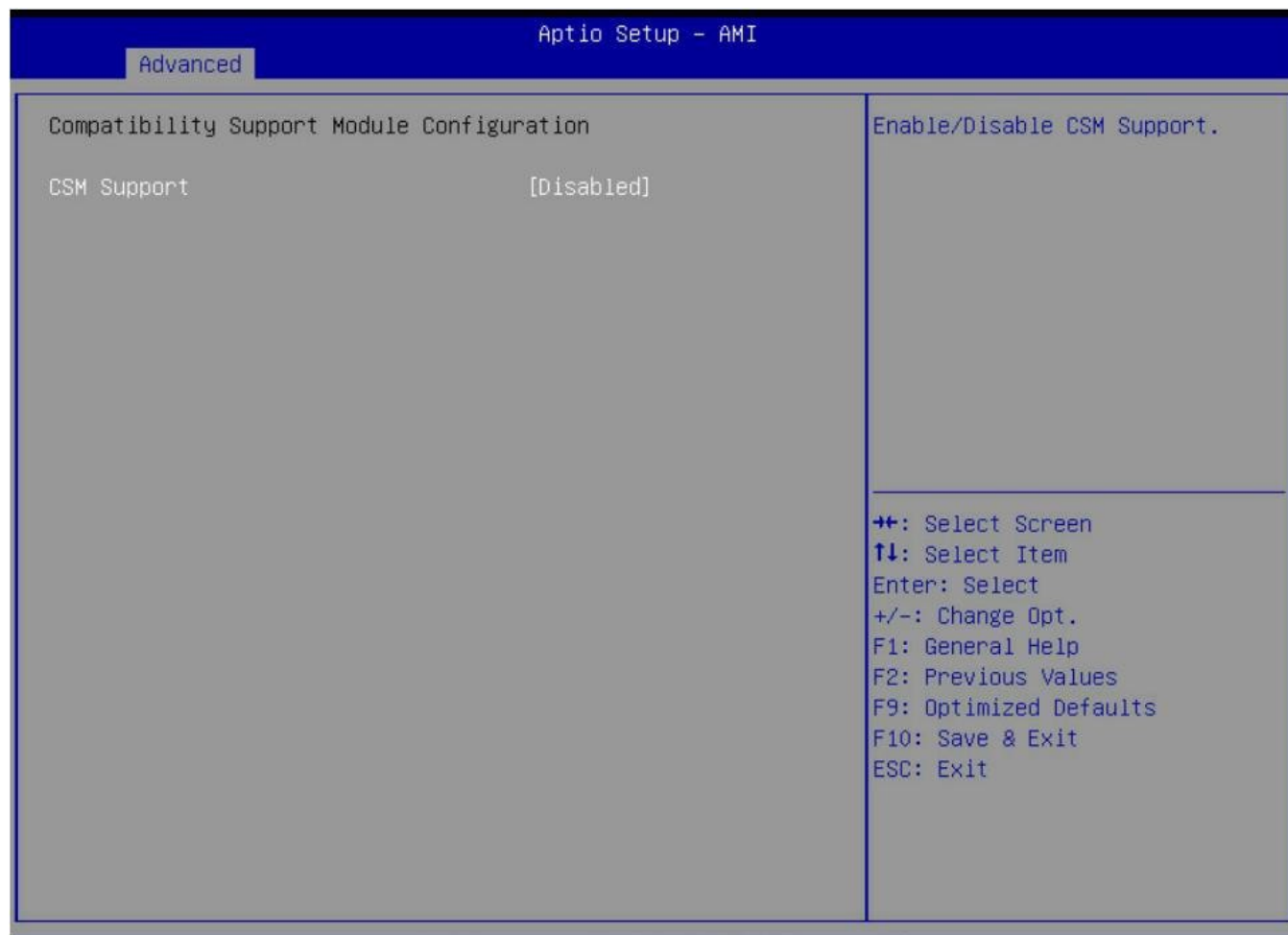


Таблица 0-1 Main

6.2. Advanced

Используйте меню **Advanced** для настройки периферийных устройств через следующие подменю.

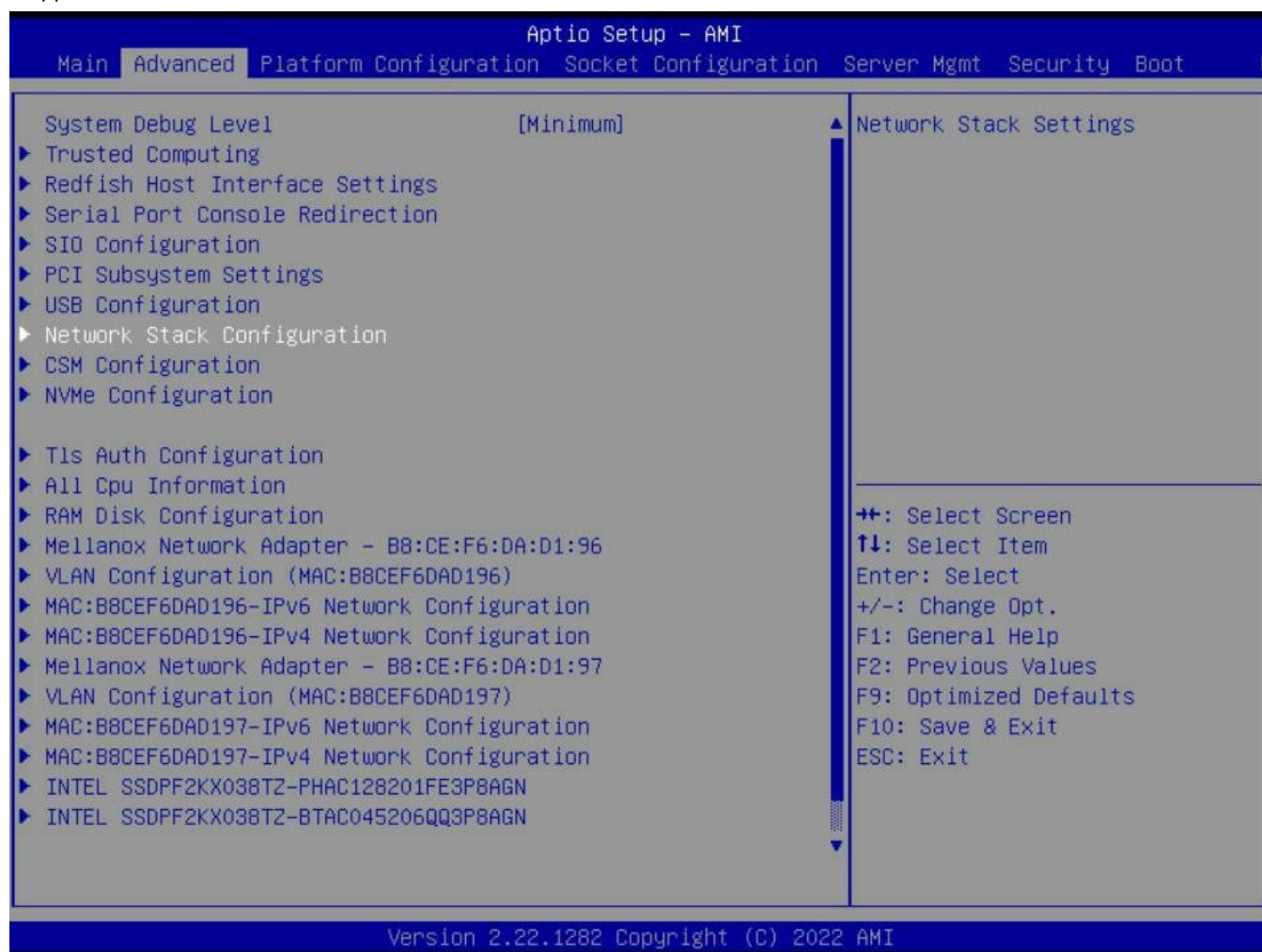
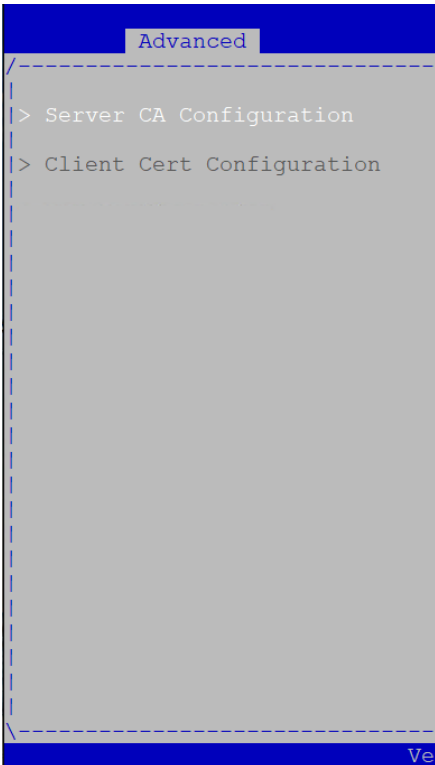


Рисунок 0-2 Advanced

Настройка BIOS	Опции	Описание
System Debug Level	Maximum/Minimum	Установка уровня отладки системы для вывода сообщений в serial порт: Disabled - без сообщений; Minimum - базовые сообщения отладки; Maximum - полные сообщения отладки.
Trusted Computing	См. подробнее.	Настройка Trusted Computing.
Redfish Host Interface Setting	См. подробнее.	Параметры Redfish Host Interface.

Настройка BIOS	Опции	Описание
 The screenshot shows the 'Advanced' BIOS menu. It contains two main options: '> Server CA Configuration' and '> Client Cert Configuration'. The 'Client Cert Configuration' option is highlighted. The bottom of the screen shows the 'Ve' logo.	См. подробнее.	Перенаправление консоли последовательного порта.

Настройка BIOS	Опции	Описание
		
Serial Port Console Redirection		
SIO Configuration	См. подробнее.	Конфигурация SIO.
PCI Subsystem Settings	См. подробнее.	Настройки PCI, PCI-X и PCI Express.
USB Configuration	См. подробнее.	Параметры конфигурации USB.
Network Stack Configuration	См. подробнее.	Настройки сетевого стека.
CSM Configuration	См. подробнее.	Конфигурация CSM: Включить/Выключить, настройки выполнения Option ROM и т.д.
NVMe Configuration	См. подробнее.	Настройки параметров устройств NVMe.
Tls Auth Configuration	См. подробнее.	Нажмите для выбора конфигурации Tls Auth.
All CPU Information	См. подробнее.	Отображение всей информации о процессоре.
RAM Disk Configuration	См. подробнее.	Нажмите для

Настройка BIOS	Опции	Описание
		добавления/удаления RAM дисков.

Таблица 0-2 Advanced

6.2.1. Trust Computing

Aptio Setup - AMI		
Advanced		
Configuration		
Security Device Support	[Enable]	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Disable Block Sid	[Disabled]	
NO Security Device Found		
		→+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.22.1282 Copyright (C) 2022 AMI		



Рисунок 0-2 Trust Computing

Настройка BIOS	Опции	Описание
TPM 2.0 Device FoundFirmware Version: 7.62Vendor: IFX Security Device Support	TPM 2.0 Device FoundFirmware Version: 7.62Vendor: IFX Enable/Disable	Устройство TPM 2.0 найденoВерсия прошивки: 7.62Производитель: IFX Включение/отключение устройства безопасности. ПРИМЕЧАНИЕ : Ваш компьютер перезагрузится во время рестарта, чтобы изменить состояние устройства.
Active PCR banks	Read only	Показать текущий используемый алгоритм хеширования банков PCR.
Available PCR banks	Read only	Показать поддерживаемый алгоритм хеширования банков PCR.
SHA-1 PCR Bank	Enabled/Disabled	Включить или отключить SHA-1 PCR Bank.
SHA256 PCR Bank	Enabled/Disabled	Включить или отключить SHA256 PCR Bank.
Pending operation	None/TPM Clear	Запланировать операцию для

		устройства безопасности.ПРИМЕЧАНИЕ: Ваш компьютер перезагрузится во время рестарта, чтобы изменить состояние устройства безопасности.
Platform Hierarchy	None/TPM Clear	Запланировать операцию для устройства безопасности. ПРИМЕЧАНИЕ : Ваш компьютер перезагрузится во время рестарта, чтобы изменить состояние устройства безопасности.
Storage Hierarchy	Enabled/Disabled	Включить или отключить иерархию платформы.
Endorsement Hierarchy	Enabled/Disabled	Включить или отключить иерархию хранилища.
TPM2.0 UEFI Spec Version	TCG_1_2/TCT_2	Выберите поддерживаемую версию спецификации TCG2.TCG_1_2: режим совместимости для Win8/Win10.TCG_2: Поддержка нового протокола TCG2 и формата событий для Win10 или более поздних версий.
Physical Present Spec Version	1.2/1.3	Выберите, чтобы сообщить ОС о поддержке версии спецификации PPI 1.2 или 1.3.
TPM 20 Interface Type	Read only	Показать интерфейс связи для устройства TPM 2.0.
Device Select	Auto/TPM 1.2/TPM 2.0	TPM 1.2 ограничит поддержку только устройствами TPM 1.2, TPM 2.0 ограничит поддержку устройствами TPM 2.0, Auto будет поддерживать оба варианта с настройкой по умолчанию на устройства TPM 2.0, если не найдены устройства TPM 1.2.



Таблица 0-3 Trust Computing

6.2.2. Redfish Host Interface Setting

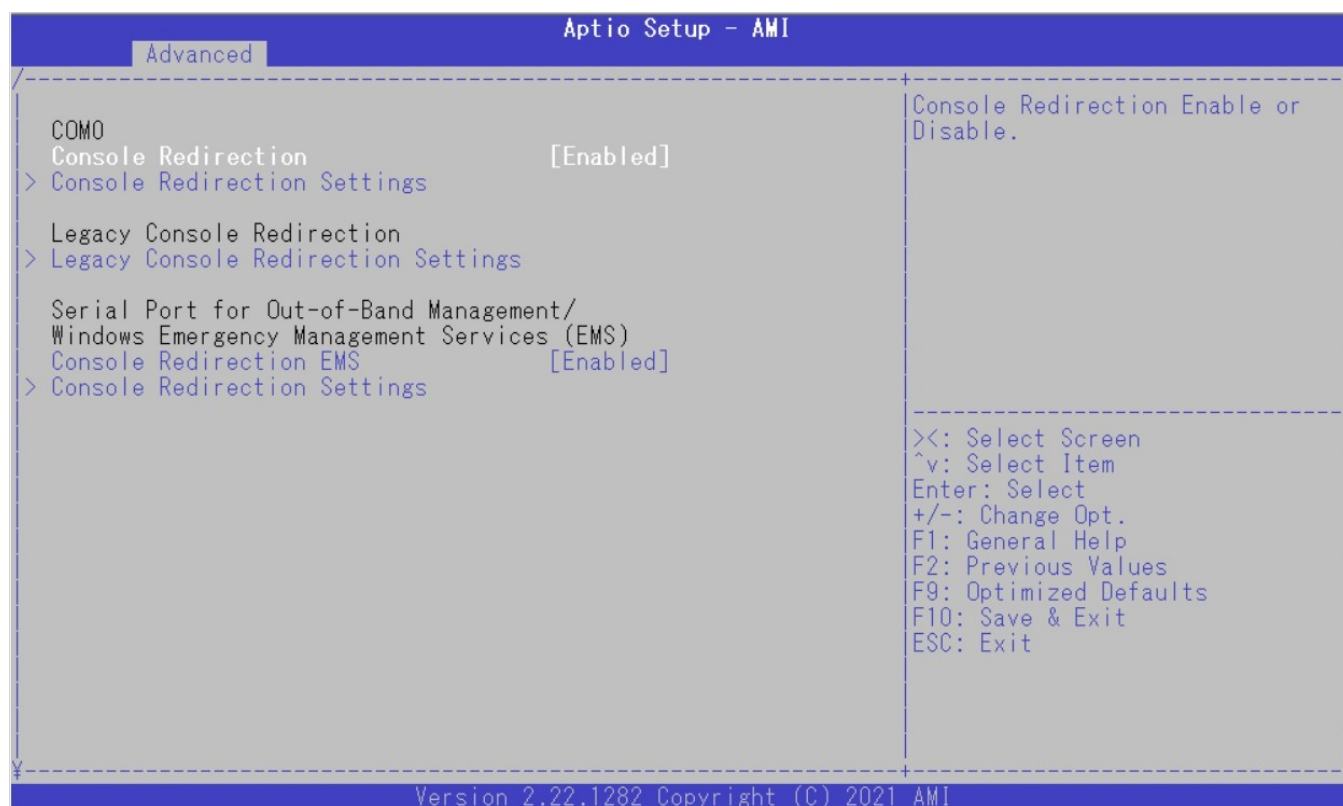
Aptio Setup - AMI	
Advanced	
Redfish Host Interface Settings	
Redfish	[Enabled]
BMC Redfish Version	1.8.0
BIOS Redfish Version	1.8.0
Authentication mode	[Basic Authentication]
Redfish BMC Settings	
IP address	169.254.0.17
IP Mask address	255.255.0.0
IP Port	443
Enable/Disable AMI Redfish ><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.22.1282 Copyright (C) 2021 AMI	
Aptio Setup - AMI	
Platform Configuration	
> PCI Express Root Port 1 > PCI Express Root Port 3 > PCI Express Root Port 5	
PCI Express Root Port 1 Settings ><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.22.1282 Copyright (C) 2021 AMI	

Рисунок 0-3 Redfish Host Interface Setting

Настройка BIOS	Опции	Описание
Redfish Host Interface Setting	Redfish Host Interface Setting	Настройка интерфейса хоста Redfish
Redish	Enabled/Disabled	Включить или отключить AMI Redfish.
BMC Redfish Version	1.8.0	Только для чтения
BIOS Redfish Version	1.8.0	Только для чтения
Authentication mode	Basic Authentication / Session Authentication	Выберите режим аутентификации.
Redfish BMC Setting	Redfish BMC Setting	Настройки Redfish BMC
IP address	169.254.0.17	Введите IP-адрес
IP Mask address	255.255.0.0	Введите маску IP-адреса
IP Port	443	Введите IP порт

Таблица 0-4 Redfish Host Interface Setting

6.2.3. Serial Port Console Redirection



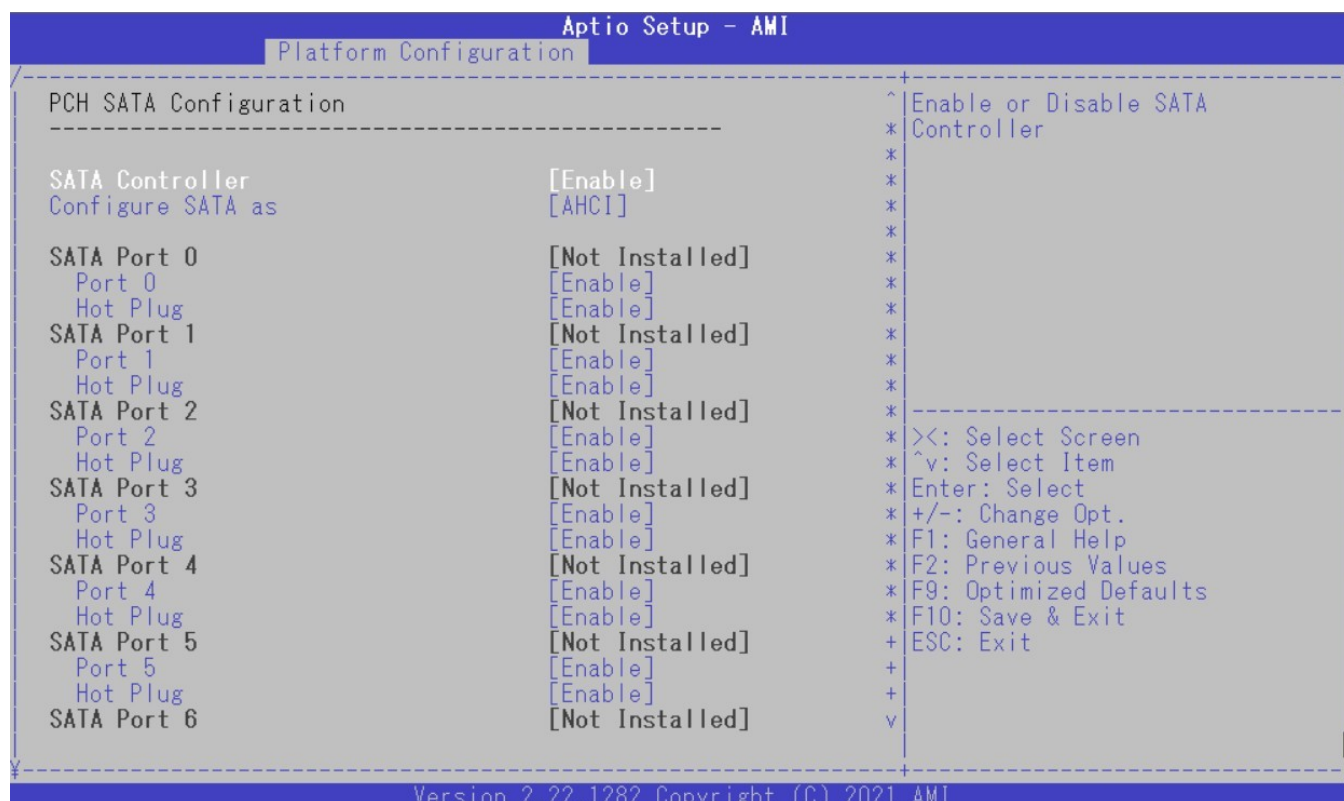


Рисунок 0-4 Serial Port Console Redirection

Настройка BIOS	Опции	Описание
COM0	COM0	COM0
Console Redirection	Enabled/Disabled	Включить или отключить перенаправление консоли.
Console Redirection Settings	См. подробнее.	Настройки определяют, как хост-компьютер и удаленный компьютер (который использует пользователь) будут обмениваться данными. Оба компьютера должны иметь одинаковые или совместимые настройки.
Legacy Console Redirection Settings	См. подробнее.	Настройки определяют, как хост-компьютер и удаленный компьютер (который использует пользователь) будут обмениваться данными. Оба компьютера должны иметь одинаковые или совместимые настройки.
Serial Port for Out-of-Band Management/Windows Emergency Management	Serial Port for Out-of-Band Management/Windows Emergency Management	Последовательный порт для Out-of-Band Management / Windows Emergency

Настройка BIOS	Опции	Описание
Services (EMS)	Services (EMS)	Management Services (EMS)
Console Redirection	Enabled/Disabled	Включить или отключить перенаправление консоли.
Console Redirection Settings	См. подробнее.	Настройки определяют, как хост-компьютер и удаленный компьютер (который использует пользователь) будут обмениваться данными. Оба компьютера должны иметь одинаковые или совместимые настройки.

Таблица 0-5 Serial Port Console Redirection

6.2.3.1. Console Redirection Settings





Рисунок 0-5 Console Redirection Settings

Настройка BIOS	Опции	Описание
COM0	COM0	COM0
Console Redirection Settings	Console Redirection Settings	Настройки перенаправления консоли
Terminal Type	VT100/VT100+/VT-UTF8/ ANSI	VT-UTF8 — предпочтительный тип терминала для out-of-band управления. Следующий лучший выбор — VT100+, затем VT100. См. выше, в разделе настройки перенаправления консоли, для получения дополнительной помощи по типам терминалов/эмуляции.
Bit per second	9600/19200/38400/57600/115200	Выбирает скорость передачи последовательного порта. Скорость должна совпадать на другой стороне. Длинные или зашумленные линии могут требовать более низких скоростей.
Data Bits	7 / 8	Биты данных
Parity	None / Even / Odd/ Mark / Space	Бит четности может быть отправлен с битами данных

Настройка BIOS	Опции	Описание
		для обнаружения некоторых ошибок передачи. Even: бит четности равен 0, если число единиц в битах данных четное. Odd: бит четности равен 0, если число единиц в битах данных нечетное. Mark: бит четности всегда 1. Space: бит четности всегда 0. Mark и Space четность не позволяют обнаруживать ошибки. Они могут использоваться как дополнительный бит данных.
Stop Bits	1 / 2	Стоп-биты указывают конец пакета последовательных данных. (Старт-бит указывает начало). Стандартная настройка - 1 стоп-бит. Связь с медленными устройствами может требовать более 1 стоп-бита.
Flow Control	None / Hardware RTS/CTS	Управление потоком может предотвратить потерю данных из-за переполнения буфера. При отправке данных, если приемные буферы заполнены, может быть отправлен сигнал 'stop' для остановки потока данных. Как только буферы станут пустыми, может быть отправлен сигнал 'start' для возобновления потока. Аппаратное управление потоком использует два провода для отправки сигналов старт/стоп.
VT-UTF8 Combo Key Support	Enabled / Disabled	Включить поддержку комбинированных клавиш VT-UTF8 для терминалов ANSI/VT100.
Recorder Mode	Disabled / Enabled	При включении этого режима будет отправляться только текст. Это для захвата данных терминала.
Resolution 100x31	Enabled / Disabled	Включает или отключает

Flow Control	None / Hardware RTS/CTS	Управление потоком может предотвратить потерю данных из-за переполнения буфера. При отправке данных, если приемные буферы заполнены, может быть отправлен сигнал 'stop' для остановки потока данных. Как только буферы станут пустыми, может быть отправлен сигнал 'start' для возобновления потока. Аппаратное управление потоком использует два провода для отправки сигналов старт/стоп.
		расширенное разрешение терминала.
Putty Keypad	VT100 / LINUX / XTERMR6 / SCO / ESCN/ VT400	Выберите FunctionKey и KeyPad в Putty.

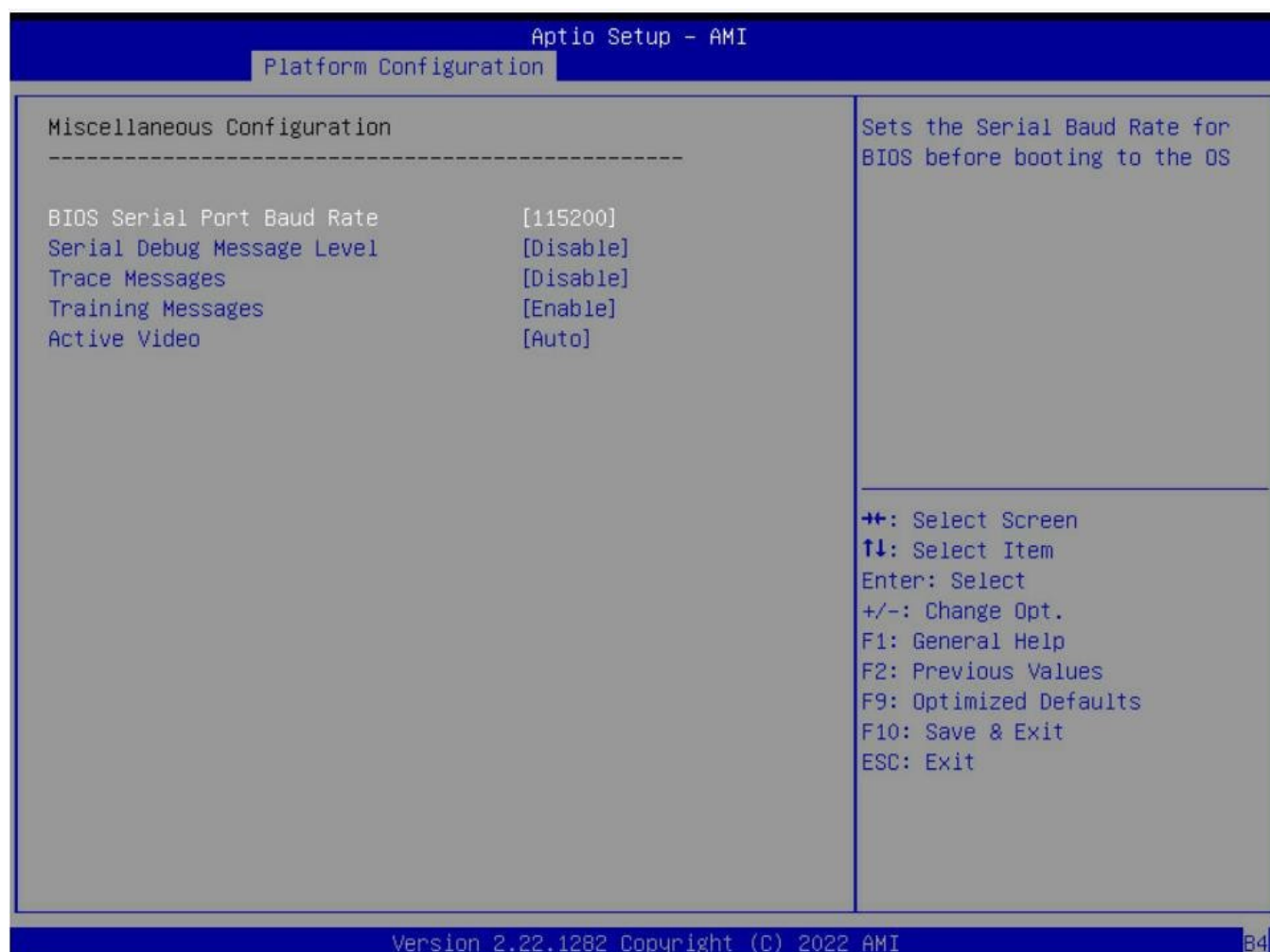


Таблица 0-6 Console Redirection Settings

6.2.3.2. Legacy Console Redirection Settings



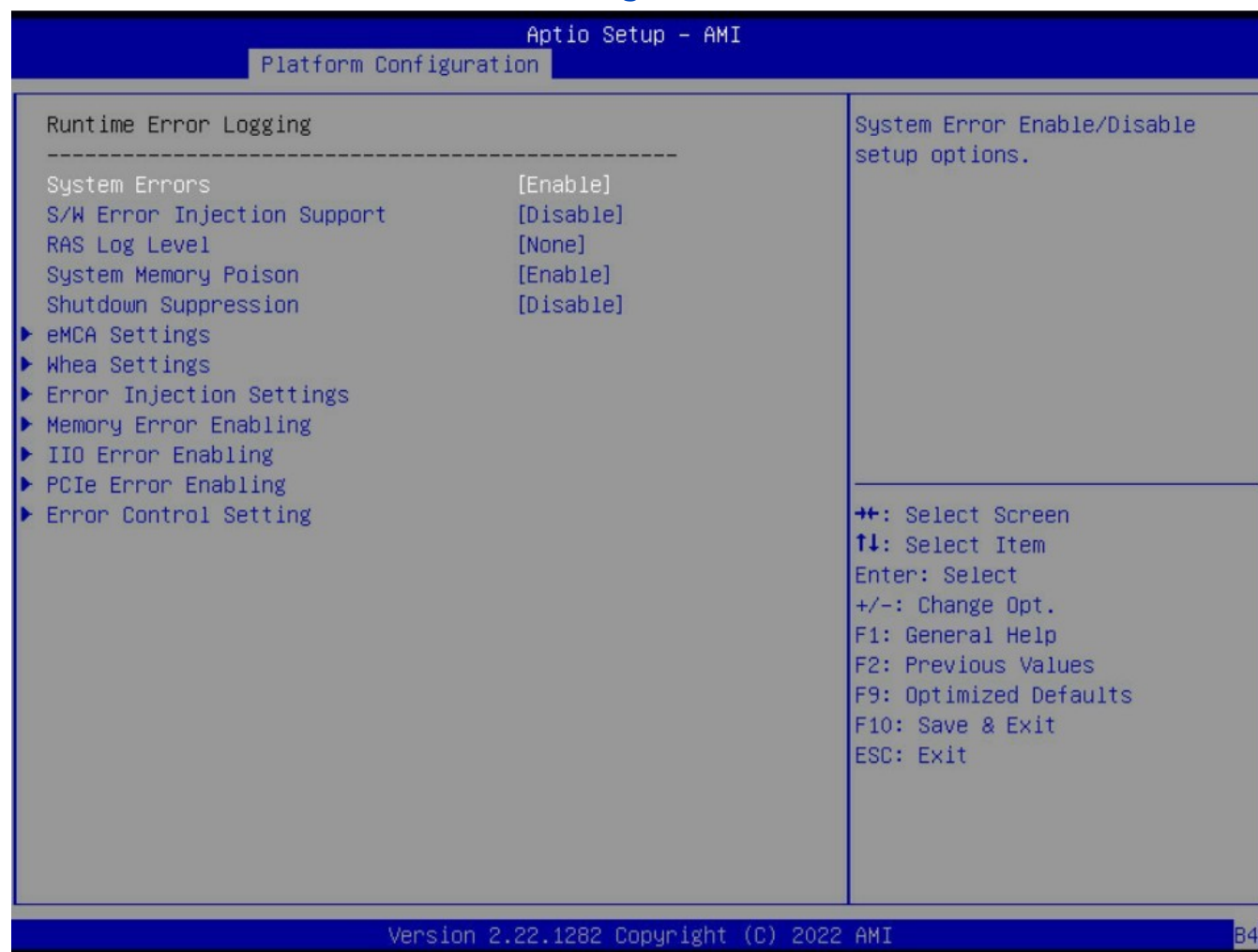
Рисунок 0-6 Legacy Console Redirection Settings

Настройка BIOS	Опции	Описание
COM0	COM0	COM0
Legacy Console Redirections	Legacy Console Redirections	Legacy перенаправления консоли
Redirection COM Port	Redirection COM Port: COM0	Выберите COM-порт для отображения перенаправления сообщений Legacy OS и Legacy OPRM
Resolution	Resolution: 80x24 / 80x25	Количество строк и столбцов, поддерживаемых перенаправлением в Legacy OS

Redirect After POST	Always Enable / BootLoader	При выборе Bootloader перенаправление консоли Legacy отключается перед загрузкой Legacy OS. При выборе Always Enable перенаправление консоли Legacy включено для Legacy OS. Настройка по умолчанию для этой опции - Always Enable.
----------------------------	-----------------------------------	--

Таблица 0-7 Legacy Console Redirection Setting

6.2.3.3. Console Redirection Settings



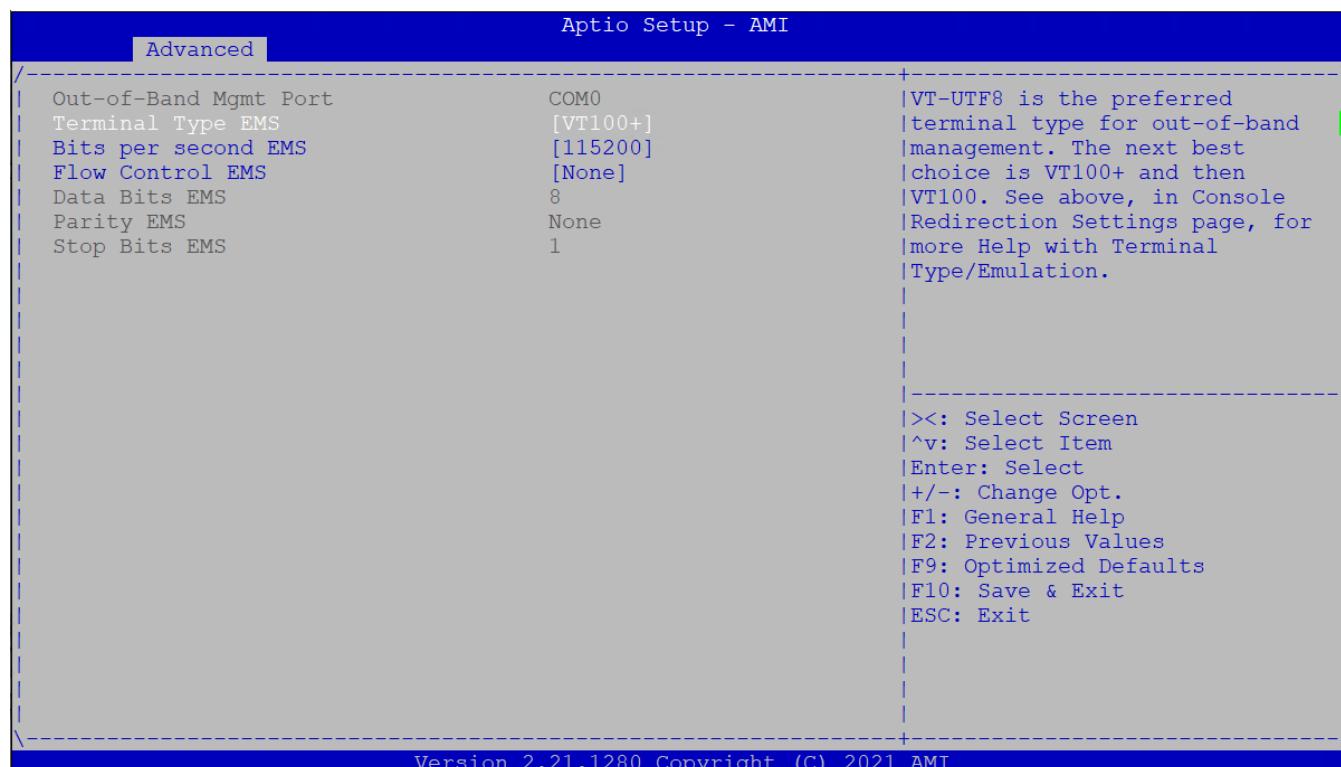


Figure 0-7 EMS Console Redirection Settings

BIOS** ****Setting**	Options	Description
Out-of-Band Mgmt Port	Read Only:COM0	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.
Terminal Type	VT100 / VT100+ / VT-UTF8/ ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bit per second	9600/19200/57600/115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control EMS	NoneHardware RTS/CTS Software Xon/Xoff	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

BIOS** ****Setting**	Options	Description
		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.
Data Bits	Read Only :8	Data Bits
Parity EMS	Read Only :None	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. They can be used as an additional data bit.
Stop Bits EMS	Read Only :1	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.

Aptio Setup - AMI	
Platform Configuration	
Whea Settings	Enable/Disable WHEA support
WHEA Support	[Enable]
Whea Log Memory Error	[Enable]
Whea Log Processor Error	[Enable]
Whea Log PCI Error	[Enable]
><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.21.1280 Copyright (C) 2021 AMI	

Table 0-8 EMS Console Redirection Settings

6.2.4. SIO Configuration

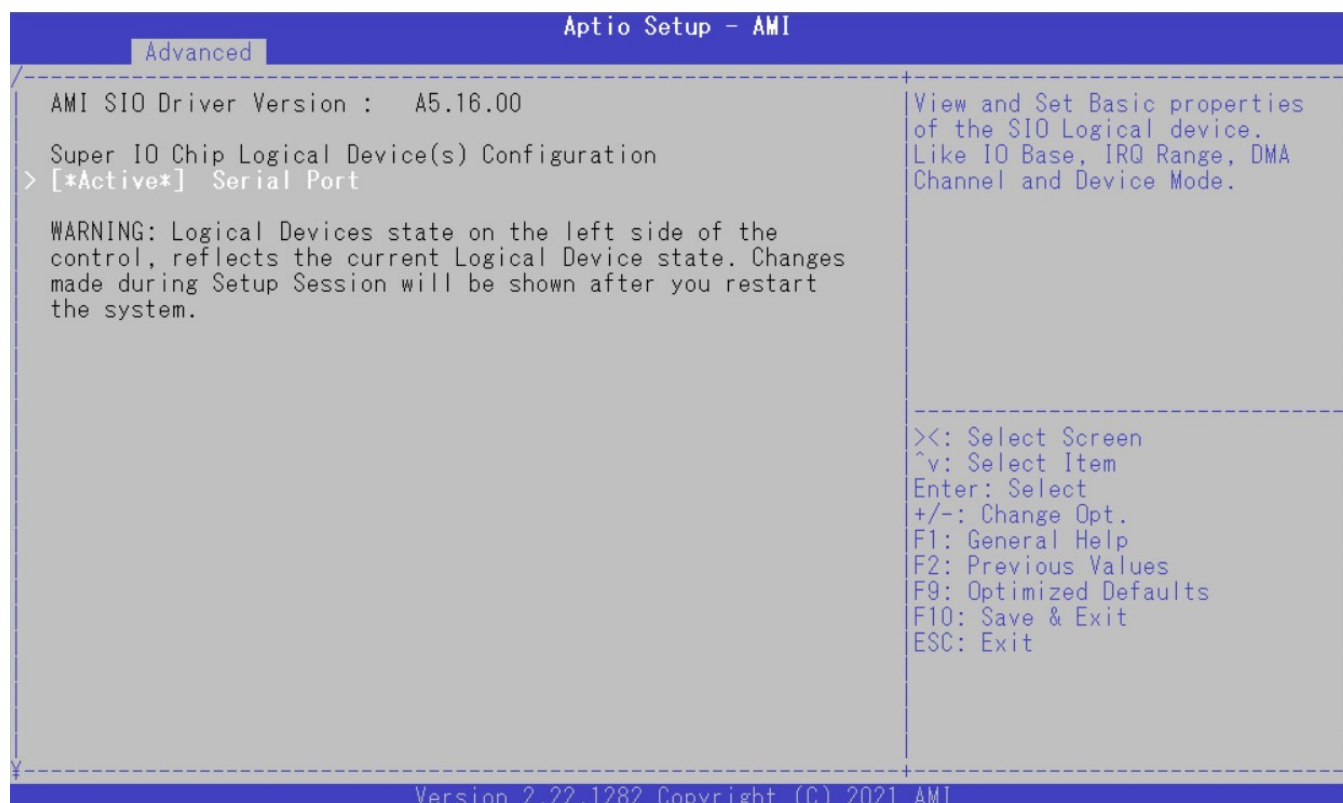


Рисунок 0-8 SIO Configuration

Настройка BIOS	Опции	Описание
AMI SIO Driver Version:	AMI SIO Driver Version:	Версия драйвера AMI SIO:
Super IO Chip Logical Device(s) Configuration:	Super IO Chip Logical Device(s) Configuration:	Конфигурация логических устройств чипа Super IO:
[Active] Serial Port 1	См. подробнее.	Просмотр и настройка основных свойств логического устройства SIO. Таких как IO Base, диапазон IRQ, канал DMA и режим устройства.
WARNING: Logical Devices state on the left side of the control, reflects the current Logical Device state. Changes made during Setup Session will be shown after you restart the system.	WARNING: Logical Devices state on the left side of the control, reflects the current Logical Device state. Changes made during Setup Session will be shown after you restart the system.	ПРЕДУПРЕЖДЕНИЕ: Состояние логических устройств в левой части элемента управления отражает текущее состояние логического устройства. Изменения, сделанные во время сеанса настройки, будут показаны после перезагрузки системы.

Таблица 0-9 SIO Configuration

6.2.4.1. Serial Port 1 Configuration

Advanced		Aptio Setup - AMI	
Serial Port 1 Configuration		Enable or Disable this Logical Device.	
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 effects.			
PROCEED WITH CAUTION.			
		><: Select Screen	
		^v: Select Item	
		Enter: Select	
		+/-: Change Opt.	
		F1: General Help	
		F2: Previous Values	
		F9: Optimized Defaults	
		F10: Save & Exit	
		ESC: Exit	
Version 2.21.1280 Copyright (C) 2021 AMI			

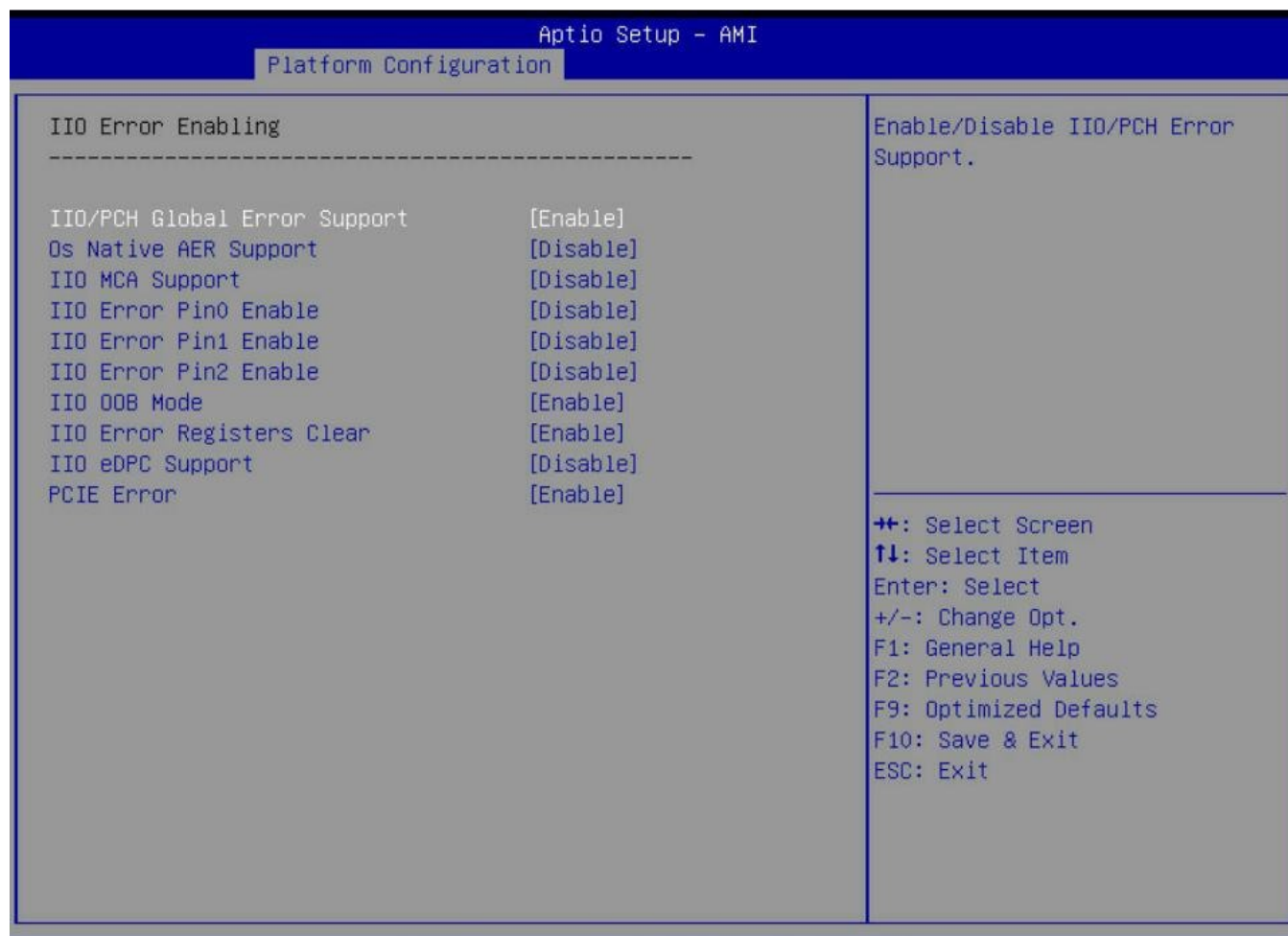


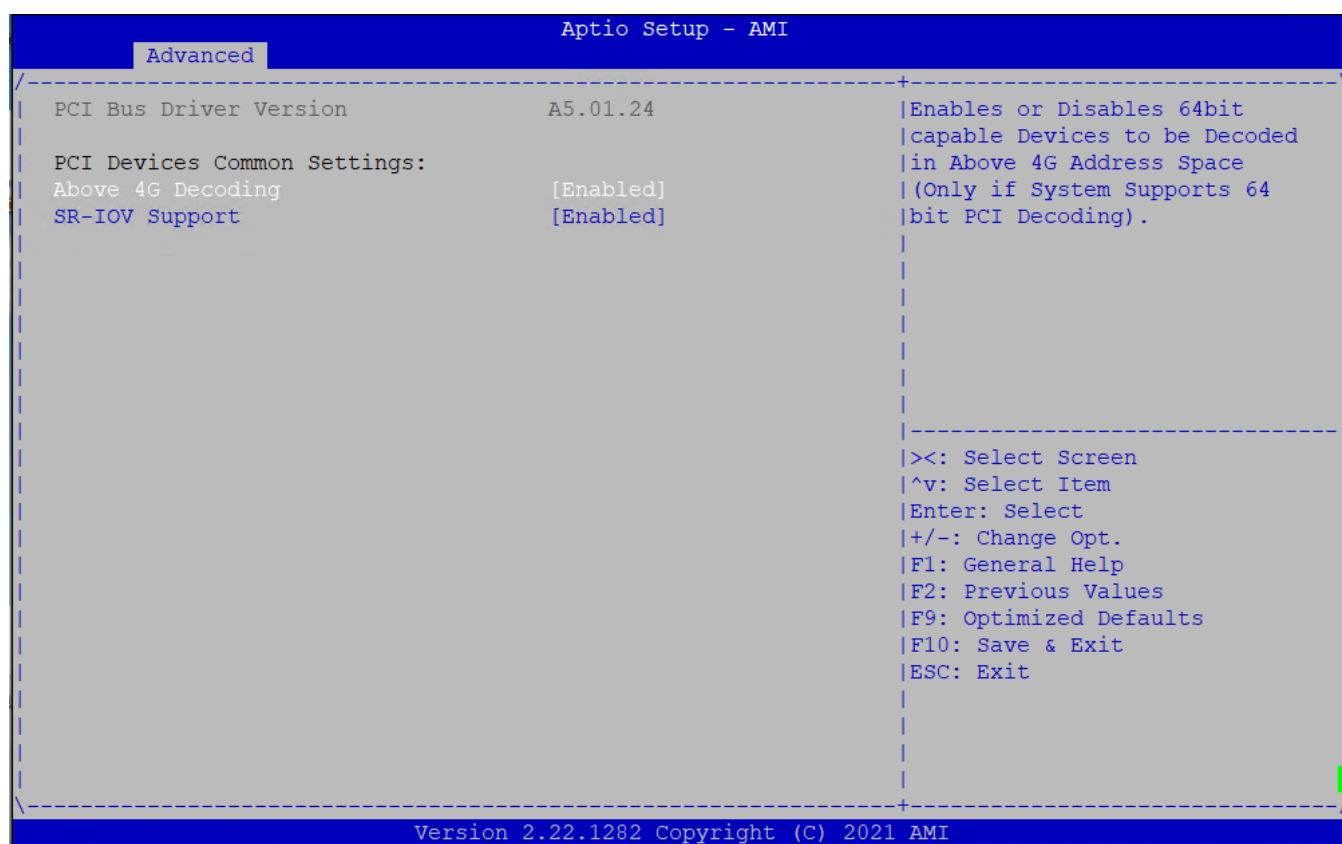
Рисунок 0-9 Serial Port 1 Configuration

Настройка BIOS	Опции	Описание	
Serial Port 1 Configuration	Serial Port 1 Configuration	Конфигурация последовательного порта 1	
Use This Device	Enable / Disable	Включить или отключить это логическое устройство.	
Logical Device Settings:Current: IO=3F8h; IRQ=4;	Logical Device Settings:Current: IO=3F8h; IRQ=4;	Настройки логического устройства:Текущие: IO=3F8h; IRQ=4;	
Possible:	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	Позволяет пользователю изменить настройки ресурсов устройства. Новыенастройки отобразятся на этой странице настройки после перезагрузки	

Настройка BIOS	Опции	Описание	
	2;DMA; IO=2E8h; IRQ=3,4,5,7,9.10,11,1 2; DMA;	системы.	
WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	ПРЕДУПРЕЖДЕНИЕ: Отключение логических устройств SIO может иметь нежелательные побочные эффекты. ДЕЙСТВУЙТЕ С ОСТОРОЖНОСТЬЮ.	

Таблица 0-10 Serial Port 1 Configuration

6.2.5. PCI Subsystem Settings



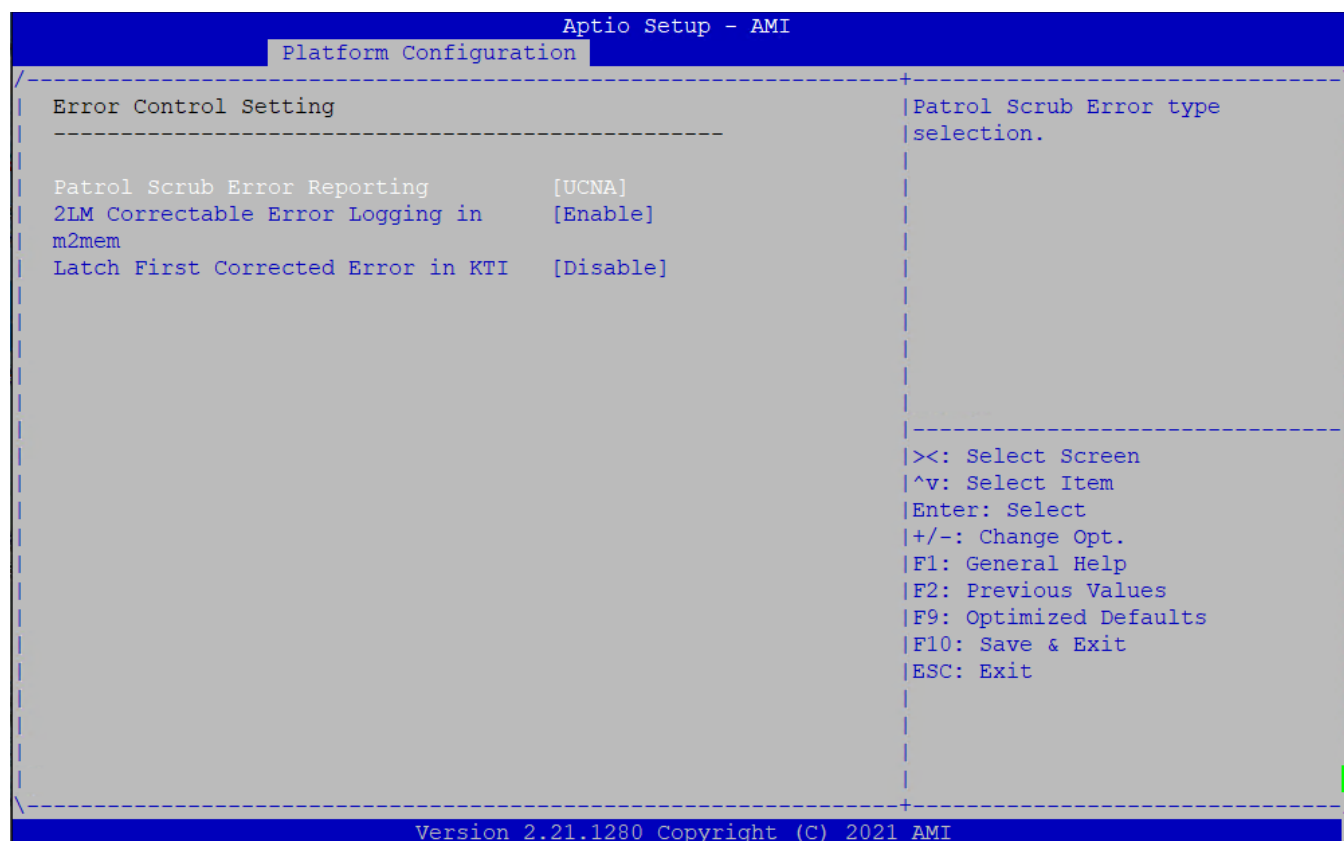


Рисунок 0-10 PCI Subsystem Settings

Настройка BIOS	Опции	Описание
PCI Bus Driver Version	Read Only	Версия драйвера шины PCI A5.01.24
PCI Devices Common Settings:	PCI Devices Common Settings:	Общие настройки устройств PCI:
Above 4G Decoding	Enabled / Disabled	Включает или отключает декодирование устройств с поддержкой 64 бит в адресном пространстве выше 4G (только если система поддерживает 64-битное декодирование PCI).
SR-IOV Support	Enabled / Disabled	Если система имеет PCIe устройства с поддержкой SR-IOV, эта опция включает или отключает поддержку Single Root IO Virtualization.

Таблица 0-11 PCI Subsystem Settings

6.2.6. USB Configuration

Aptio Setup - AMI		
Advanced		
USB Configuration		Enables 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.
USB Module Version	26	
USB Controllers:		
1 XHCI		
USB Devices:		
1 Keyboard, 1 Mouse, 1 Hub		
Legacy USB Support	[Enabled]	
XHCI Hand-off	[Enabled]	
USB Mass Storage Driver Support	[Enabled]	
Port 60/64 Emulation	[Enabled]	
USB hardware delays and time-outs:		
USB transfer time-out	[20 sec]	
Device reset time-out	[20 sec]	
Device power-up delay	[Auto]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1280 Copyright (C) 2021 AMI		

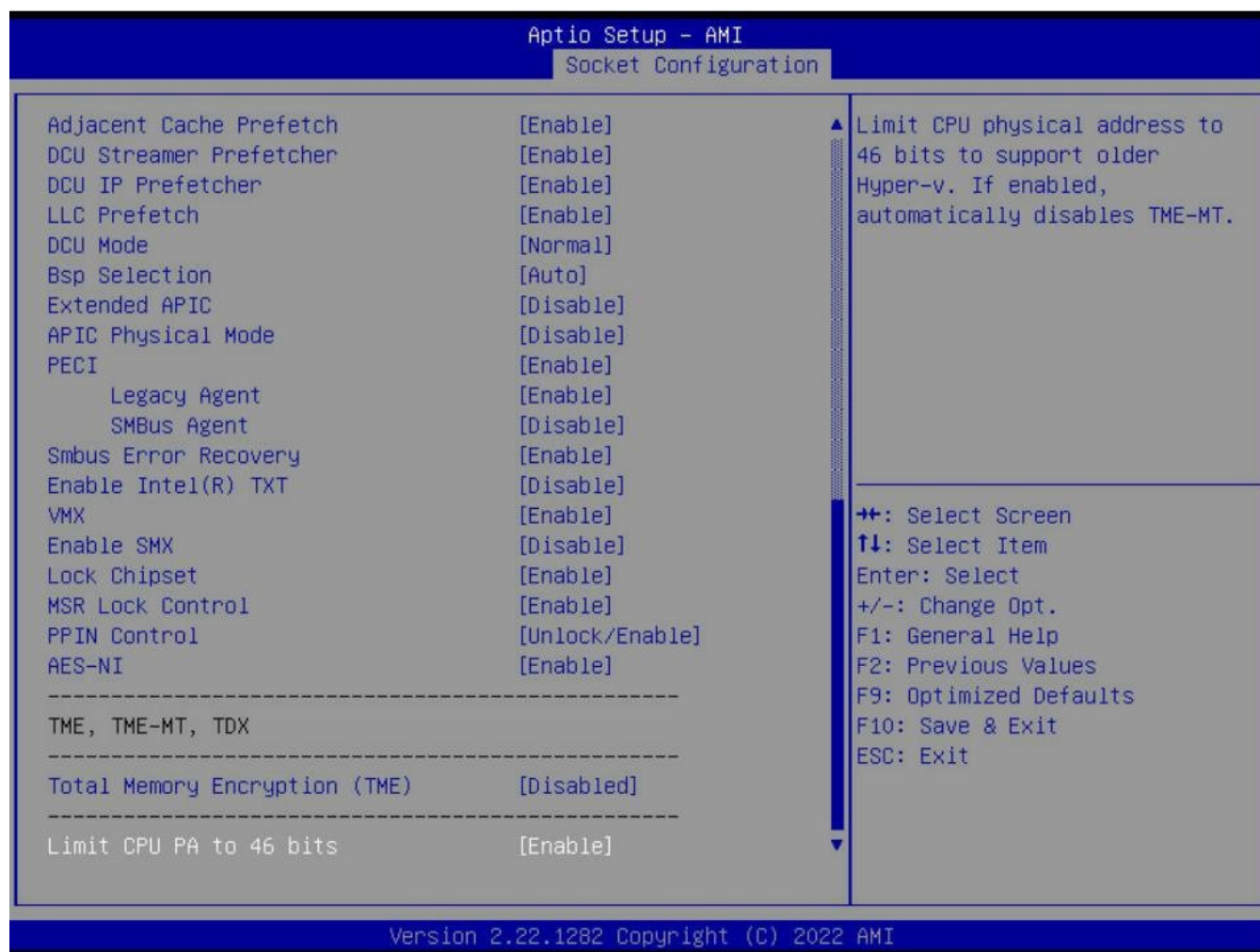


Рисунок 0-11 USB Configuration

Настройка BIOS	Опции	Описание
USB Configuration	USB Configuration	Конфигурация USB
USB Module Version	Read Only	Версия модуля USB 26
USB Controllers:	USB Controllers:	USB контроллеры:
Read Only	Read Only	Только для чтения
USB Devices:	USB Devices:	USB устройства:
Read Only	Read Only	Только для чтения
Legacy USB Support	Enabled / Disabled / Auto	Включает поддержку Legacy USB. Опция AUTO отключает поддержку legacy, если USB устройства не подключены. Опция DISABLE оставит USB устройства доступными только для приложений EFI.
XHCI Hand-off	Enabled / Disabled	Это обходное решение для ОС без поддержки XHCI hand-off. Смена владельца

Настройка BIOS	Опции	Описание
		ХHCI должна выполняться драйвером ХHCI.
USB Mass Storage Driver Support	Enabled / Disabled	Включить/отключить поддержку драйвера USB Mass Storage.
Port 60/64 Emulation	Enabled / Disabled	Включает поддержку эмуляции портов ввода-вывода 60h/64h. Это должно быть включено для полной поддержки legacy USB клавиатур для ОС, не поддерживающих USB.
USB hardware delays and time-outs:	USB hardware delays and time-outs:	Аппаратные задержки и таймауты USB:
USB transfer time-out	1 sec5 sec	Значение таймаута для Control, Bulk и Interrupt передач.
	10 sec20 sec	
Device reset time-out	10 sec20 sec30 sec40 sec	Таймаут команды Start Unit для USB накопителей.
Device power-up delay	Auto Manual	Максимальное время, которое устройство будетзанимать до того, как оно правильно сообщит о себе хост-контроллеру. 'Auto' использует значение по умолчанию: для корневого портаэто 100 мс, для порта концентратора задержка берется из дескриптора концентратора.

Aptio Setup - AMI			Socket Configuration
▶ Per-Socket Configuration			▲ = MLC Spatial Prefetcher (MSR 1A4h Bit[1])
Processor BSP Revision	606A6 - ICX D1		
Processor Socket	Socket 0	Socket 1	
Processor ID	000606A6*	000606A6	
Processor Core	36	36	
Processor Frequency	2.400GHz	2.400GHz	
Processor Max Ratio	18H	18H	
Processor Min Ratio	08H	08H	
Microcode Revision	0D000331	0D000331	
L1 Cache RAM(Per Core)	80KB	80KB	
L2 Cache RAM(Per Core)	1280KB	1280KB	
L3 Cache RAM(Per Package)	55296KB	55296KB	
Processor 0 Version	Intel(R) Xeon(R) Platin um 8360Y CPU @ 2.40GHz		
Processor 1 Version	Intel(R) Xeon(R) Platin um 8360Y CPU @ 2.40GHz		
Hyper-Threading [ALL]	[Enable]		↔: Select Screen
Skip Flex Ratio Override	[Disabled]		↑↓: Select Item
Check CPU BIST Result	[Enabled]		Enter: Select
Core Failover	[Enabled]		+/-: Change Opt.
Machine Check	[Enable]		F1: General Help
Max CPUID Value Limit	[Disable]		F2: Previous Values
Hardware Prefetcher	[Enable]		F9: Optimized Defaults
Adjacent Cache Prefetch	[Enable]		F10: Save & Exit
			ESC: Exit
Version 2.22.1282 Copyright (C) 2022 AMI			

Таблица 0-12 USB Configuration

6.2.7. Network Stack Configuration

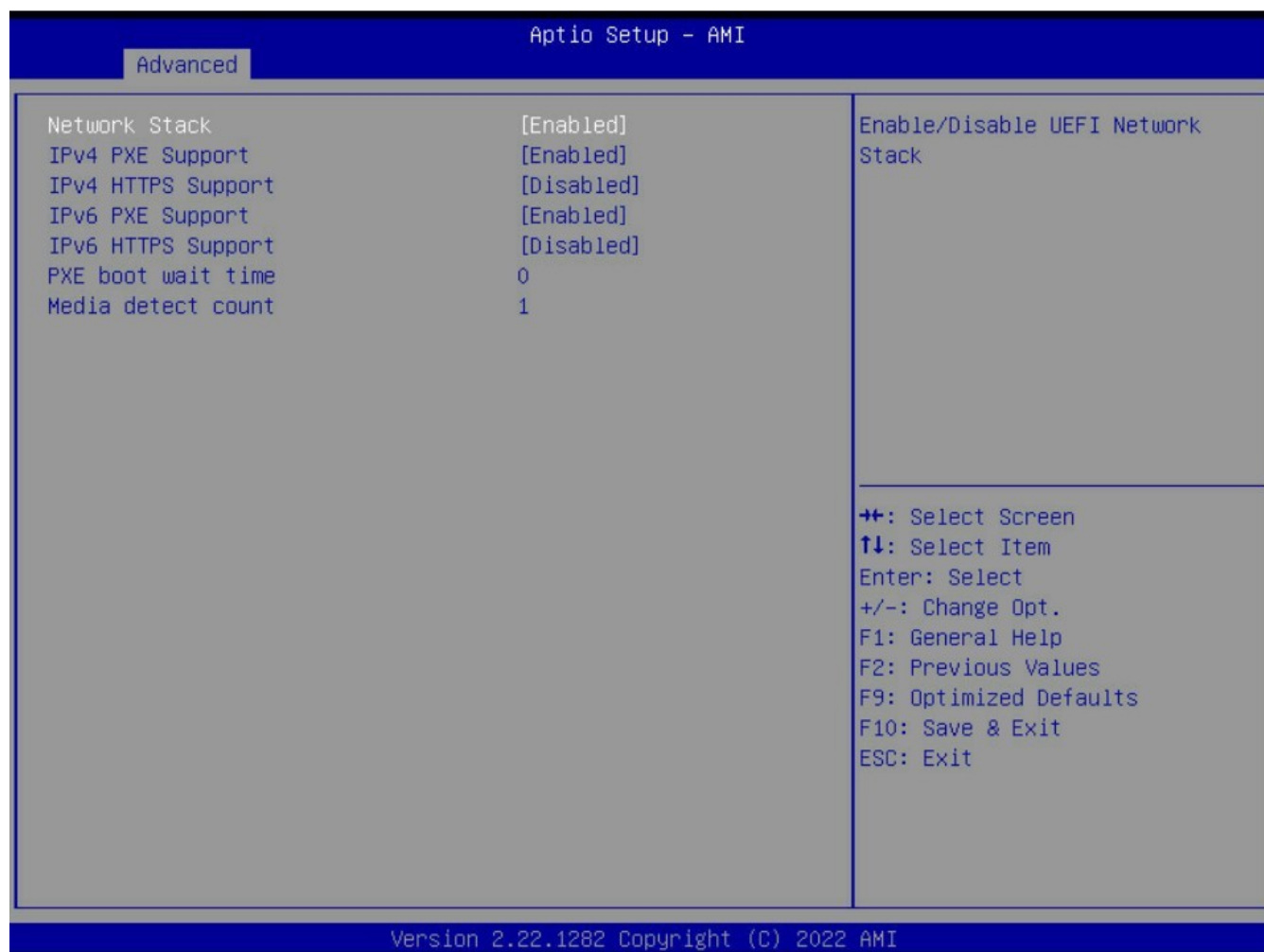


Рисунок 0-12 Network Stack Configuration

Настройка BIOS	Опции	Описание
Network Stack	Enabled/Disabled	Включить/выключить UEFI Network Stack
Ipv4 PXE Support	Enabled/Disabled	Включить поддержку Ipv4 PXE Boot. Если отключено, опция загрузки Ipv4 PXE не будет создана.
Ipv4 HTTP Support	Enabled/Disabled	Включить поддержку Ipv4 HTTP Boot. Если отключено, опция загрузки Ipv4 HTTP не будет создана.
Ipv6 PXE Support	Enabled/Disabled	Включить поддержку Ipv6 PXE Boot. Если отключено, опция загрузки Ipv6 PXE не будет создана.

		создана.
Ipv6 HTTP Support	Enabled/Disabled	Включить поддержку Ipv6 HTTP Boot. Если отключено, опция загрузки Ipv6 HTTP не будет создана.
PXE boot wait time	Default: 0	Время ожидания в секундах для нажатия клавиши ESC для прерывания загрузки PXE. Используйте клавиши +/- или цифровые клавиши для установки значения.
Media detect count	Default: 1	

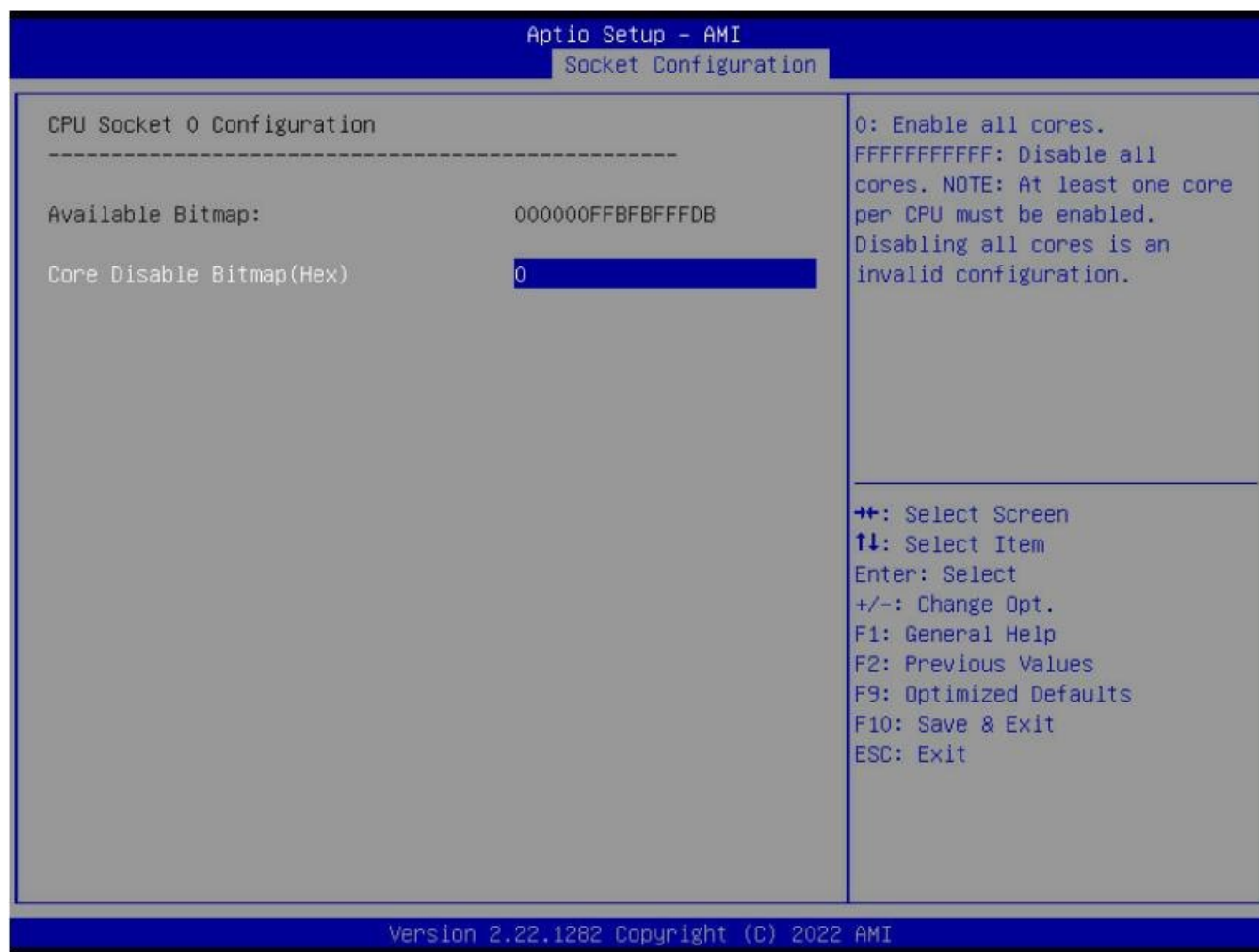


Таблица 0-13 Network Stack Configuration

CSM Configuration

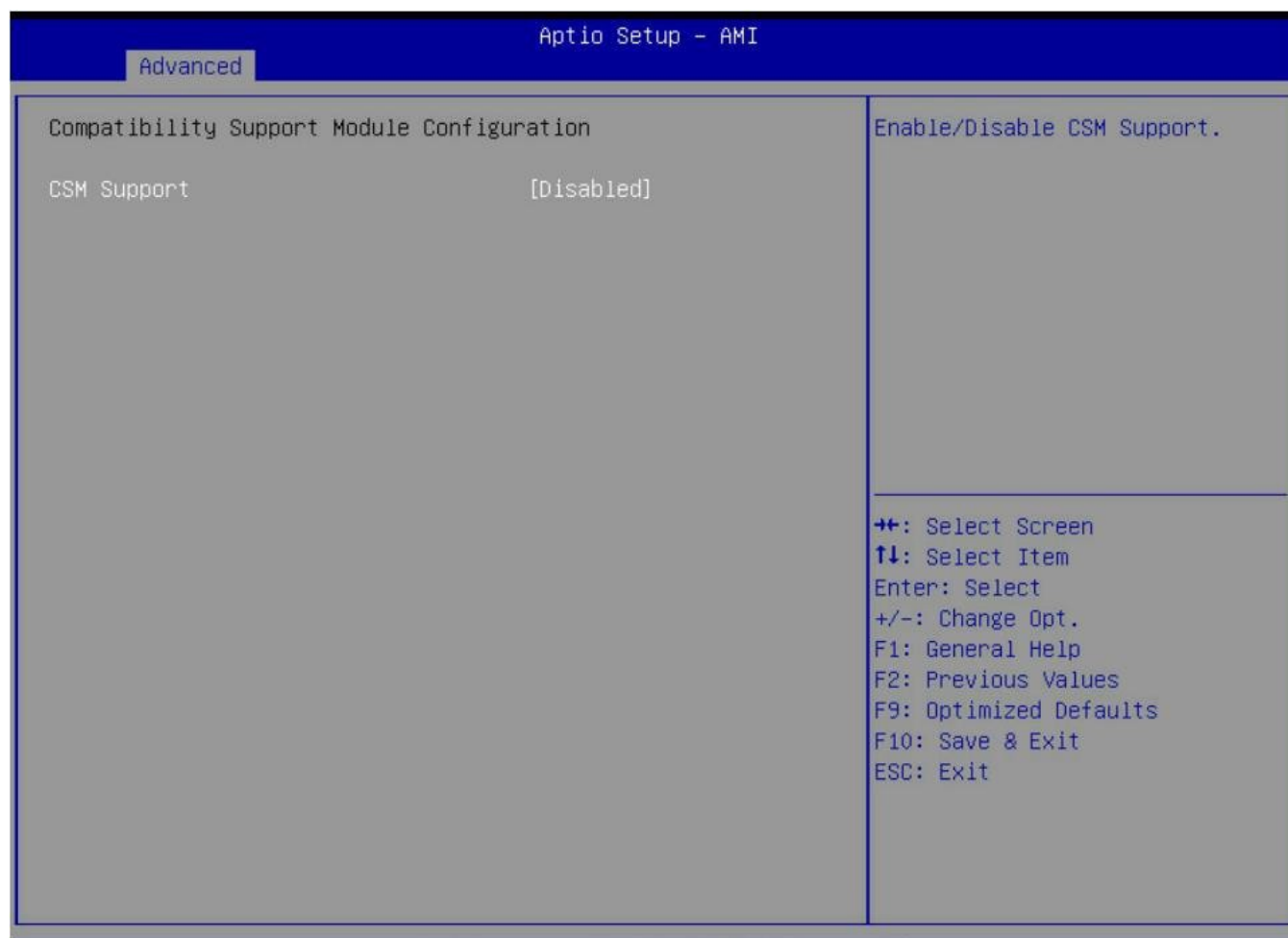


Рисунок 0-13 CSM Configuration

Настройка BIOS	Опции	Описание
Compatibility Support Module Configuration	Compatibility Support Module Configuration	Конфигурация модуля поддержки совместимости (CSM)
CSM Support	Enabled / Disabled	Включить/выключить поддержку CSM.
GateA20 Active	Upon Request/ Always	UPON REQUEST - GA20 может быть отключен с помощью сервисов BIOS. ALWAYS - не разрешать отключение GA20; эта опция полезна, когда любой код RT выполняется выше 1MB.

INT19 Trap Response	Immediate / Postponed	Реакция BIOS на перехват INT19 через Option ROM: IMMEDIATE - выполнять перехват немедленно, POSTPONED - выполнять перехват во время legacy загрузки.
Boot option filter	Legacy only / UEFI only	Установить, какой тип опций загрузки будет включен.
Option ROM execution	Option ROM execution	Выполнение Option ROM
Network	Legacy / UEFI	Управляет выполнением UEFI и Legacy PXE OpROM
Storage	Legacy / UEFI	Управляет выполнением UEFI и Legacy Storage OpROM
Video	Legacy / UEFI	Управляет выполнением UEFI и Legacy Video OpROM
Other PCI devices	Legacy / UEFI	Определяет политику выполнения OpROM для устройств, отличных от Network, Storage или Video.

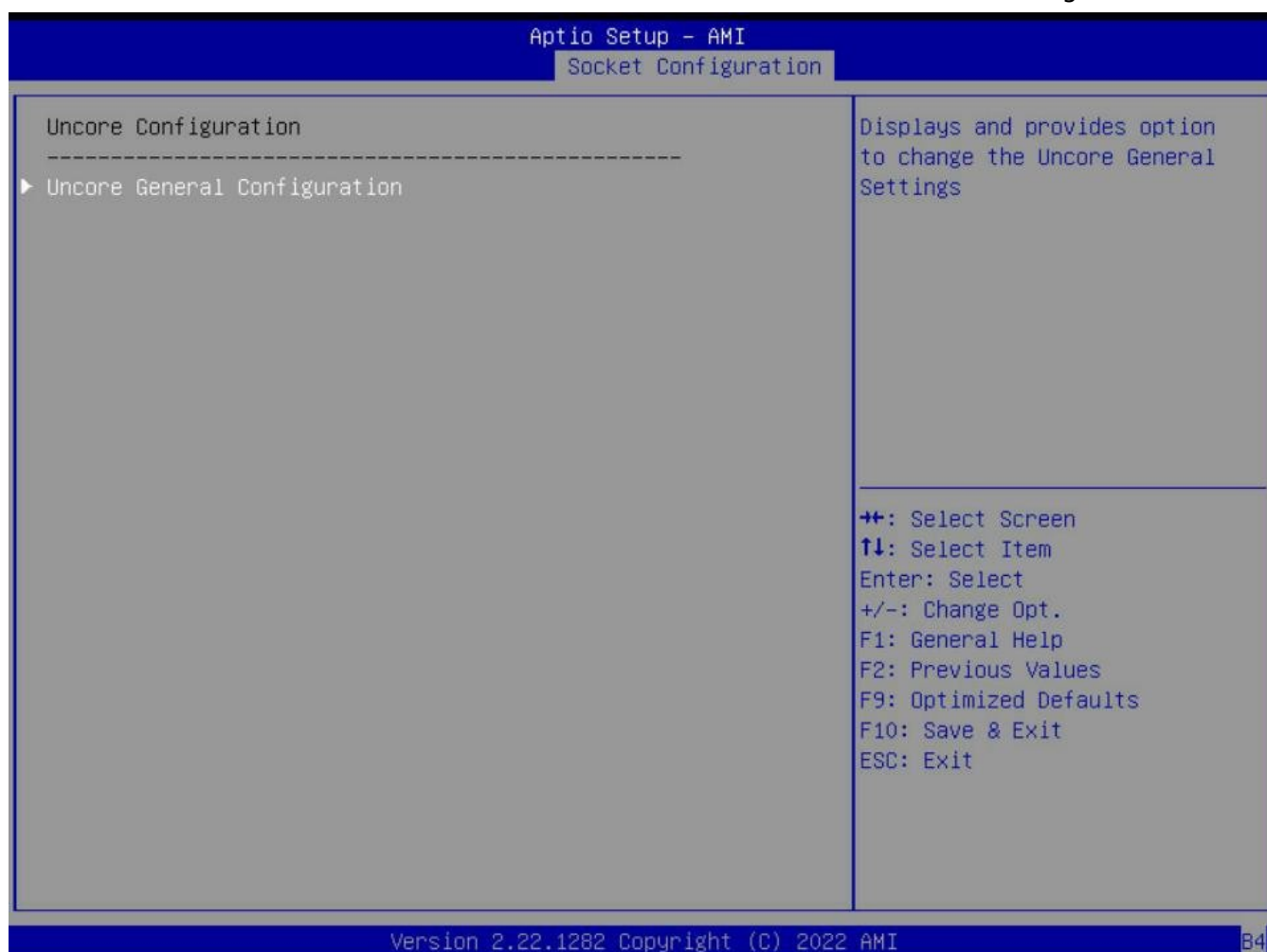


Таблица 0-14 CSM Configuration

6.2.8. NVMe Configuration

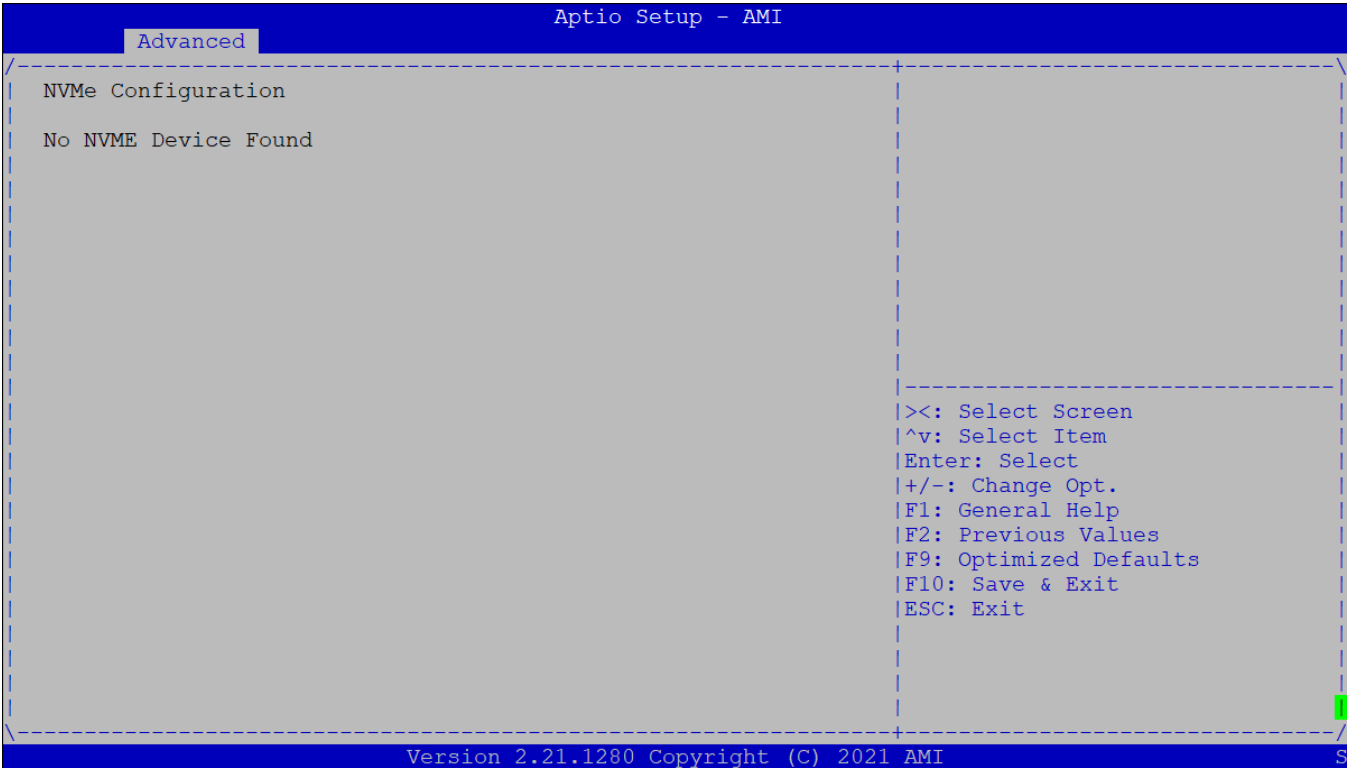
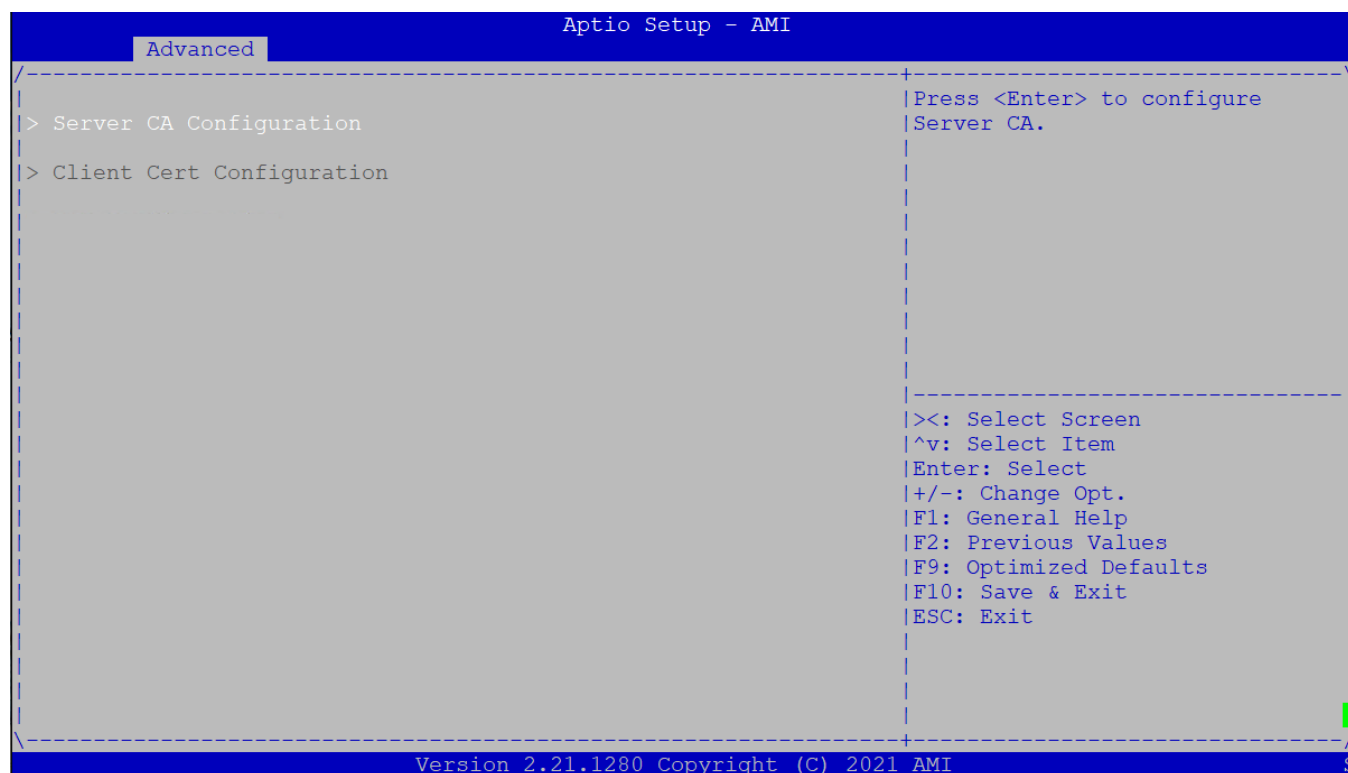


Рисунок 0-14 NVMe Configuration

Настройка BIOS	Опции	Описание
NVMe controller and Drive information	NVMe controller and Drive information	Информация о контроллере и дисках NVMe
Read Only	Read Only	Только для чтения

Таблица 0-15 NVMe Configuration

6.2.9. Tls Auth Configuration



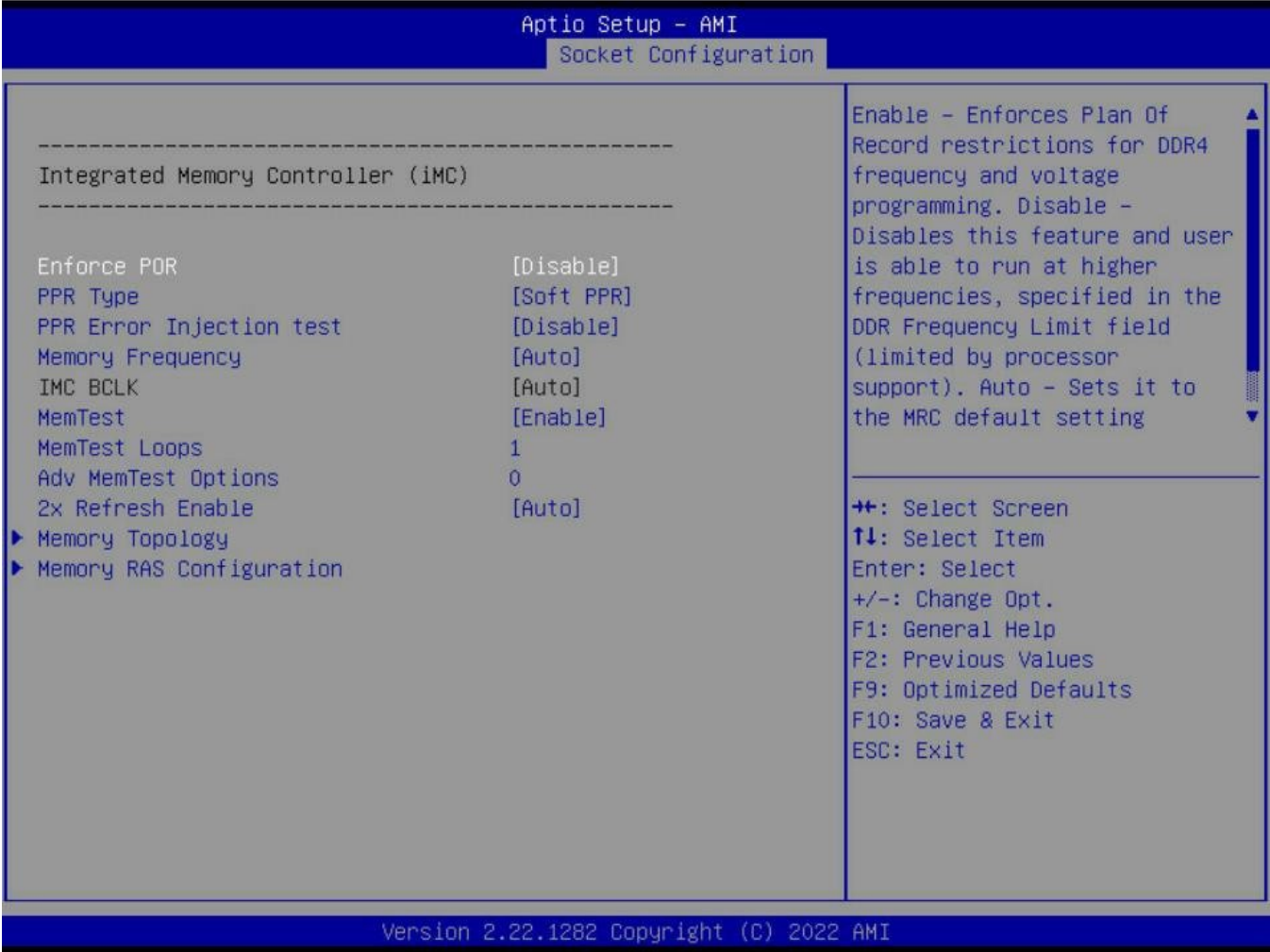
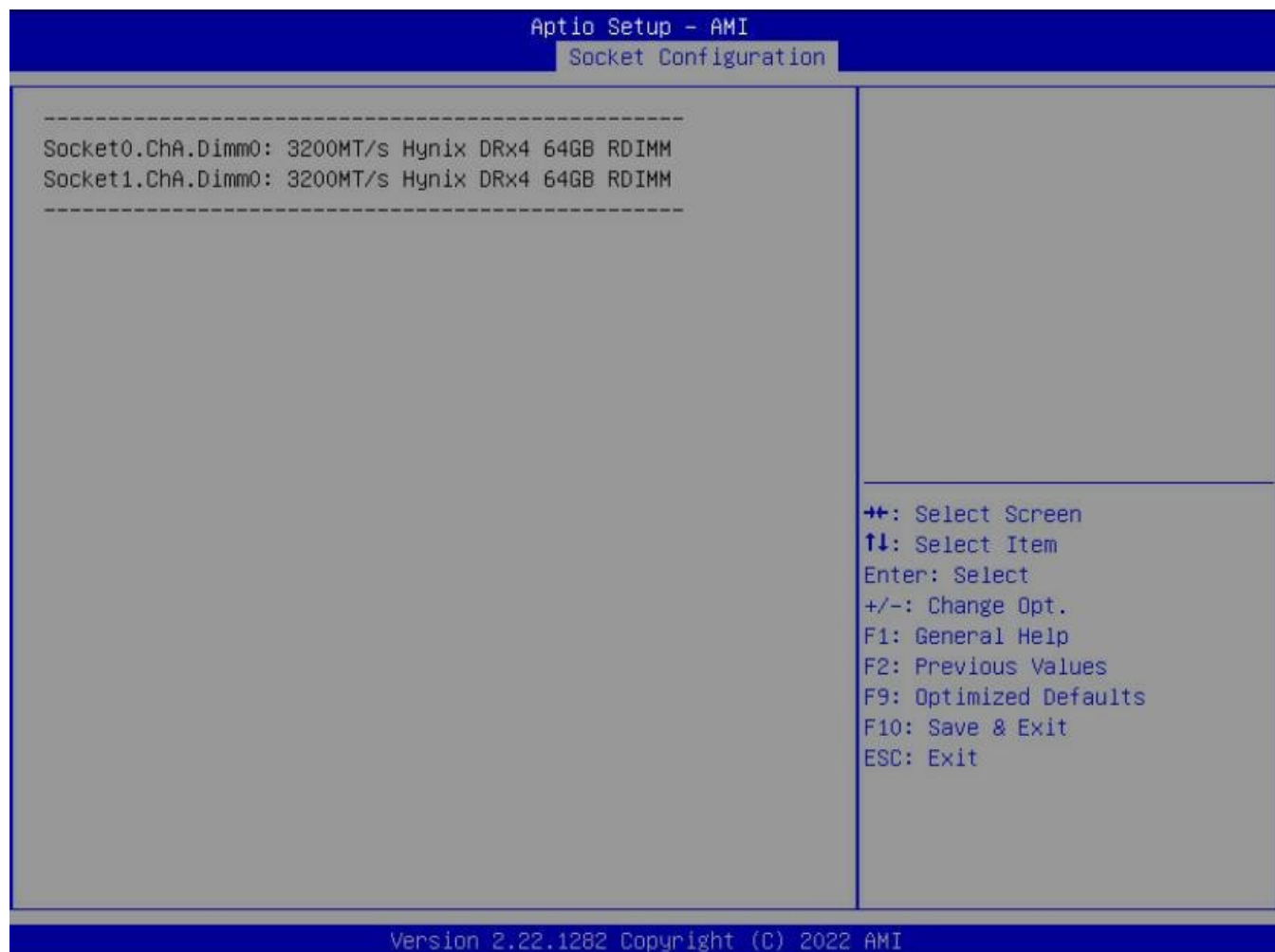


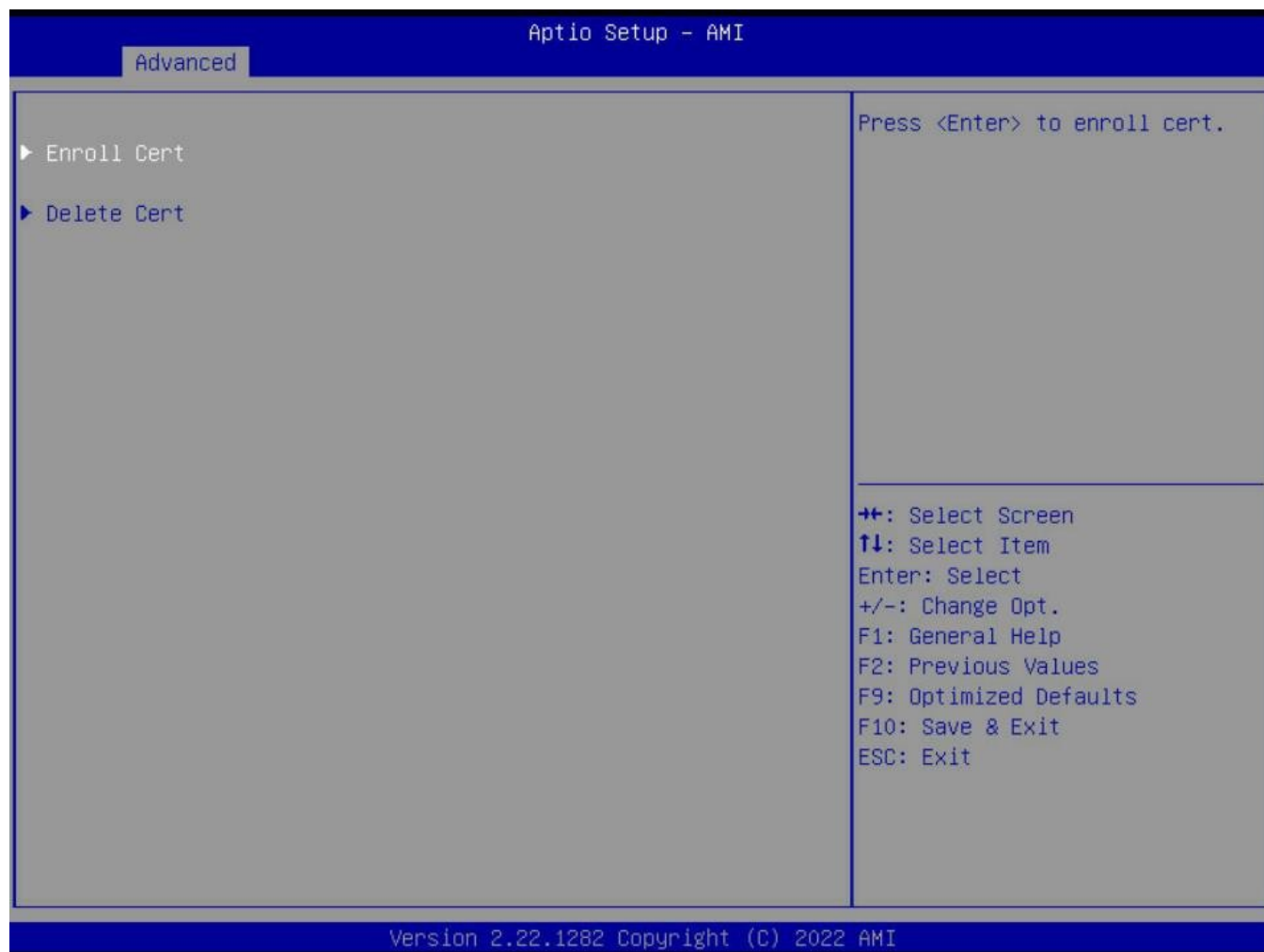
Рисунок 0-15 Tls Auth Configuration

Настройка BIOS	Опции	Описание
Server CA Configuration	См. подробнее.	Нажмите для настройки Server CA.

Client Cert Configuration Read Only

Таблица 0-16 Tls Auth Configuration





Настройка Server CA

6.2.10. All CPU Information

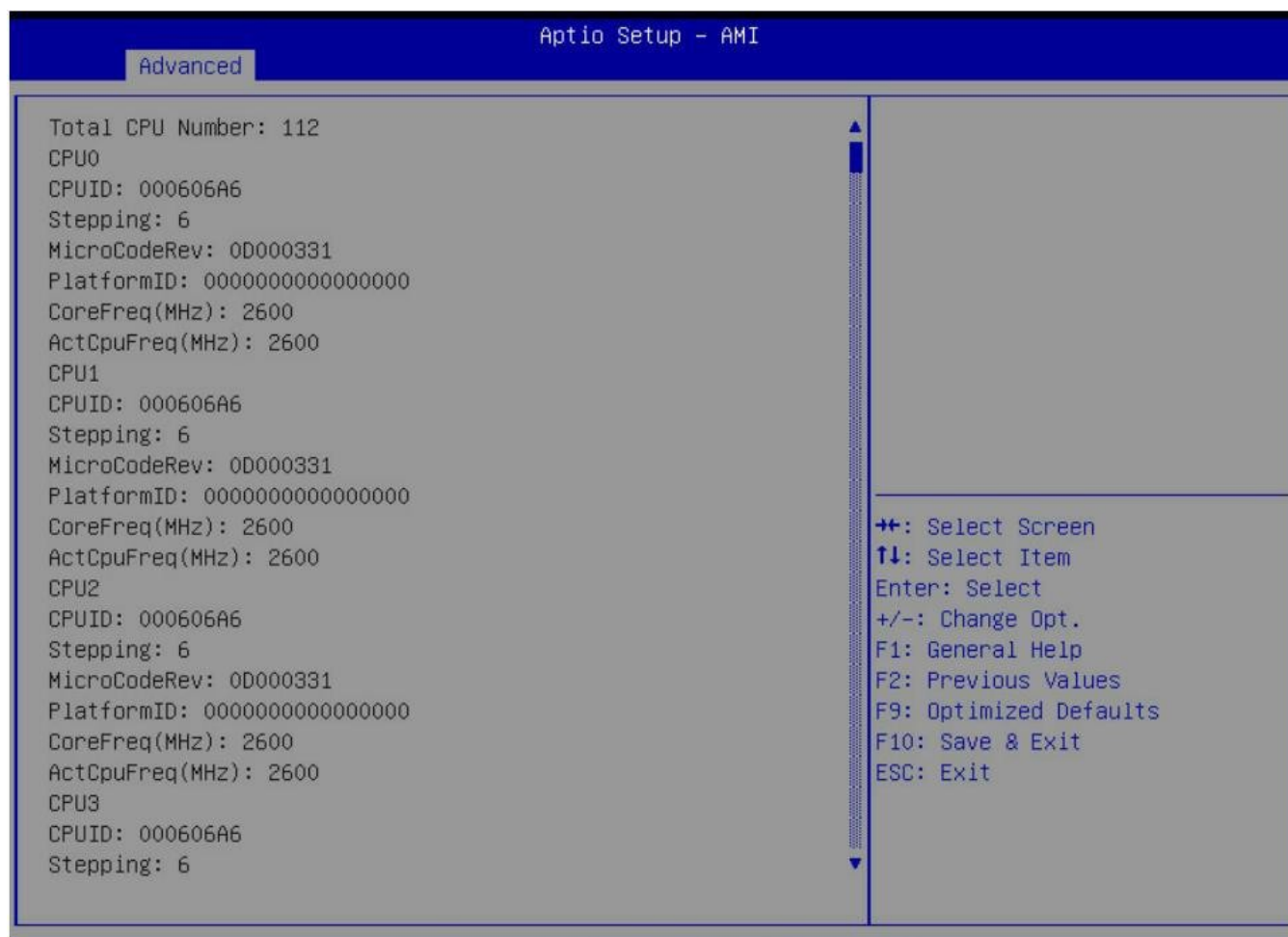
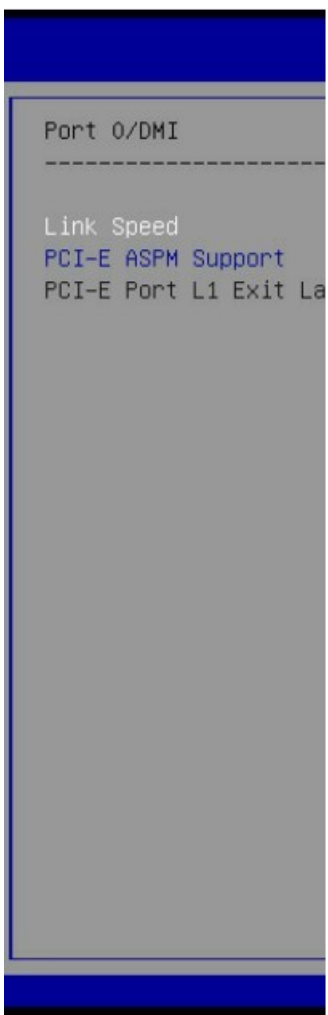
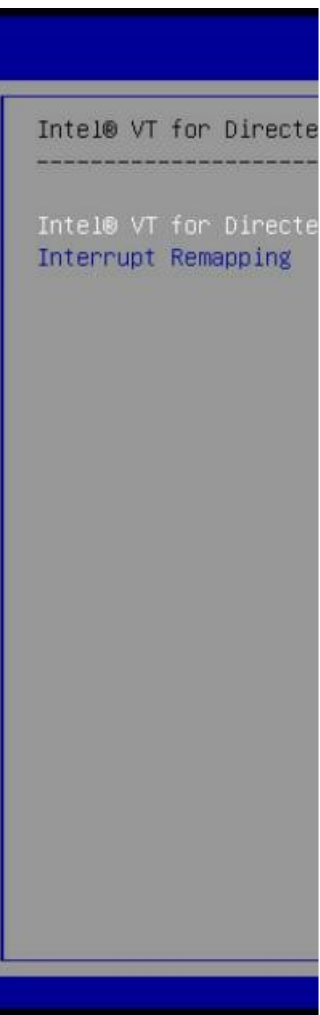


Рисунок 0-16 All CPU Information

Настройка BIOS	Опции	Опции	Описание
NVMe controller and Drive information	NVMe controller and Drive information	NVMe controller and Drive information	Информации о контроллере и дисках NVMe

Настройка BIOS	Опции	Опции	Описание
		Total CPU Number: 112	Всего процессоров: 112
IOU0 (IIIO PCIe Port 1 IOU1 (IIIO PCIe Port 2 IOU3 (IIIO PCIe Port 4 IOU4 (IIIO PCIe Port 5 ▶ Port 0/DMI ▶ Port 1A ▶ Port 1B ▶ Port 1C ▶ Port 2A ▶ Port 4A ▶ Port 5A	Port 1A ----- PCI-E Port Hot Plug Capable Surprise Hot Plug Cap PCI-E Port Link Disab Link Speed PCI-E Port Link Statu PCI-E Port Link Max PCI-E Port Link Speed PCI-E Port Clocking PCI-E Port Clock Gati Data Link Feature Exc PCI-E Port MPSS PCI-E Port D-state PCI-E Completion Time PCI-E ASPM Support PCI-E Port L1 Exit La		

Настройка BIOS	Опции	Опции	Описание
			
Read Only:	Read Only:		
		CPU0	CPU0
		CPUID: 000606A6	CPUID: 000606A6
		Stepping: 6	Stepping: 6
		MicroCodeRev: 0D000331	MicroCodeRev: 0D000331
		PlatformID: 0000000000000000	PlatformID: 0000000000000000
		CoreFreq (MHz): 2600	CoreFreq (MHz): 2600
		ActCpuFreq (MHz): 2600	ActCpuFreq (MHz): 2600
		CPU1	CPU1
		CPUID: 000606A6	CPUID: 000606A6
		Stepping: 6	Stepping: 6
		MicroCodeRev: 0D000331	MicroCodeRev: 0D000331
		PlatformID:	PlatformID:

Настройка BIOS	Опции	Опции	Описание
		0000000000000000	0000000000000000
		CoreFreq (MHz): 2600	CoreFreq (MHz): 2600
		ActCpuFreq (MHz): 2600	ActCpuFreq (MHz): 2600
		CPU2	CPU2
		CPUID: 000606A6	CPUID: 000606A6
		Stepping: 6	Stepping: 6
		MicroCodeRev: 0D000331	MicroCodeRev: 0D000331
		PlatformID: 0000000000000000	PlatformID: 0000000000000000
		CoreFreq (MHz): 2600	CoreFreq (MHz): 2600
		ActCpuFreq (MHz): 2600	ActCpuFreq (MHz): 2600
		CPU3	CPU3
		CPUID: 000606A6	CPUID: 000606A6
		Stepping: 6	Stepping: 6

Таблица 0-17 All CPU Information

6.2.11. RAM Disk Configuration

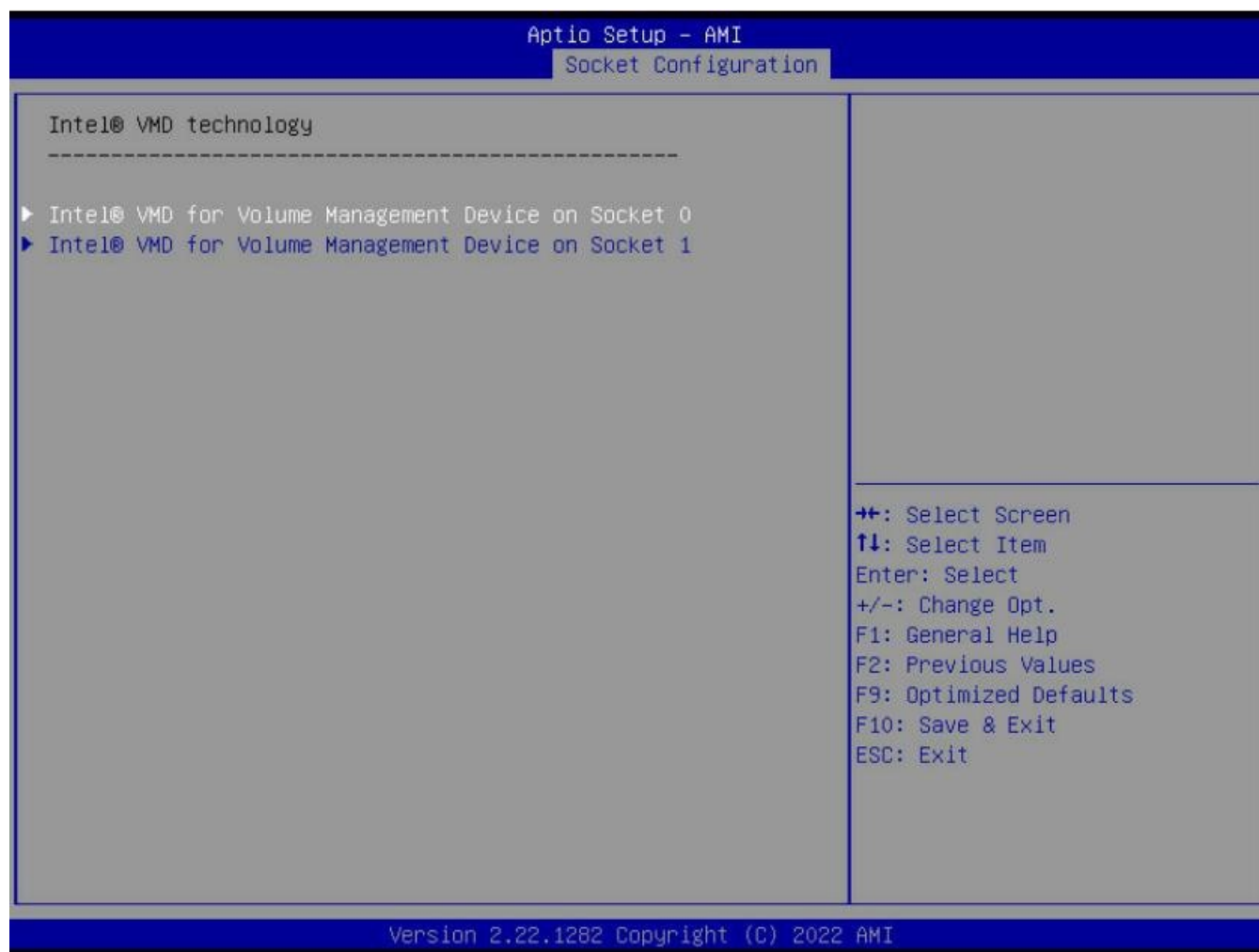




Рисунок 0-17 RAM Disk Configuration

Настройка BIOS	Опции	Описание
Disk Memory Type : [Boot Service Data]	Disk Memory Type : [Boot Service Data]	Тип памяти диска : [Boot Service Data]
Create raw	См. подробнее.	
Create from file	См. подробнее.	

Таблица 0-18 RAM Disk Configuration

6.2.11.1. Create raw

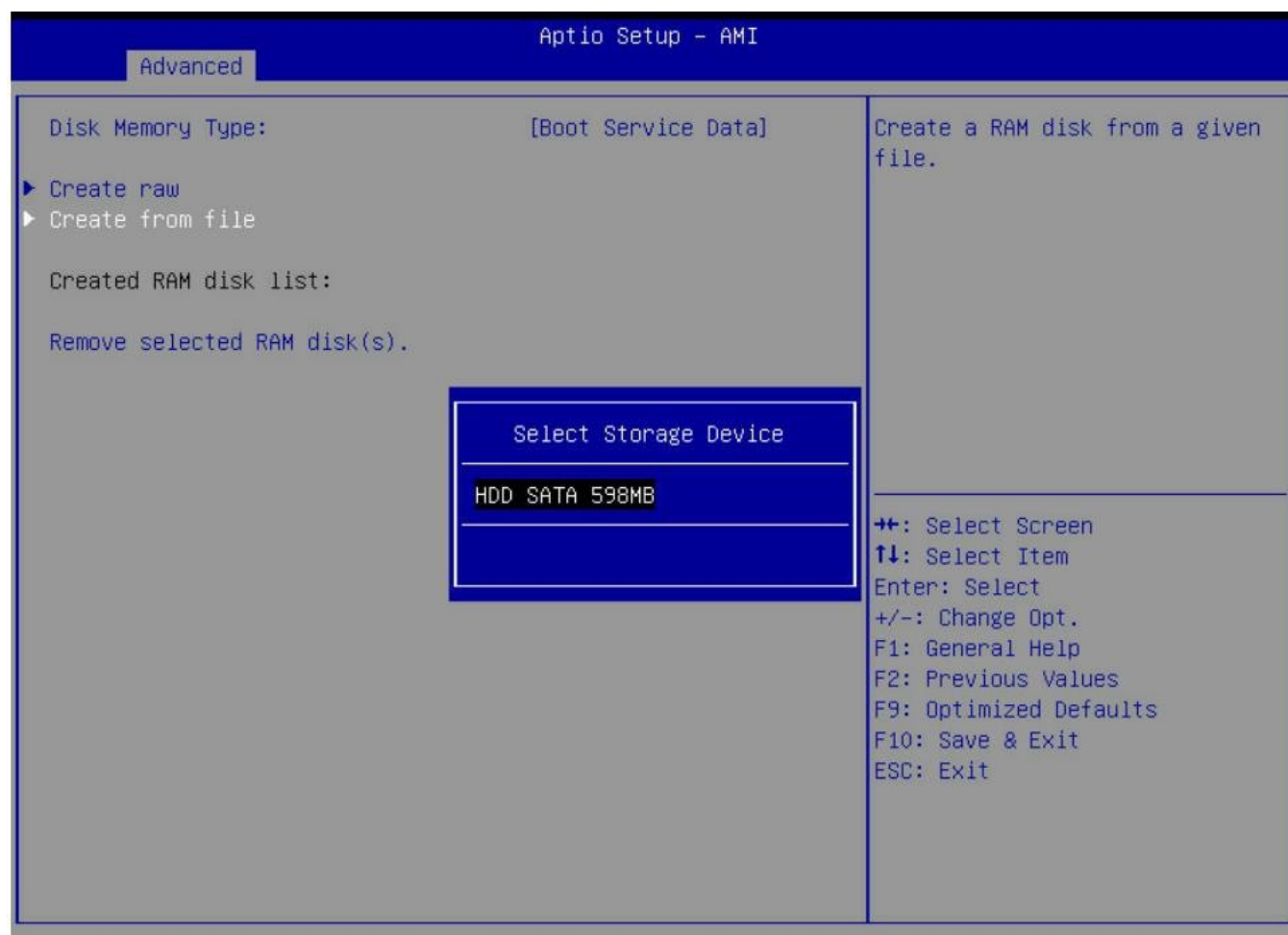
Aptio Setup - AMI	
Advanced	
Size (Hex):	1
Create & Exit	
Discard & Exit	
The valid RAM disk size should be multiples of the RAM disk block size.	
<>: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.22.1282 Copyright (C) 2021 AMI	
Aptio Setup - AMI	
Socket Configuration	
CPU P State Control	Enable/Disable EIST (P-States)
SpeedStep (Pstates)	[Enable]
EIST PSD Function	[HW ALL]
Boot performance mode	[Max Performance]
Energy Efficient Turbo	[Enable]
Turbo Mode	[Enable]
<>: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.22.1282 Copyright (C) 2021 AMI	

Рисунок 0-18 Create raw

Настройка BIOS	Опции	Описание
Size (Hex):	1	Допустимый размер RAM диска должен быть кратен размеру блока RAM диска.
Create & Exit		Создать новый RAM диск с заданным начальным и конечным адресом.
Discard & Exit		Отменить и выйти.
WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	ПРЕДУПРЕЖДЕНИЕ: Отключение логических устройств SIO может иметь нежелательные побочные эффекты. ДЕЙСТВУЙТЕ С ОСТОРОЖНОСТЬЮ.

Таблица 0-19 Create raw

6.2.11.2. Create from file



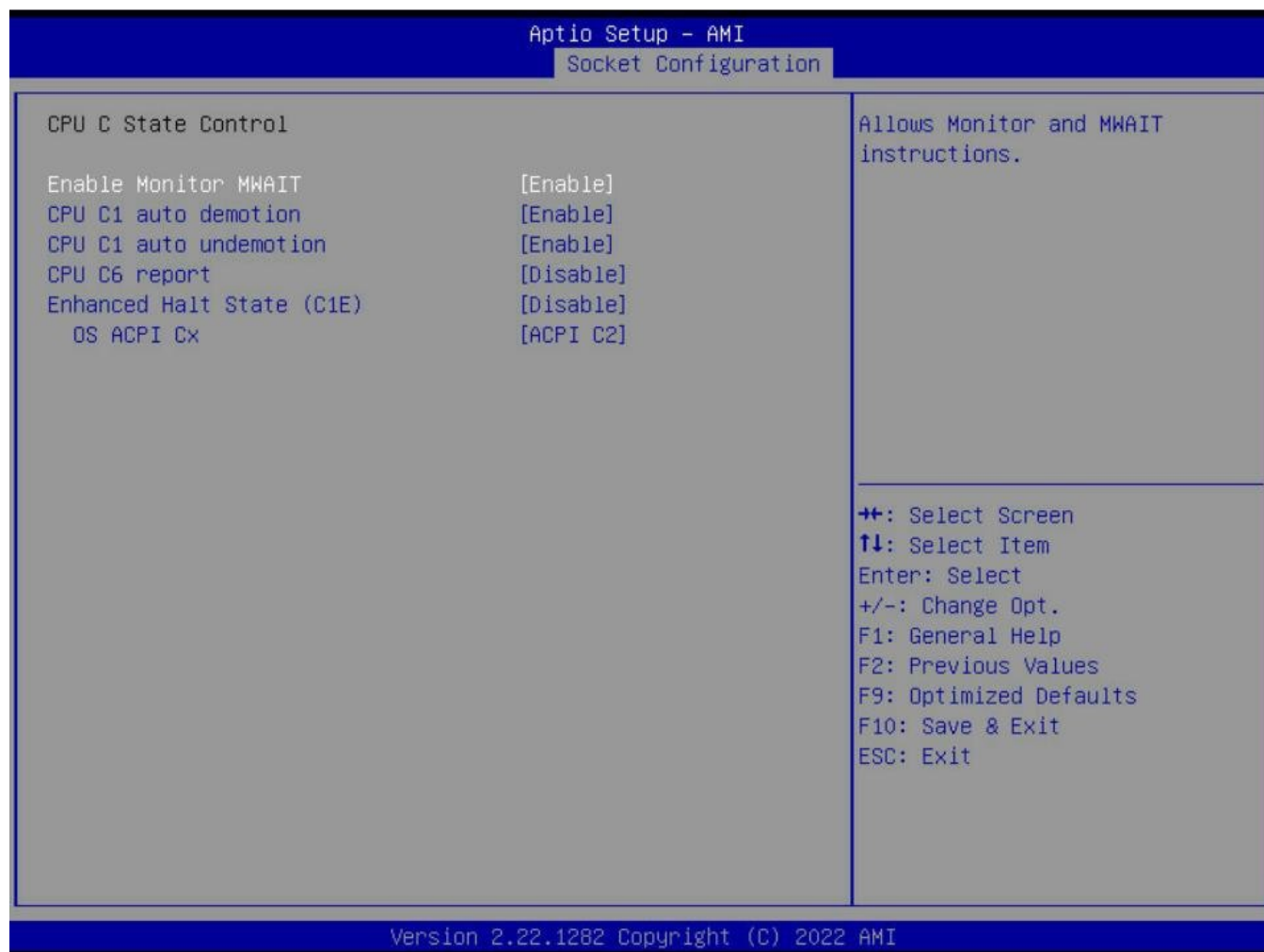


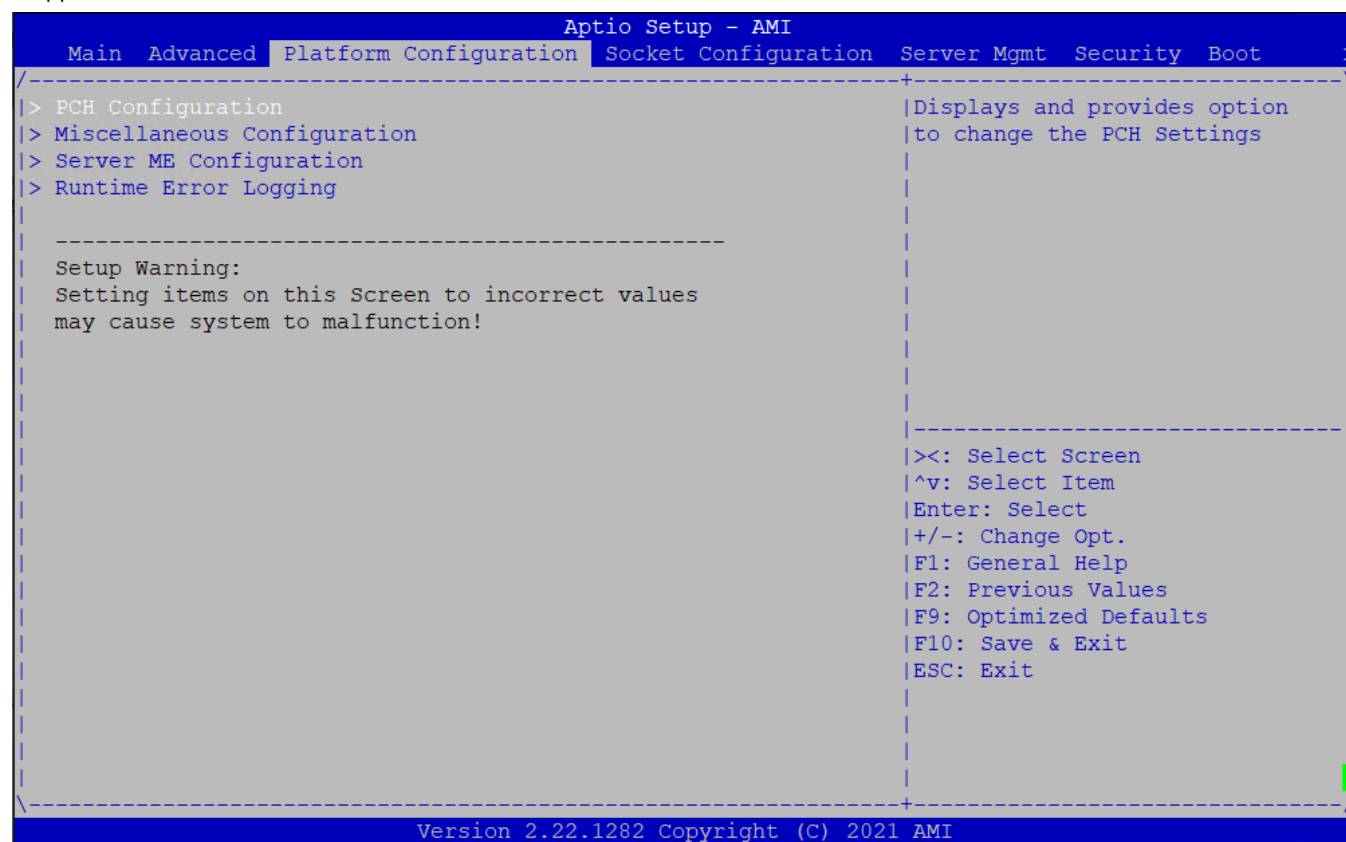
Рисунок 0-19 Create from file

Настройка BIOS	Опции	Описание
Select Storage Device:	HDD SATA 96MB	Создать RAM диск из заданного файла.
WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.	ПРЕДУПРЕЖДЕНИЕ: Отключение логических устройств SIO может иметь нежелательные побочные эффекты. ДЕЙСТВУЙТЕ С ОСТОРОЖНОСТЬЮ.

Таблица 0-20 Create from file

6.3. Platform Configuration

Используйте меню **Platform Configuration** для настройки устройств PCH через следующие подменю.



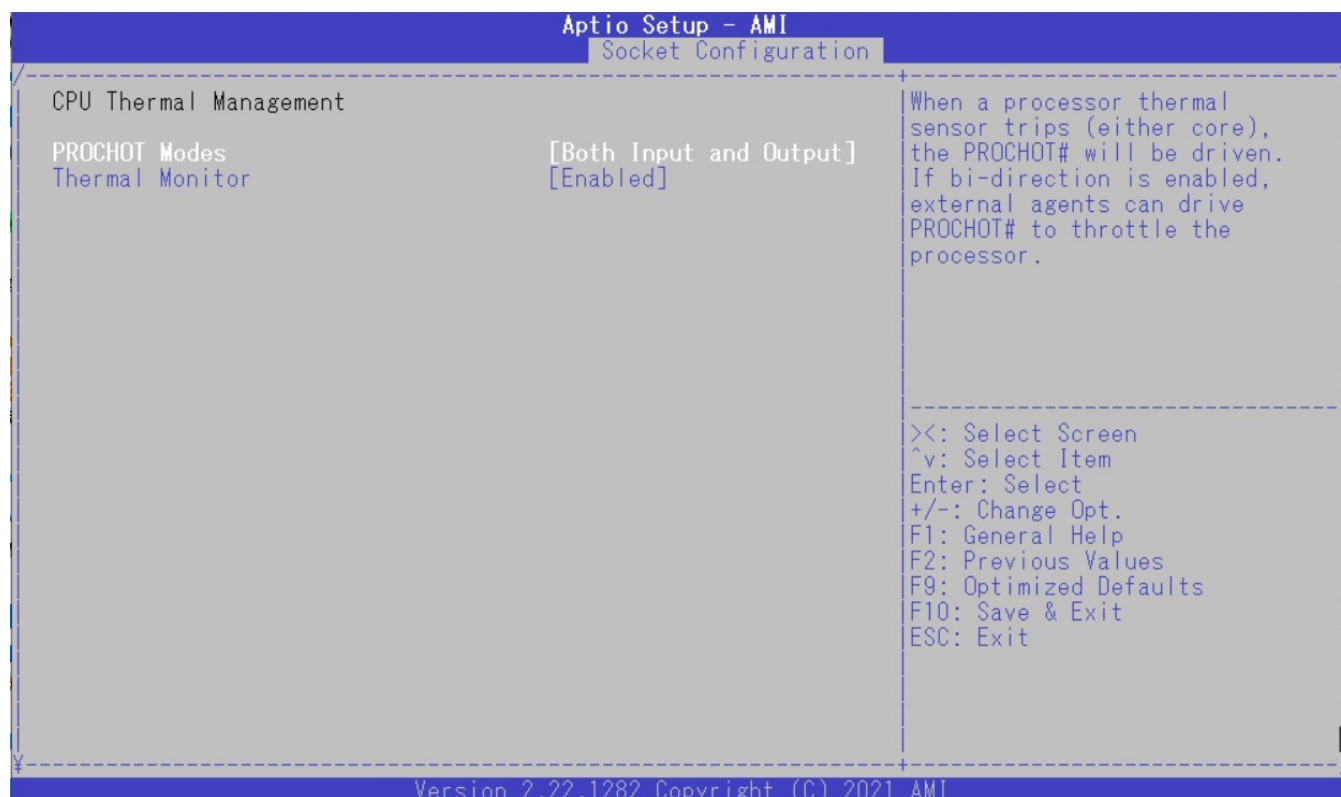


Рисунок 0-20 Platform Configuration

Настройка BIOS	Опции	Описание
PCH Configuration	См. подробнее.	Отображает и предоставляет опцию для изменения настроек PCH.
Miscellaneous Configuration	См. подробнее.	Отображает и предоставляет опцию для изменения настроек Miscellaneous.
Server ME Configuration	См. подробнее.	Настройка параметров Server ME Technology
Runtime Error Logging	См. подробнее.	Нажмите для просмотра или изменения конфигурации журнала ошибок времени выполнения.

Таблица 0-21 Platform Configuration

6.3.1. PCH Configuration



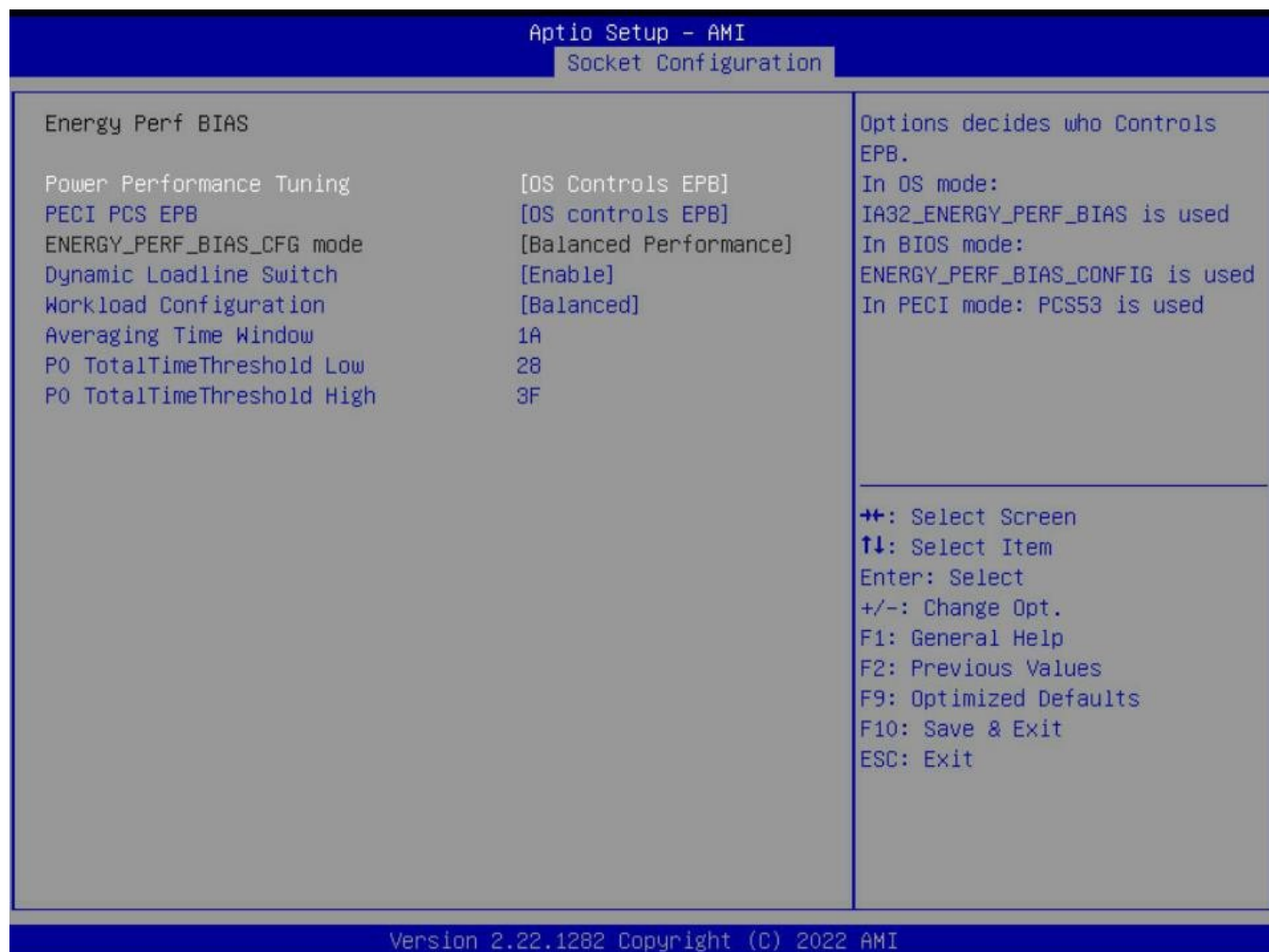


Рисунок 0-21 PCH Configuration

Настройка BIOS	Опции	Описание
PCH Configuration	PCH Configuration	Конфигурация PCH
PCH Devices	См. подробнее	PCIe контроллер и настройки.
PCI Express Configuration	См. подробнее	PCIe контроллер и настройки.
PCH SATA Configuration	См. подробнее.	Контроллер SATA и настройки.
PCH sSATA Configuration	См. подробнее	Контроллер sSATA и настройки.
USB Configuration	См. подробнее	Контроллер USB и настройки.

Таблица 0-22 PCH Configuration

6.3.1.1. PCH Devices



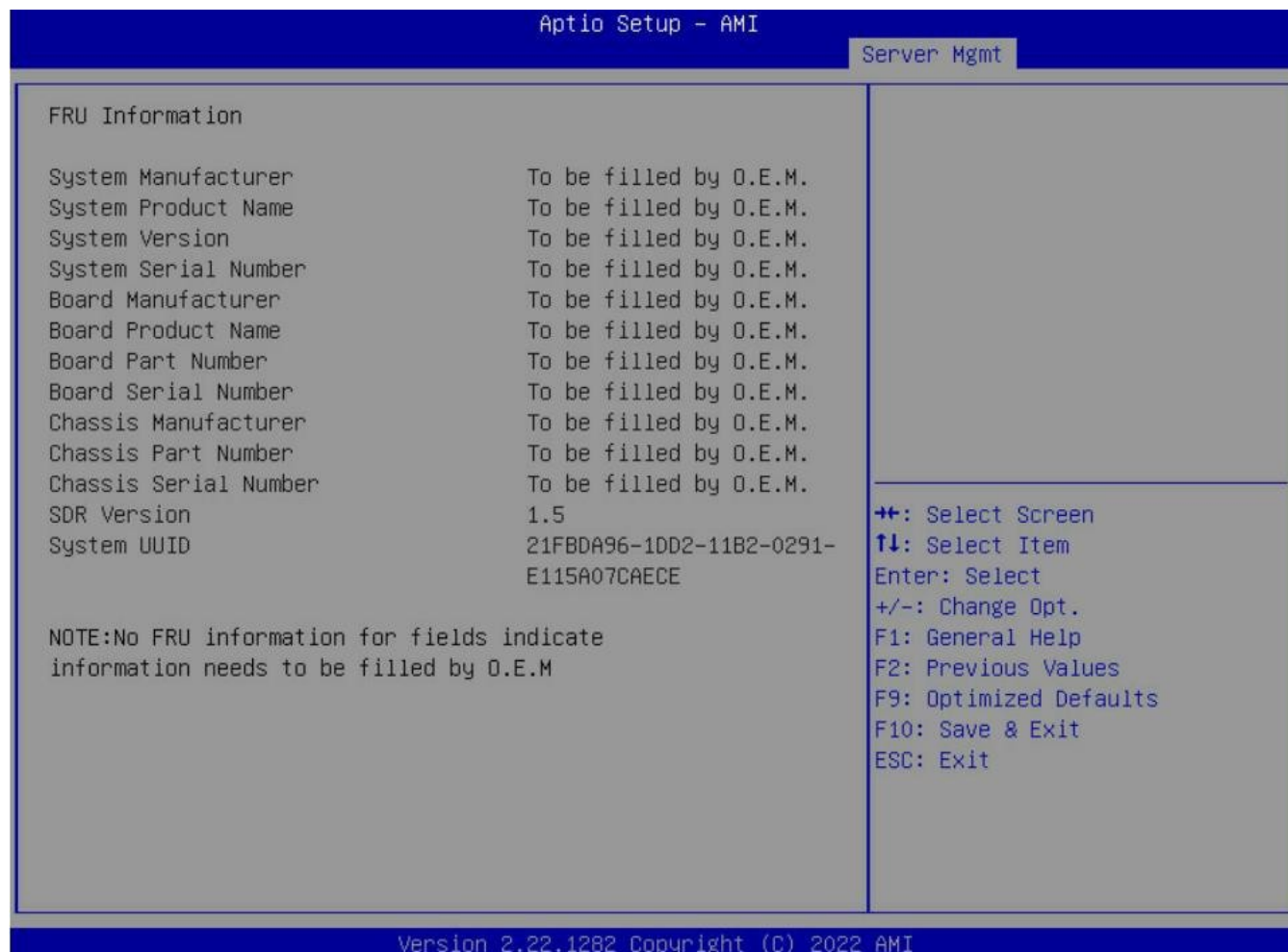


Рисунок 0-22 PCH Devices

Настройка BIOS	Опции	Описание
PCH Devices	PCH Devices	Устройства PCH
Serial IRQ Mode	Quiet / Continuous	Настройка режима Serial IRQ.

Таблица 0-23 PCH Devices

6.3.1.2. PCIE Express Configuration



Рисунок 0-23 PCI Express Configuration

Настройка BIOS	Опции	Описание
PCI Express Root Port	См. подробнее	Настройки корневого порта PCI Express.

Таблица 0-24 PCI Express Configuration

6.3.1.3. PCI Express Root Port

Aptio Setup - AMI			Server Mgmt
No. of log entries in SEL : 893			^ HEX:
DATE	TIME	SENSOR TYPE	* 01 00 02 E1 BF 17
			+ 60 20 00 04 01 50
			+ 01 57 5F 5F
02/01/21	08:46:25	Temperature	+ Generator ID: BMC - LUN #0
02/01/21	08:46:53	Temperature	+ (Channel #0)
02/01/21	08:53:47	Temperature	+ Sensor Number: 0x50 Reserved
02/01/21	08:54:34	Temperature	+ or Unknown
02/01/21	08:59:25	Temperature	+ Event Description: Record
02/01/21	09:00:08	Temperature	+ Type-0x02. Assertion Event.
02/01/21	09:16:17	Temperature	+
02/01/21	09:16:50	Temperature	+
02/01/21	09:17:56	Temperature	+ -----
02/01/21	09:18:31	Temperature	+ ><: Select Screen
02/01/21	09:21:47	Temperature	+ ^v: Select Item
02/01/21	09:22:19	Temperature	+ Enter: Select
02/02/21	07:50:16	Temperature	+ +/-: Change Opt.
02/02/21	07:51:19	Temperature	+ F1: General Help
02/01/21	09:01:51	Temperature	+ F2: Previous Values
02/01/21	09:02:33	Temperature	+ F9: Optimized Defaults
02/05/21	04:53:21	Temperature	+ F10: Save & Exit
02/05/21	04:53:53	Temperature	+ ESC: Exit
02/05/21	04:55:05	Temperature	+
02/05/21	04:55:39	Temperature	+
02/25/21	04:55:50	Temperature	v
Version 2.22.1282 Copyright (C) 2021 AMI			



Рисунок 0-24 PCI Express Configuration Root Port

Настройка BIOS	Опции	Описание
PCI Express Root Port x	PCI Express Root Port x	Корневой порт PCI Express x
PCI Express Root Port x	Enabled / Disabled	Управление корневым портом PCI Express
PCIE ASPM	Disable ASPM / ASPM L1/ ASPM Auto	Настройка ASPM корневого порта PCI Express
Hot Plug	Enabled / Disabled	Включить/выключить Hot Plug для PCI Express
Advanced Error Reporting	Enabled / Disabled	Включить/выключить расширенные отчеты об ошибках
PCIE Speed	Auto / Gen1 / Gen2 / Gen3	Настройка скорости PCIe
Max Payload Size	MPL 128B / MPL 256B	Выбор максимального размера полезной нагрузки PCIE

Таблица 0-25 PCI Express Configuration Root Port

6.3.1.4. PCH SATA Configuration

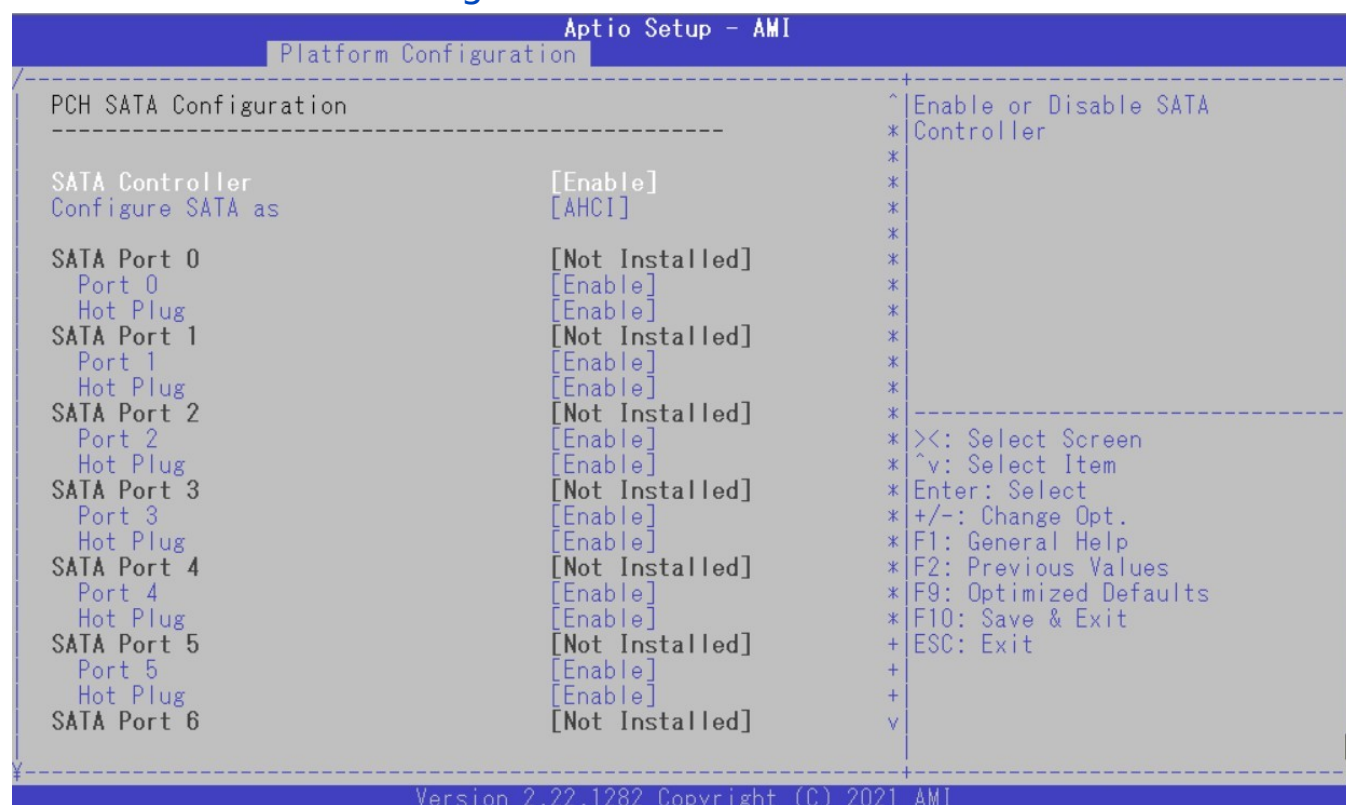




Рисунок 0-25 PCH SATA Configuration

Настройка BIOS	Опции	Описание
PCH SATA Configuration	PCH SATA Configuration	Конфигурация PCH SATA
SATA Controller	Enabled / Disabled	Включить или отключить контроллер SATA
Configure SATA as	AHCI / RAID	Укажите, подключен ли порт SATA к SSD или HDD
SATA Port 0~7	Read only	Только для чтения
Port 0~7	Enabled / Disabled	Включить или отключить SATA порт 0~7
Hot Plug	Enabled / Disabled	Обозначает этот порт как поддерживающий горячую замену

Таблица 0-26 PCH SATA Configuration

6.3.1.5. PCH sSATA Configuration

Platform Configuration		Aptio Setup - AMI
PCH sSATA Configuration		Enable or Disable SATA Controller
sSATA Controller	[Enable]	
Configure sSATA as	[AHCI]	
sSATA Port 0	[Not Installed]	
Port 0	[Enable]	
Hot Plug	[Enable]	
sSATA Port 1	[Not Installed]	
Port 1	[Enable]	
Hot Plug	[Enable]	
sSATA Port 2	[Not Installed]	
Port 2	[Enable]	
Hot Plug	[Enable]	
sSATA Port 3	[Not Installed]	
Port 3	[Enable]	
Hot Plug	[Enable]	
sSATA Port 4	[Not Installed]	
Port 4	[Enable]	
Hot Plug	[Enable]	
sSATA Port 5	[Not Installed]	
Port 5	[Enable]	
Hot Plug	[Enable]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.22.1282 Copyright (C) 2021 AMI		

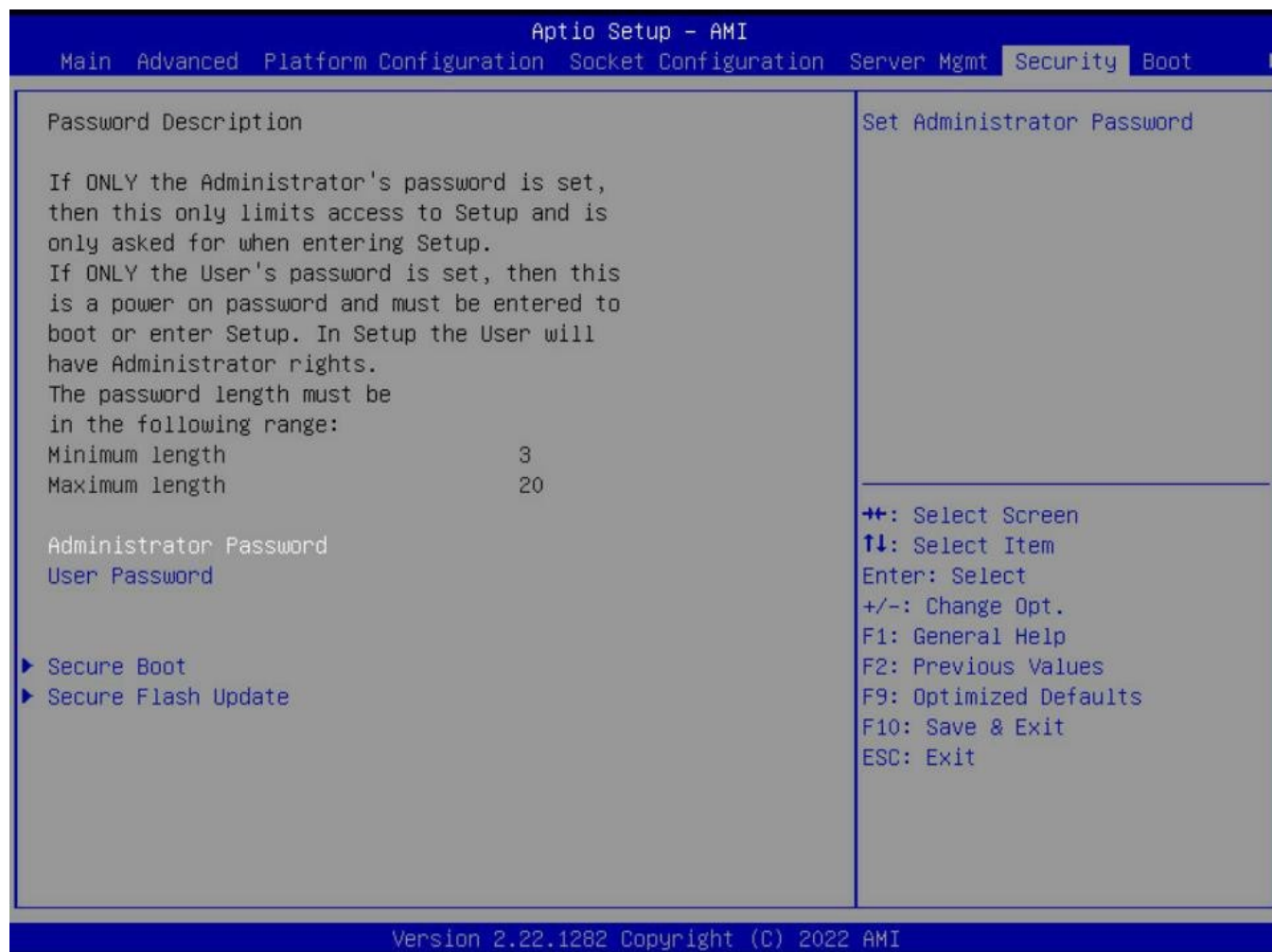


Рисунок 0-26 PCH sSATA Configuration

Настройка BIOS	Опции	Описание
PCH sSATA Configuration	PCH sSATA Configuration	Конфигурация PCH sSATA
sSATA Controller	Enabled / Disabled	Включить или отключить контроллер SATA.
Configure sSATA as	AHCI / RAID	Укажите, подключен ли порт SATA к SSD или HDD.
sSATA Port 0~5	Read only	Только для чтения
Port 0~5	Enabled / Disabled	Включить или отключить sSATA порт.
Hot Plug	Enabled / Disabled	Обозначает этот порт как поддерживающий горячую замену

Таблица 0-27 PCH sSATA Configuration

6.3.1.6. USB Configuration



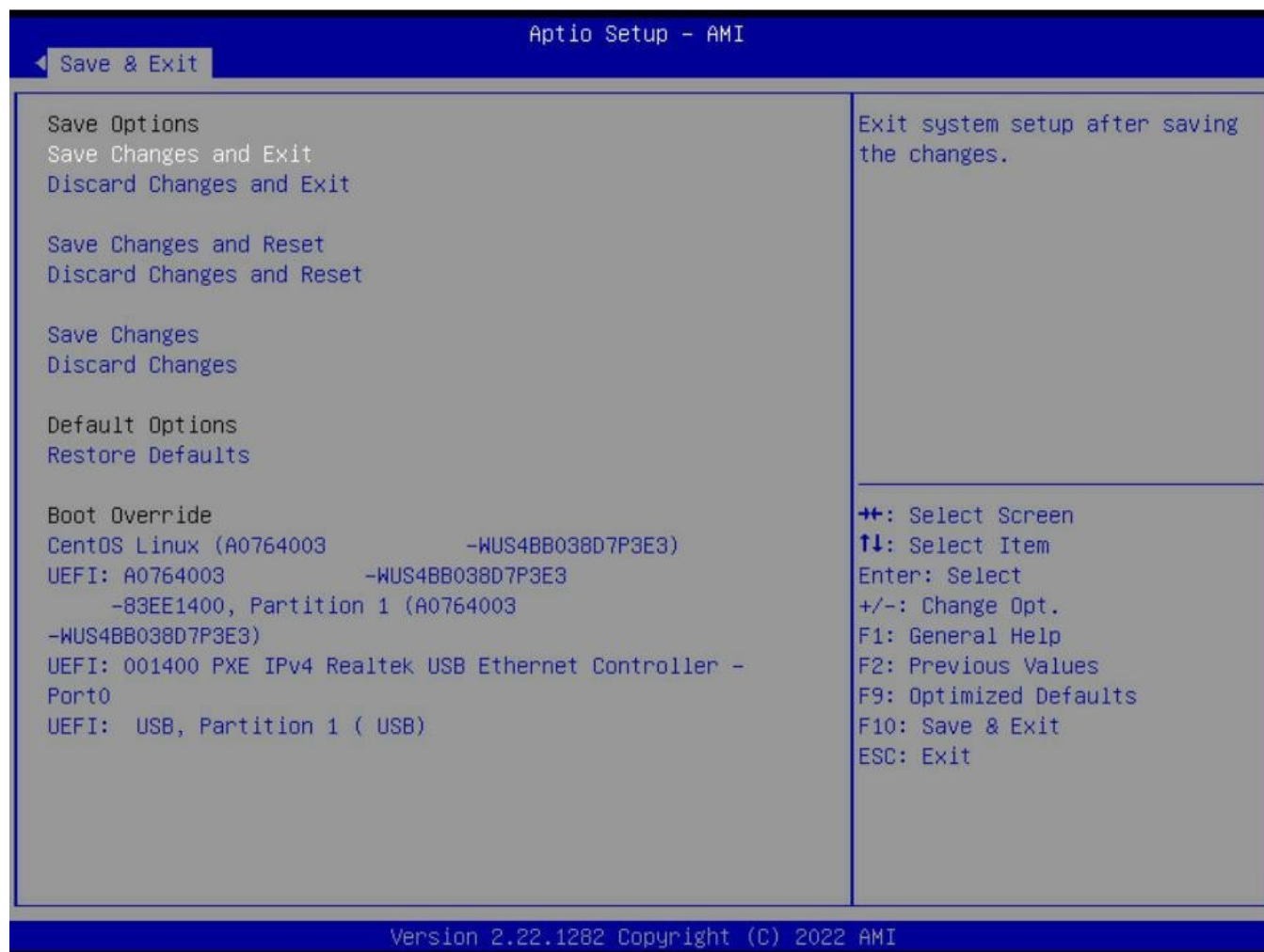


Рисунок 0-27 USB Configuration

Настройка BIOS	Опции	Описание
USB Per-Connector Disable	Enable / Disable	Выборочное включение/отключение каждого физического разъема USB (физического порта). Как только разъем отключен, любые USB устройства, подключенные к разъему, не будут обнаружены BIOS или ОС.

Таблица 0-28 USB Configuration

6.3.2. Miscellaneous Configuration



Рисунок 0-28 Miscellaneous Configuration

Настройка BIOS	Опции	Описание
Miscellaneous Configuration	Miscellaneous Configuration	Различные настройки
BIOS Serial Port Baud Rate	115200 / 921600	Устанавливает скорость последовательного порта BIOS перед загрузкой ОС
Serial Debug Message Level	Disable / Minimum / Normal / Maximum / Auto / Fixed PCD	Disable = нет сообщений, Minimum = критические сообщения, Normal = критические и информационные сообщения, Maximum = все сообщения, Auto = Minimum (по умолчанию) или Normal (Advanced Debug mode)
Trace Messages	Disable / Enable / Enable for registry writes only.	Включает отображение каждого ввода-вывода

Настройка BIOS	Опции	Описание
Training Messages	Enable / Disable	Включить для отображения результатов обучения. Результаты обучения также отображаются, если уровень отладки установлен на Maximum.
Active Video	Auto / Onboard Device /PCIE Device	Выберите активный тип видео

Таблица 0-29 Miscellaneous Configuration

6.3.3. Server ME Configuration

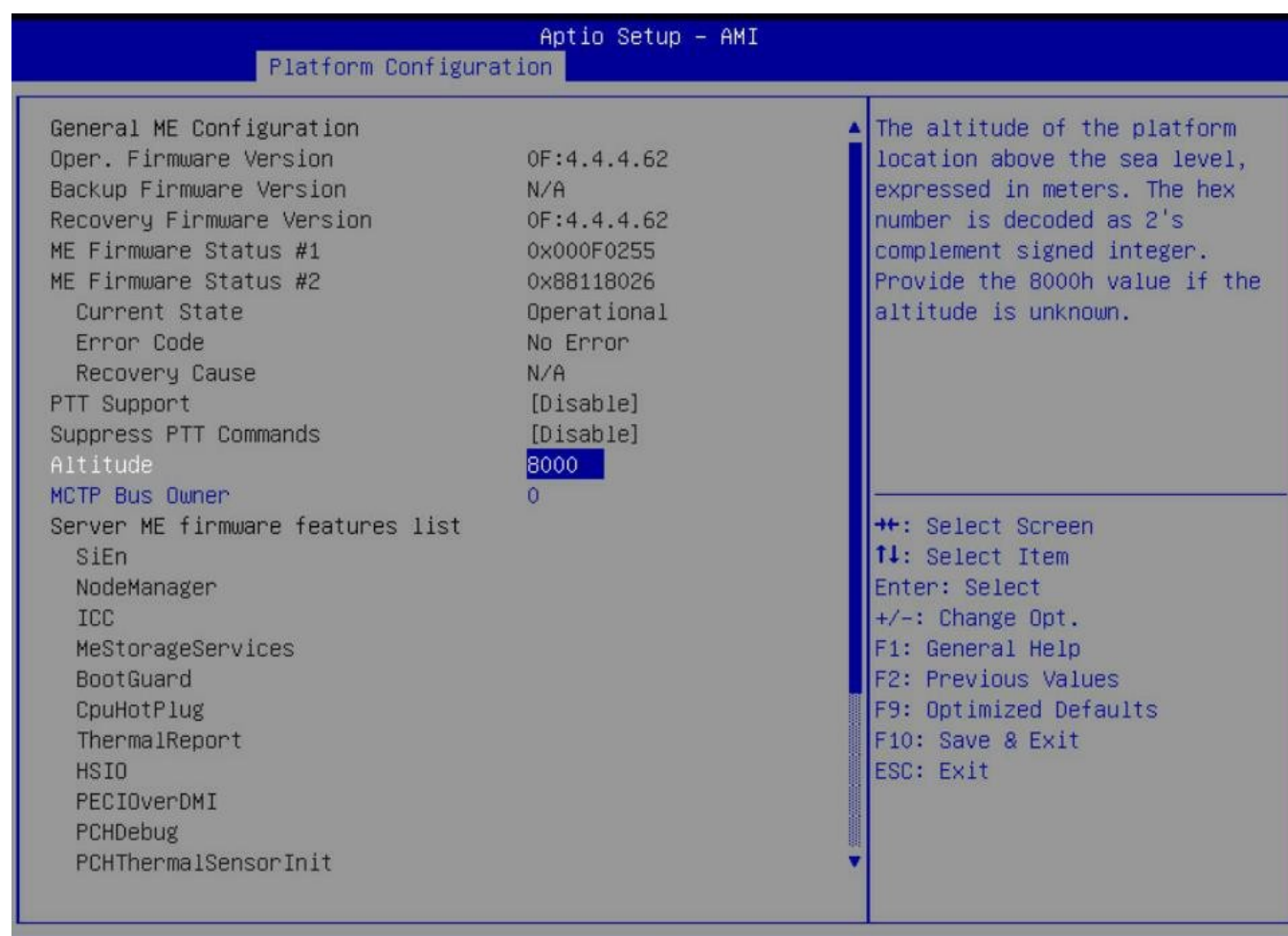


Рисунок 0-29 Server ME Configuration

Настройка BIOS	Опции	Описание
General ME Configuration	General ME Configuration	Общая конфигурация ME
Operational Firmware Version	Read Only	Версия операционной прошивки, выбранной для

Настройка BIOS	Опции	Описание
		запуска.
ME Firmware Type	Read Only	Тип прошивки ME (Workstation/HEDT или SPS)
Recovery Firmware Version	Read Only	Версия прошивки восстановления - запускается, когда ME находится в режиме восстановления.
ME Firmware Features	Read Only	Список функций прошивки Server ME
ME Firmware Status #1	Read Only	Регистр ME Firmware Status #1 в конфигурационном пространстве HECI-1.
ME Firmware Status #2	Read Only	Регистр ME Firmware Status #2 в конфигурационном пространстве HECI-1.
Current State	Read Only	Текущее состояние прошивки ME, биты [3:0] в MEFS1.
Error Code	Read Only	Код ошибки прошивки Server ME, биты [15:12] в MEFS1.
Altitude	8000	Высота местоположения платформы над уровнем моря, выраженная в метрах. Шестнадцатеричное число декодируется как 2's complement signed integer. Укажите значение 8000h, если высота неизвестна.
MCTP Bus Owner	0	Местоположение владельца шины MCTP на PCIe: [15:8] шина, [7:3] устройство, [2:0] функция. Если все нули, отправка владельца шины отключена.
Server ME firmware features list	Read Only	SiEn ICCBootGuard DeepSxDirectMeUpdate

Таблица 0-30 Server ME Configuration

6.3.4. Runtime Error Logging

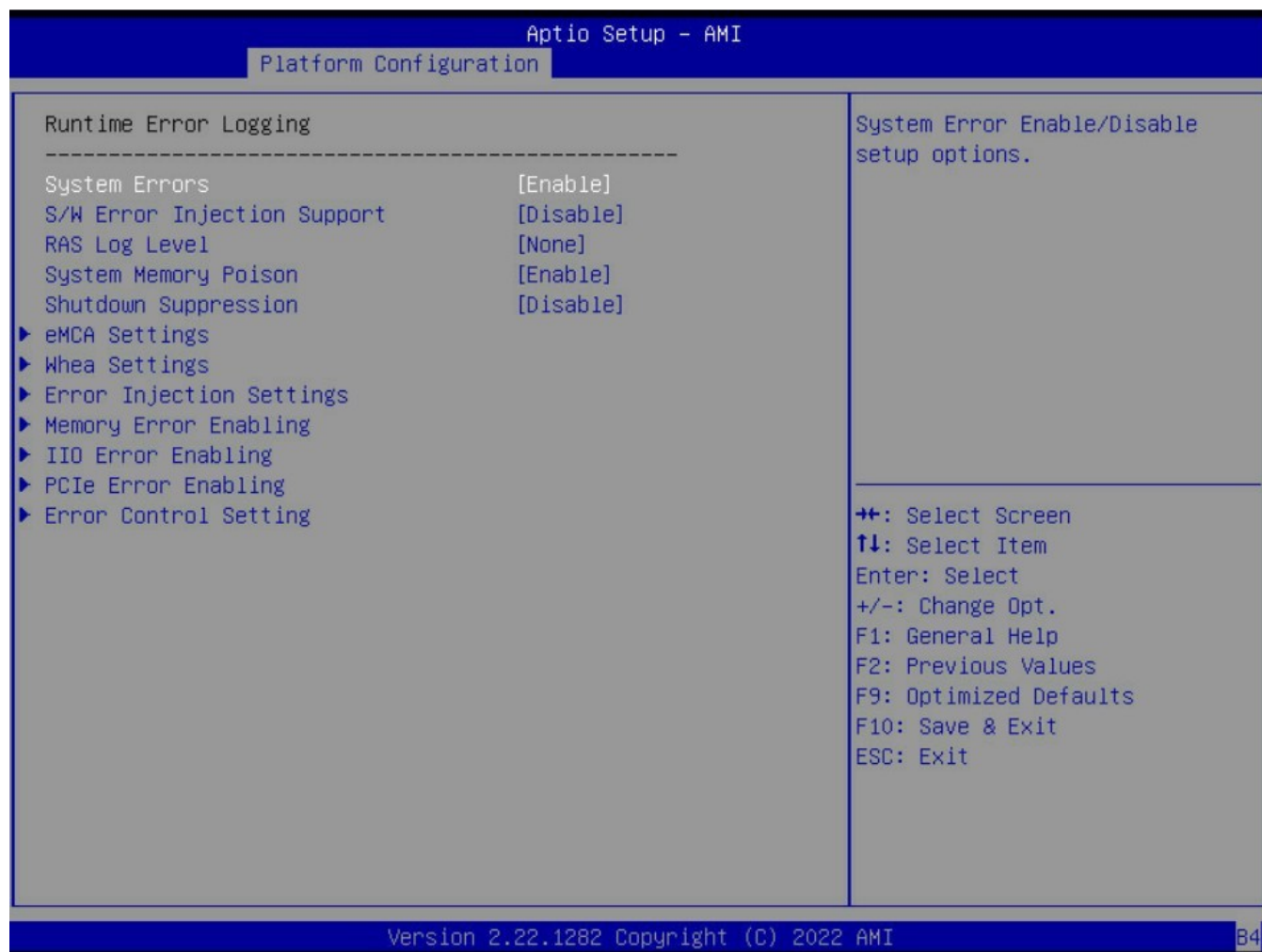


Рисунок 0-30 Runtime Error Logging

Настройка BIOS	Опции	Описание
Runtime Error Logging	Runtime Error Logging	Журнал ошибок времени выполнения
System Errors	Disable / Enable	Опция включения и настройки журнала системных ошибок.
S/W Error Injection Support	Disable / Enable	Когда включено, S/W Error Injection поддерживается путем разблокировки MSR 0x790
RAS Log Level	None /MIN (BASIC_FLOW) / MID (BASIC_FLOW,	Опции настройки RAS Log.
	FUNC_FLOW) /MAX (BASIC_FLOW, FUNC_FLOW, REG)	
System Memory Poison	Disable / Enable	Включить/отключить memory

	FUNC_FLOW) /MAX (BASIC_FLOW, FUNC_FLOW, REG)	
		poison.
Shutdown Suppression	Disable / Shutdown Suppression and Log MCA IERR /Shutdown Log MCA IERR	Настраивает подавление выключения и журнал MCA IERR.
eMCA Settings:	См. подробнее	Нажмите для просмотра или изменения конфигурации eMCA.
Whea Settings :	См. подробнее	Нажмите для просмотра или изменения конфигурации WHEA.
Error Injection Settings	См. подробнее	Нажмите для просмотра или изменения конфигурации Error Injection.
Memory Error Enabling:	См. подробнее	Нажмите для просмотра или изменения опций включения ошибок памяти.
IIO Error Enabling:	См. подробнее	Нажмите для просмотра или изменения опций включения ошибок IIO.
PCIe Error Enabling	См. подробнее	Нажмите для просмотра или изменения опций включения ошибок PCIe.
Error Control Setting	См. подробнее	Нажмите для просмотра или изменения опций настройки контроля ошибок.

Таблица 0-31 Runtime Error Logging

6.3.4.1. eMCA Settings

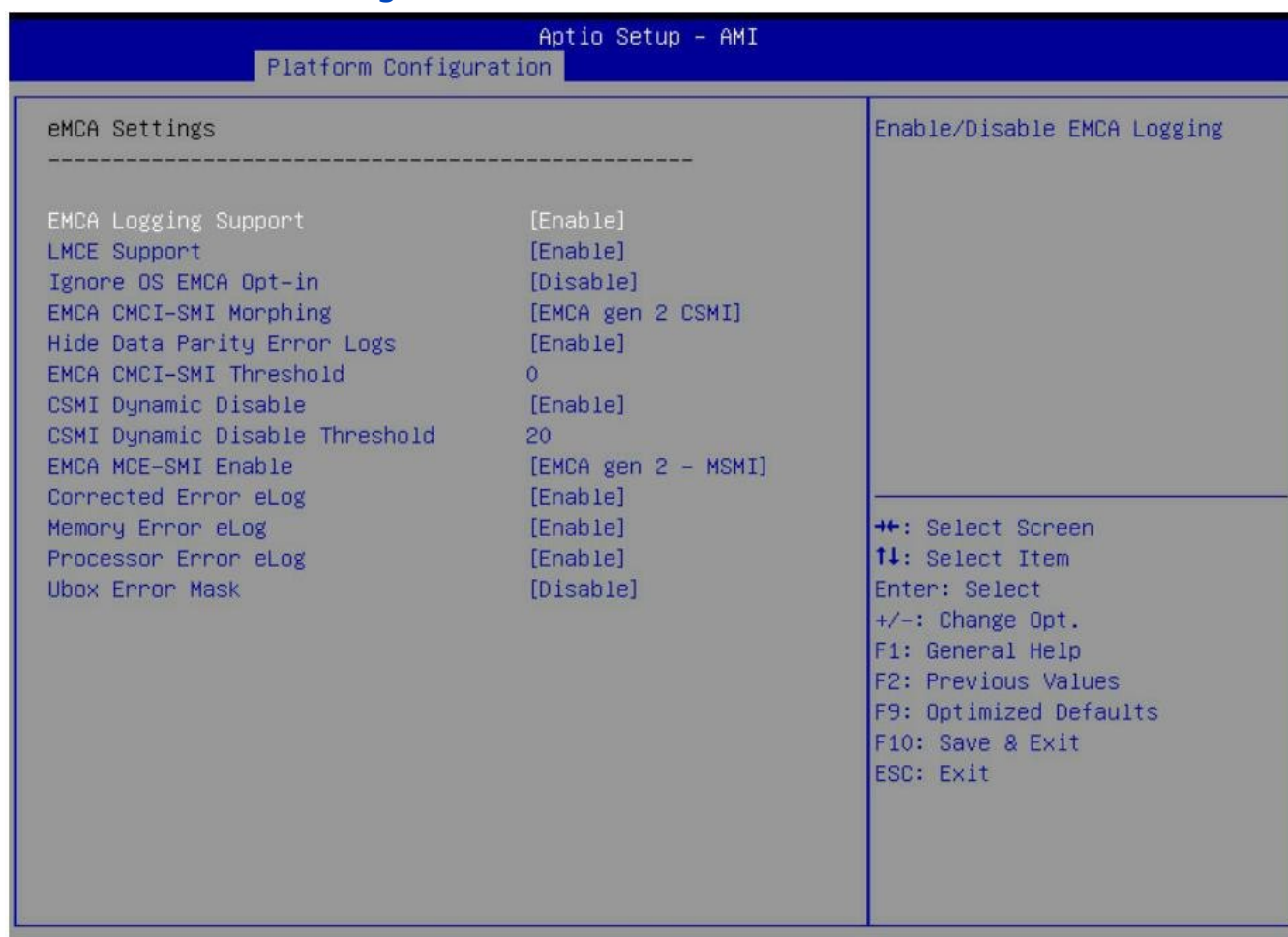


Рисунок 0-31 eMCA Settings

Настройка BIOS	Опции	Описание
eMCA Settings	eMCA Settings	Настройки eMCA
EMCA Logging Support	Enable/Disable	Включить/Отключить логирование EMCA.
LMCE Support	Enable/Disable	Включить/Отключить поддержку прошивки Local MCE.
Ignore OS EMCA Opt-in	Enable/Disable	Включить/Отключить игнорирование OS EMCA Opt-in и лога.
EMCA CMCI-SMIMorphing	Disable/EMCA gen 2 CSMI	Включить/Отключить EMCA CSMI.
EMCA MCE-SMIThreshold	0	Установить порог исправляемых ошибок для сигнализации CMCI-CSMI.
EMCA CMCI-SMI Enable	Disable/EMCA gen 2 MSMI	Включить/Отключить EMCA Uncorrected SMI для gen2.

Настройка BIOS	Опции	Описание
CSMI Dynamic Disable	Enable/Disable	[Enable] - BIOS отключает CSMI при достижении порога ошибок. [Disabled] - CSMI всегда включен.
Corrected Error eLog	Enable/Disable	Включить/Отключить eLog исправленных ошибок.
Memory Error eLog	Enable/Disable	Включить/Отключить eLog ошибок памяти.
Processor Error eLog	Enable/Disable	Включить/Отключить eLog ошибок процессора.
Ubox Error Mask	Enable/Disable	Маскировать генерацию SMI для ошибок Ubox.

Таблица 0-32 eMCA Settings

6.3.4.2. Whea Settings

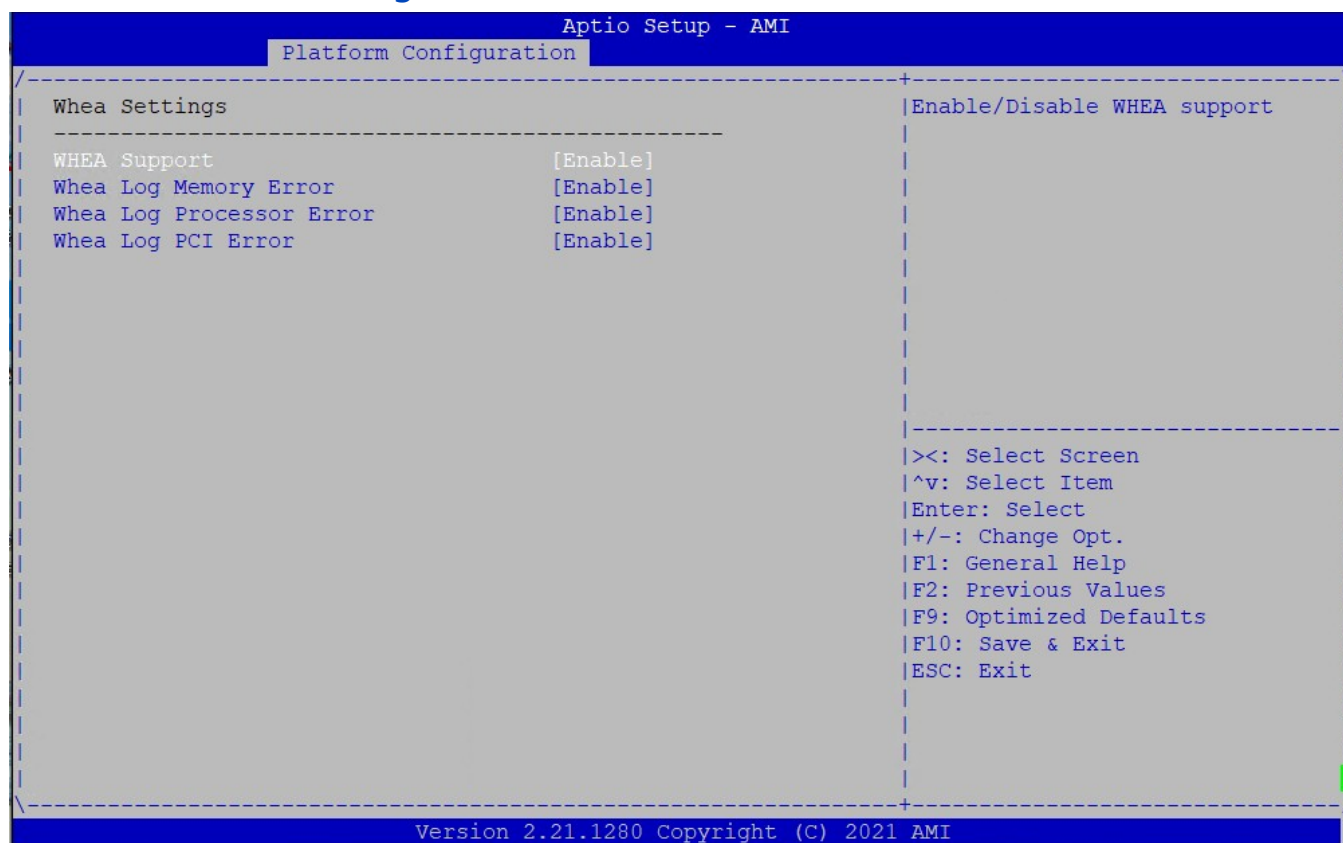


Рисунок 0-32 Whea Settings

Настройка BIOS	Опции	Описание
Whea Settings	Whea Settings	Настройки Whea
WHEA Support	Enable/Disable	Включить или отключить поддержку WHEA
WHEA Log Memory Error	Enable/Disable	Включить/Отключить Whea

Настройка BIOS	Опции	Описание
WHEA Log Processor Error	Enable/Disable	Log ошибок памяти. Включить/Отключить Whea Log ошибок процессора.
WHEA Log PCI Error	Enable/Disable	Включить/Отключить Whea Log ошибок PCI.

Таблица 0-33 Whea Settings

6.3.4.3. Error Injection Settings

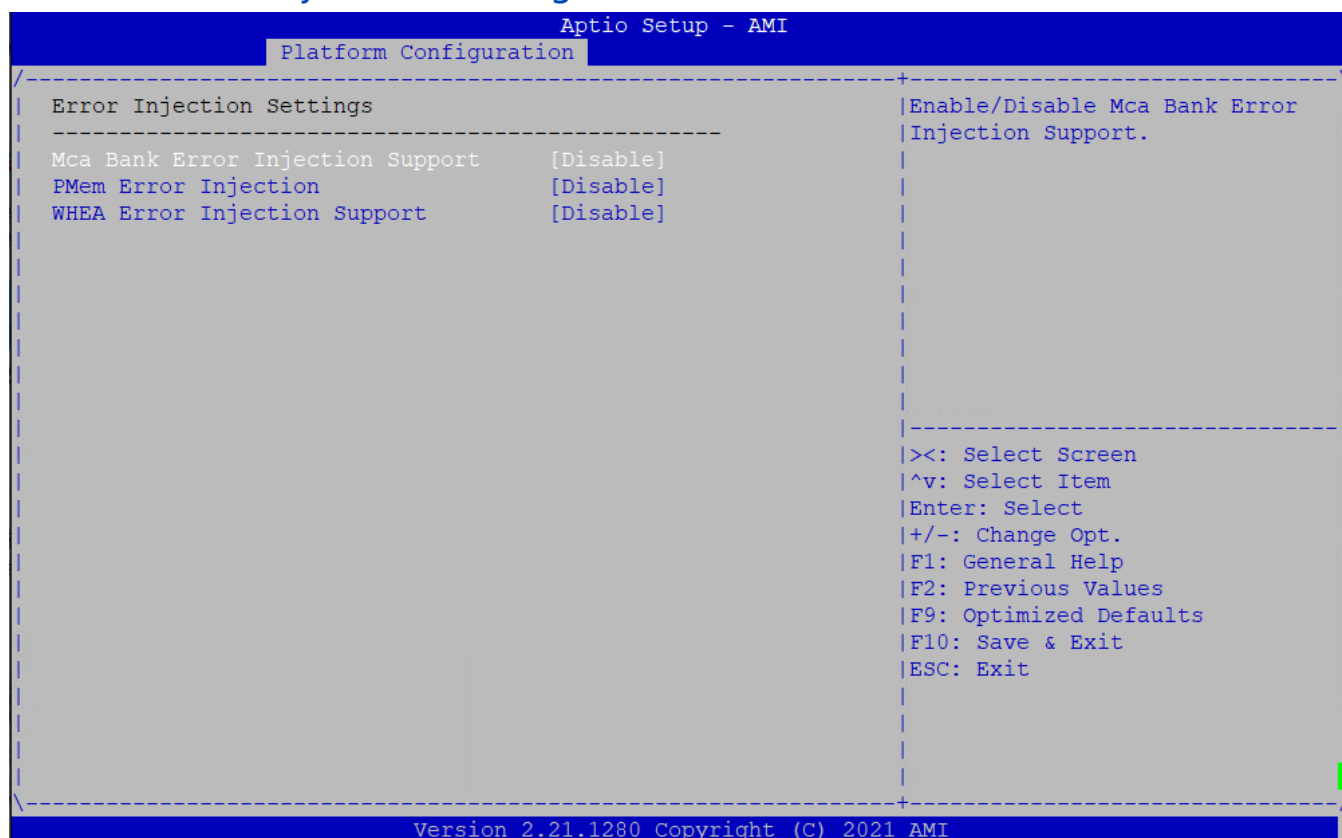


Рисунок 0-33 Error Injection Settings

Настройка BIOS	Опции	Описание
Error Injection Settings	Error Injection Settings	Настройки внедрения ошибок
Mca Bank Error Injection Support	Enable/Disable	Включить/Отключить Mca Bank Error Injection Support.
PMem Error Injection	Enable/Disable	Включить/Отключить PMem Error Injection.
WHEA Error Injection Support	Enable/Disable	Включить/Отключить WHEA Error Injection Support.

Таблица 0-34 Error Injection Settings

6.3.4.4. Memory Error Enabling

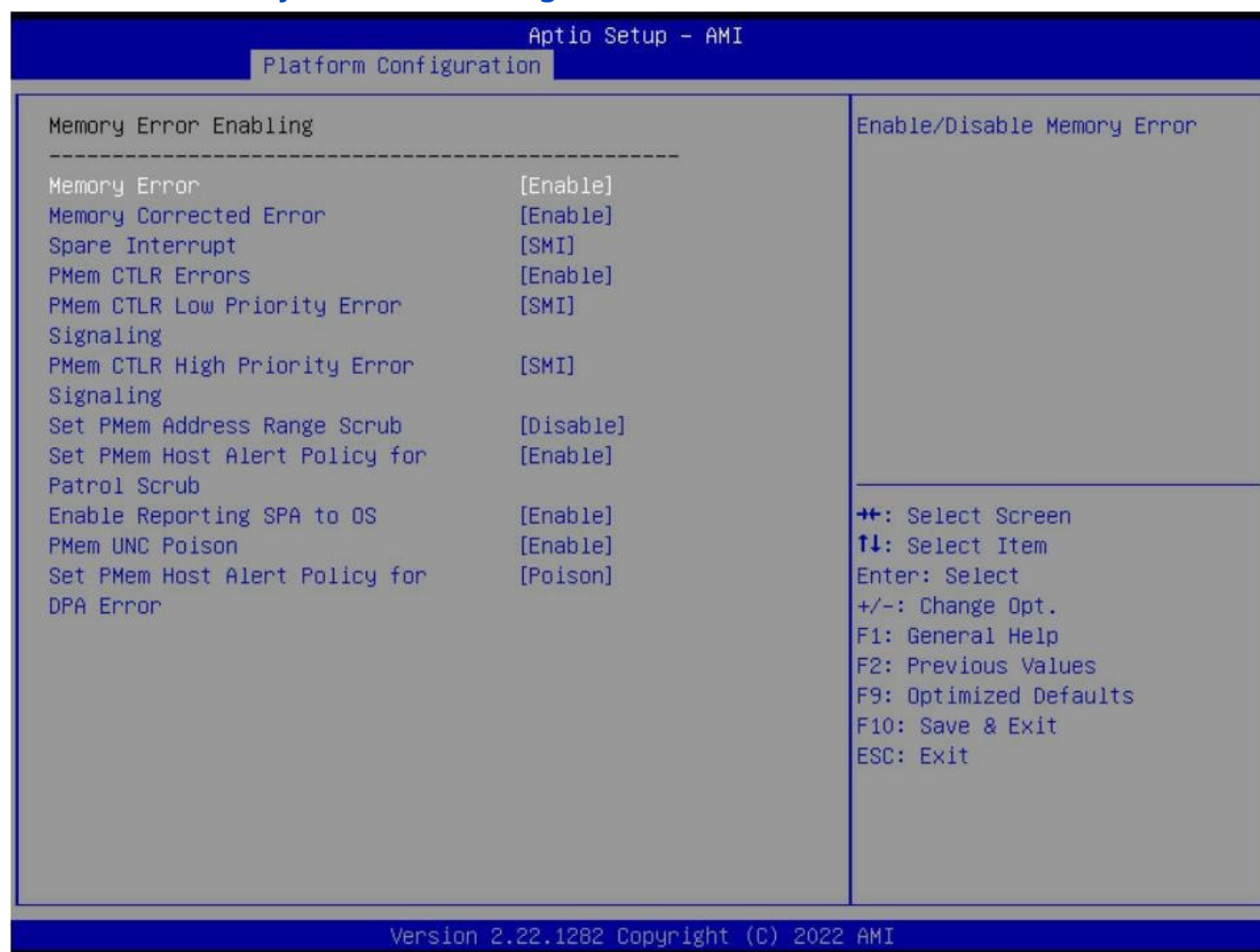


Рисунок 0-34 Memory Error Settings

Настройка BIOS	Опции	Описание
Memory Error Enabling	Memory Error Enabling	Включение ошибок памяти
Memory Error	Enable/Disable	Включить/Отключить ошибку памяти.
Memory Corrected Error	Enable/Disable	Включить/Отключить исправленную ошибку памяти.
Spare Interrupt	Disable / SMI / Error Pin/CMCI	Выбор резервного прерывания (Spare Interrupt).
PMem CTLR Errors	Enable/Disable	Включить/Отключить отчетность и логирование ошибок PMem CTLR
PMem CTLR Low Priority Error	Disable / SMI /ERR0# Pin	Выбор сигнализации для ошибок, отнесенных к низкому приоритету

Настройка BIOS	Опции	Описание
PMem CTLR High Priority Error	Disable / SMI /ERR0# Pin	Сигнализация ошибки высокого приоритета PMem CTLR
Set PMem Address Range Scrub	Enable/ Disable	Включить/Отключить очистку диапазона физических адресов PMem DIMM (Scrub).
Set PMem Host Alert Policy for Patrol Scrub	Enable /Disable	Включить/Отключить сигнализацию прерывания DDRT при получении неисправимой ошибки для PMem Patrol Scrub.
Enable Reporting SPA to OS	Enable/ Disable	Включить отчетность SPA для ОС (Отключать только для валидации восстановления MCE).
PMem UNC Poison	Enable /Disable	Включить PMem UNC Poison
Set PMem Host Alert Policy for DPA Error	Poison / Viral	Настройка сигнализации Poison или Viral при получении ошибки физического адреса DIMM.

Таблица 0-35 Memory Error Settings

6.3.4.5. IIO Error Enabling

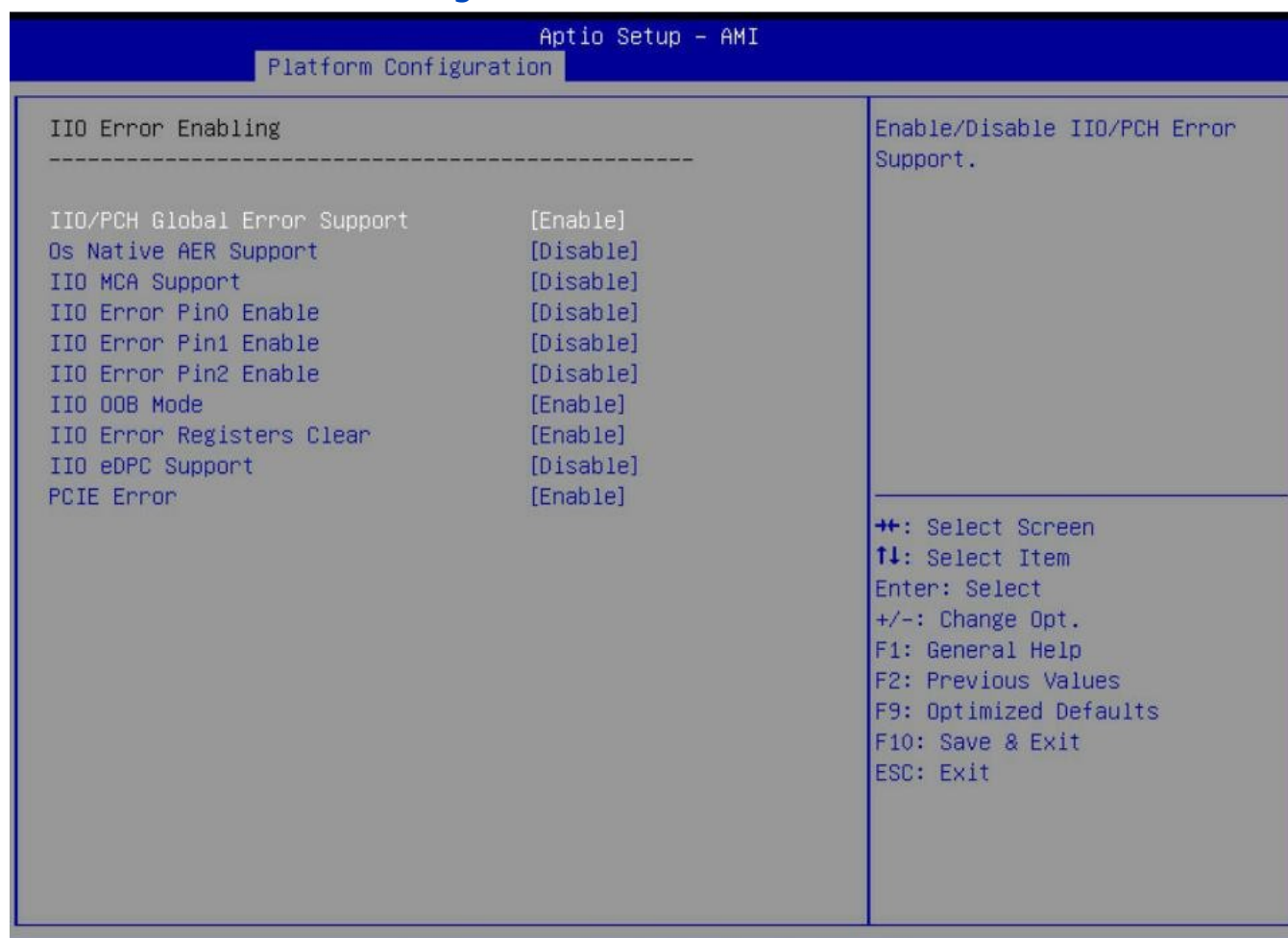


Рисунок 0-35 IIO Error Enabling

Настройка BIOS	Опции	Описание
IIO Error Enabling	IIO Error Enabling	Включение ошибок IIO
IIO/PCH Global Error Support	Enable/Disable	Включить/Отключить поддержку глобальных ошибок IIO/PCH.
Os Native AER Support	Enable/Disable	Выбор FFM или OS native для обработки ошибок AER. Если выбрано OS native, BIOS также инициализирует FFM до рукопожатия, что зависит от возможностей ОС.
IIO MCA Support	Enable/Disable	Включить/Отключить поддержку IIO MCA.
IIO Error Pin0 Enable	Enable/Disable	Включить/Отключить IIO Error Pin0
IIO OOB Mode	Enable/Disable	Включить/Отключить генерацию системных

Настройка BIOS	Опции	Описание
		событий, когда Error Pin включен.
IIO Error Registers Clear	Enable/Disable	Включить/Отключить очистку регистров ошибок IIO
IIO eDPC Support	Disable/On Fatal Error/On Fatal and Non-Fatal Errors	Включить/Отключить поддержку IIO eDPC
PCIe Error	Enable/Disable	Включить/Отключить ошибку PCIe.

Таблица 0-36 IIO Error Enabling

6.3.4.6. PCIe Error Enabling

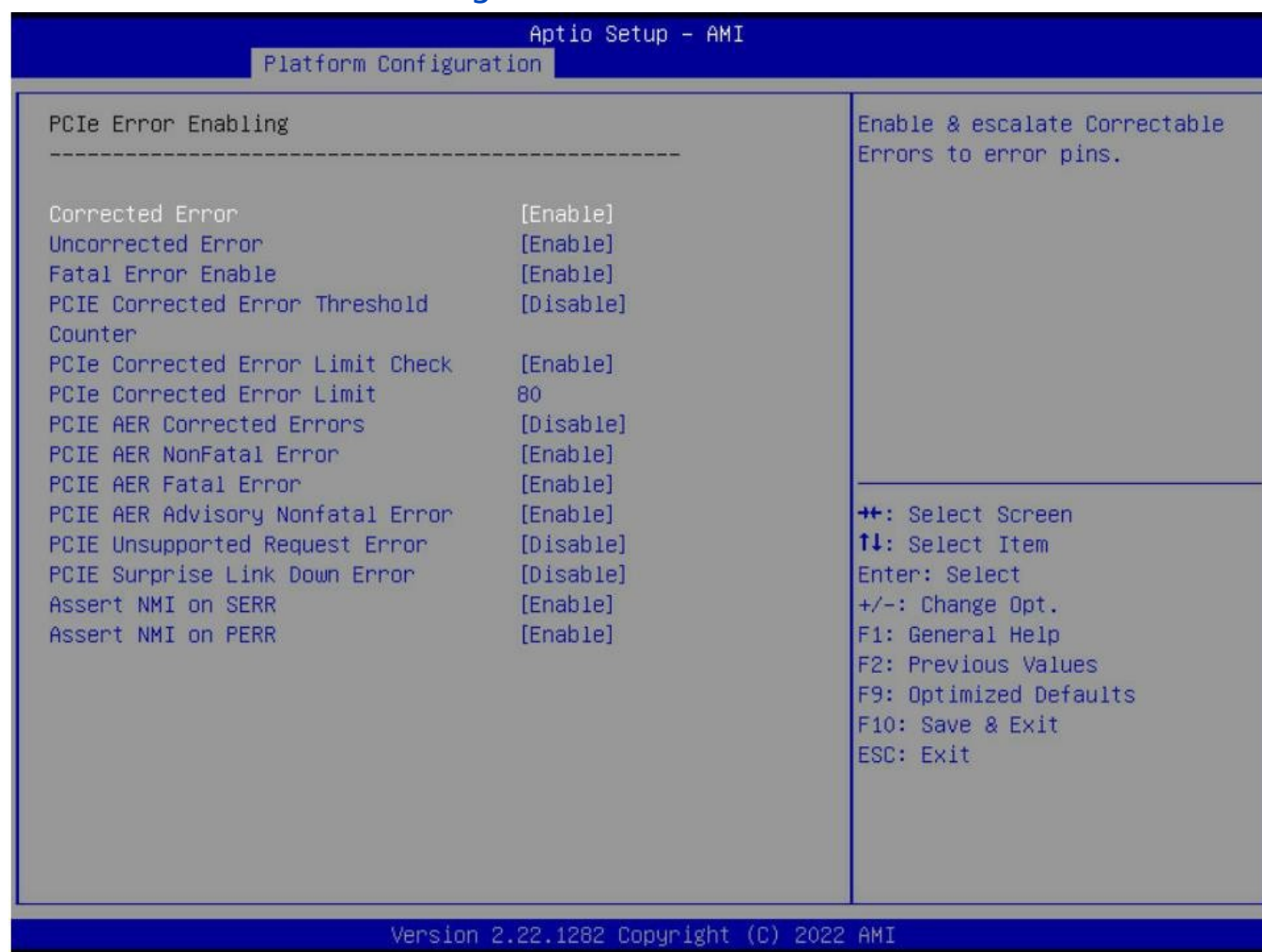


Рисунок 0-36 PCIe Error Enabling

Настройка BIOS	Опции	Описание
PCIe Error Enabling	PCIe Error Enabling	Включение ошибок PCIe
Corrected Error	Enable / Disable	Включить и передать

Настройка BIOS	Опции	Описание
		исправляемые ошибки на выводы ошибок.
Uncorrected Error	Enable/Disable	Включить и передать неисправимые/восстанавливаемые ошибки на выводы ошибок.
Fatal Error Enable	Enable/Disable	Включить и передать фатальные ошибки на выводы ошибок.
PCIe Corrected Error Threshold Counter	Enable/Disable	Включить/Отключить счетчик исправленных ошибок PCIe
PCIe Corrected Error Limit Check	Enable/Disable	Включить/Отключить функцию запрета сообщения об исправленных ошибках PCIe для устройства, если они превышают заданный лимит.
PCIe Corrected Error Limit	80	Лимит исправленных ошибок PCIe
PCIe AER Corrected Errors	Enable/Disable	Включить/Отключить исправленные ошибки PCIe AER.
PCIe AER Nonfatal Error	Enable/Disable	Включить/Отключить нефатальные ошибки PCIe AER.
PCIe AER Fatal Error	Enable/Disable	Включить/Отключить фатальные ошибки PCIe AER
PCIe AER Advisory Nonfatal Error	Enable/Disable	Включить/Отключить консультативные нефатальные ошибки PCIe AER.
PCIe Unsupported Request Error	Enable/Disable	Включить/Отключить ошибку неподдерживаемого запроса PCIe
PCIe Surprise Link Down Error	Enable/Disable	Включить/Отключить ошибку неожиданного разрыва связи PCIe (Surprise Link Down)
—	—	—
Assert NMI on SERR	Enable/Disable	При SERR генерировать NMI и регистрировать ошибку.Примечание: Опция [Enabled] должна быть выбрана для Assert NMI on SERR, чтобы опция Assert NMI on PERR была видимой.
Assert NMI on PERR	Enable/Disable	При PERR генерировать NMI и регистрировать

Настройка BIOS	Опции	Описание
		ошибку.Примечание: Эта опция активна только если выбрана опция Assert NMI on SERR [Enabled].

Таблица 0-37 PCIe Error Enabling

6.3.4.7. Error Control Setting

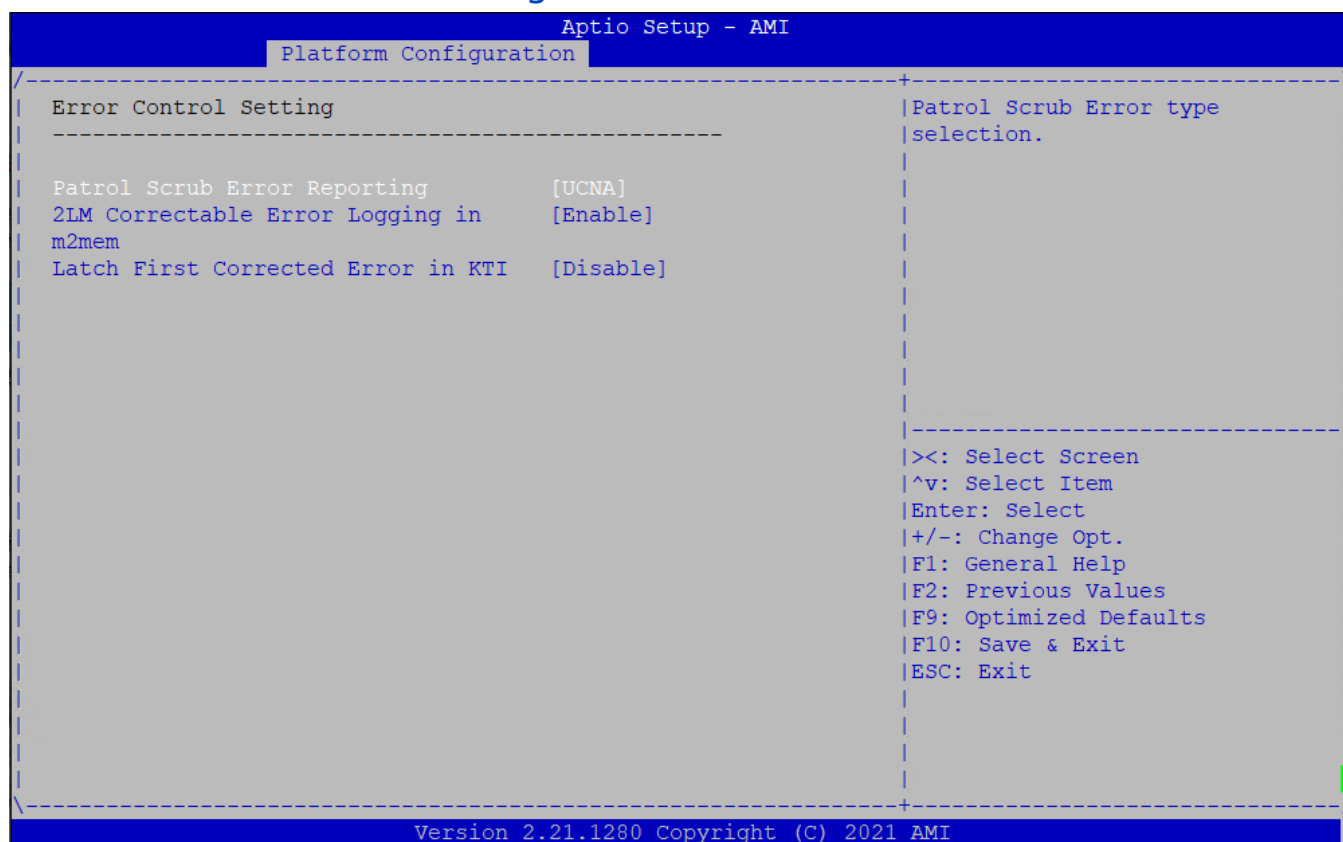


Рисунок 0-37 Error Control Setting

Настройка BIOS	Опции	Описание
Error Control Setting	Error Control Setting	Настройка контроля ошибок
Patrol Scrub Error Reporting	UCNA	Выбор типа сообщения об ошибке Patrol Scrub.
2LM Correctable Error Logging in m2mem	Enable/Disable	Включить или отключить логирование исправляемых ошибок 2LM в m2mem.
Latch First Corrected Error in KTI	Enable/Disable	Включить или отключить фиксацию первой исправленной ошибки в KTI.

Таблица 0-38 Error Control Setting

6.0.0.0.1. Displays system information. (Such as BIOS Information, Memory Information, System Language, System Date, System Time, Access level).

Advanced:

6.0.0.0.2. Use this menu to control multiple components.

*Platform Configuration:***

6.0.0.0.3. Control PCH, ME Subsystem and Runtime Error.

*Socket Configuration:**** **Control Processor, Memory, IIO and Power Management.*

Server Mgmt:**

6.0.0.0.4. Configure BMC components. (Such system event logs, BMC network).

:

6.0.0.0.5. Set Administrator Password and User Password.

Boot:

6.0.0.0.6. Set boot options such as Boot Configuration, Boot Option Priorities.

Save system setup configurations and Boot override.

Aptio Setup - AMI		
Advanced		
USB Configuration		Enables 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.
USB Module Version	26	
USB Controllers:		
1 XHCI		
USB Devices:		
1 Keyboard, 1 Mouse, 1 Hub		
Legacy USB Support	[Enabled]	
XHCI Hand-off	[Enabled]	
USB Mass Storage Driver Support	[Enabled]	
Port 60/64 Emulation	[Enabled]	
USB hardware delays and time-outs:		
USB transfer time-out	[20 sec]	
Device reset time-out	[20 sec]	
Device power-up delay	[Auto]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1280 Copyright (C) 2021 AMI		

The following sections completely describe the configuration options found in the menu items at the top of the BIOS screen and listed above.

6.4. Socket Configuration

Используйте меню **Socket Configuration** для настройки устройств UPI, Memory, IIO через следующие подменю.

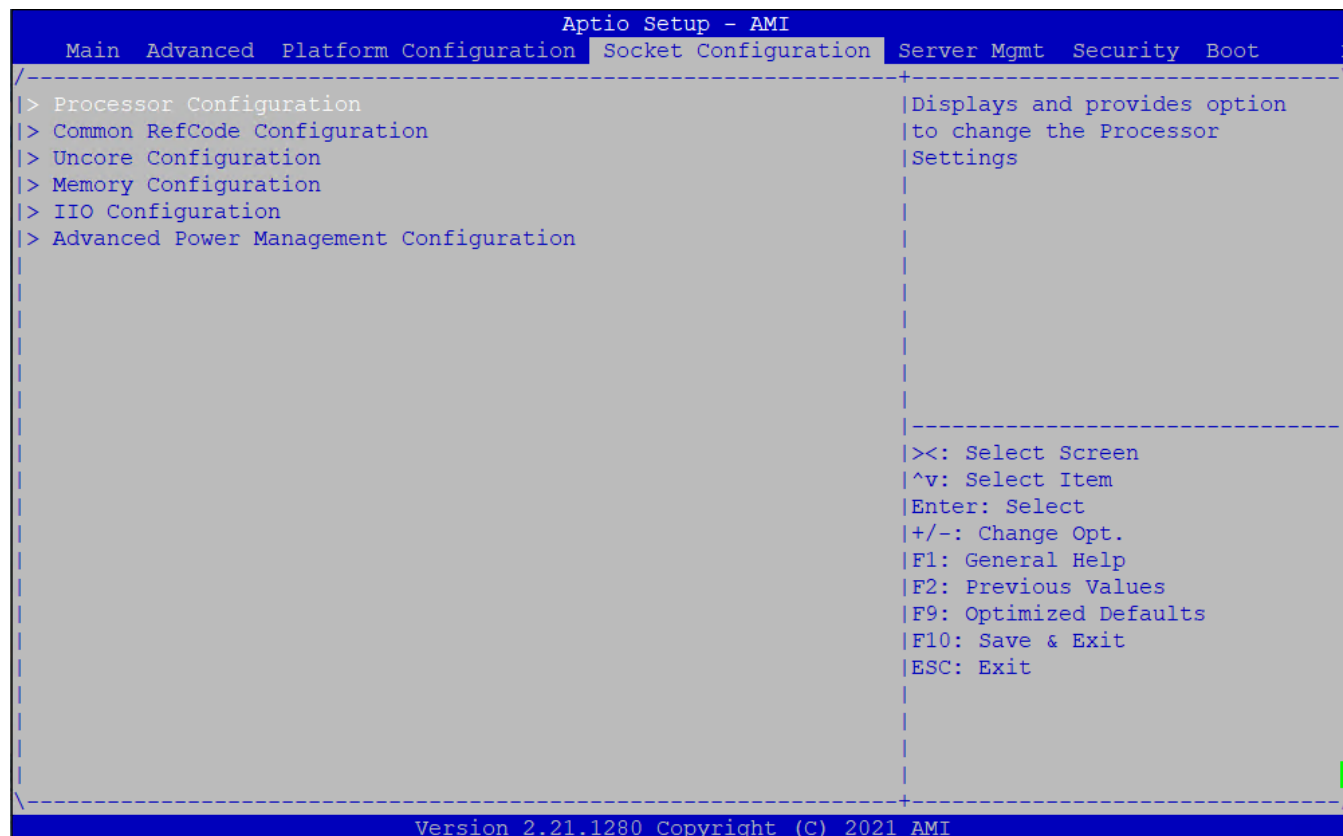


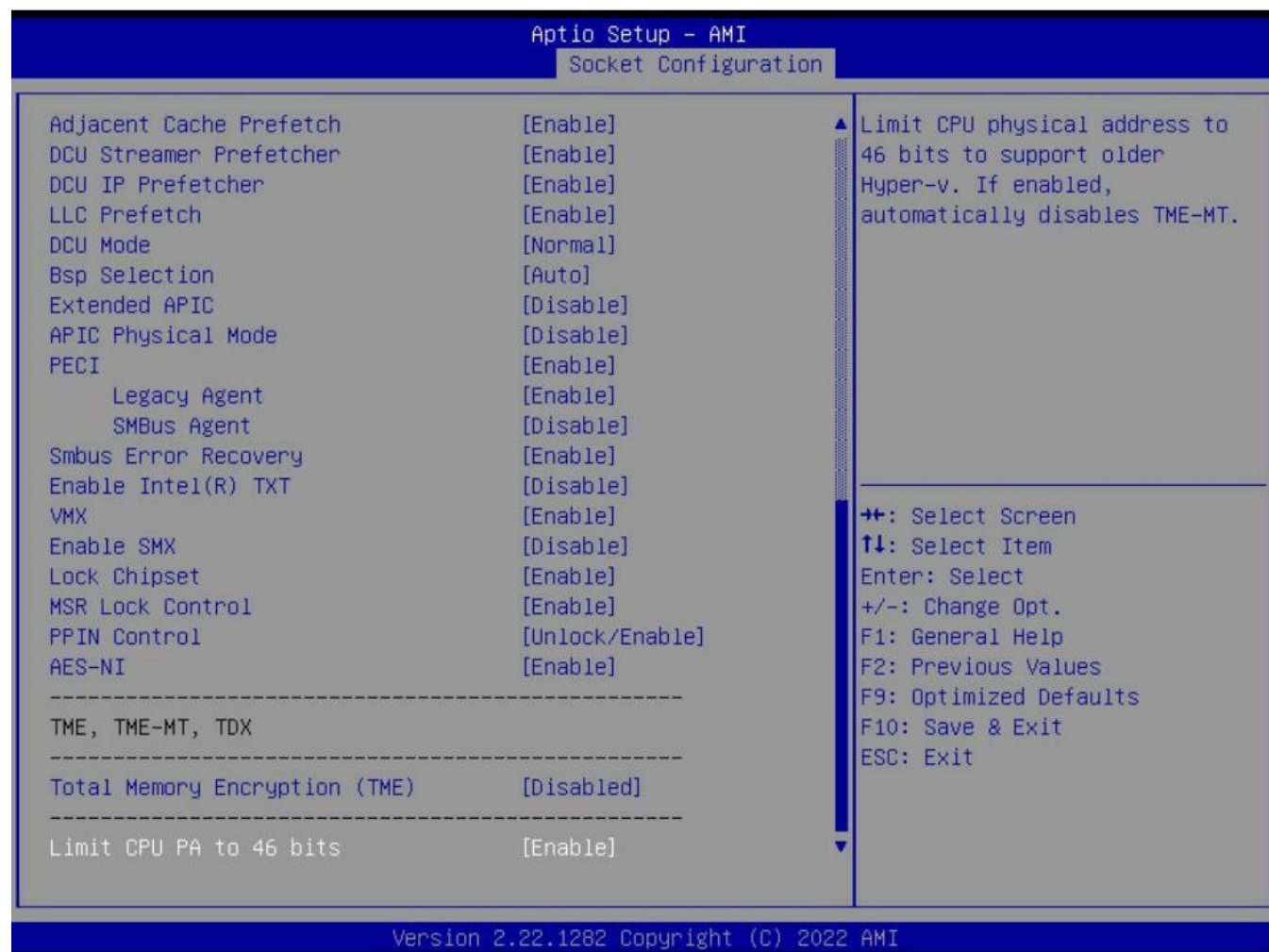
Рисунок 0-38: Socket Configuration

Настройка BIOS	Опции	Описание
Processor Configuration	См. подробнее	Отображает и предоставляет опцию для изменения настроек процессора.
Common RefCode Configuration	См. подробнее	Отображает и предоставляет опцию для изменения общих настроек RefCode
Uncore Configuration	См. подробнее	Отображает и предоставляет опцию для изменения настроек Uncore.
Memory Configuration	См. подробнее	Отображает и предоставляет опцию для изменения настроек памяти.
IIO Configuration	См. подробнее	Отображает и предоставляет опцию для изменения настроек IIO.

Настройка BIOS	Опции	Описание
Advanced Power Management Configuration	См. подробнее	Отображает и предоставляет опцию для изменения настроек управления питанием.

Таблица 0-39 Socket Configuration

6.4.1. Processor Configuration



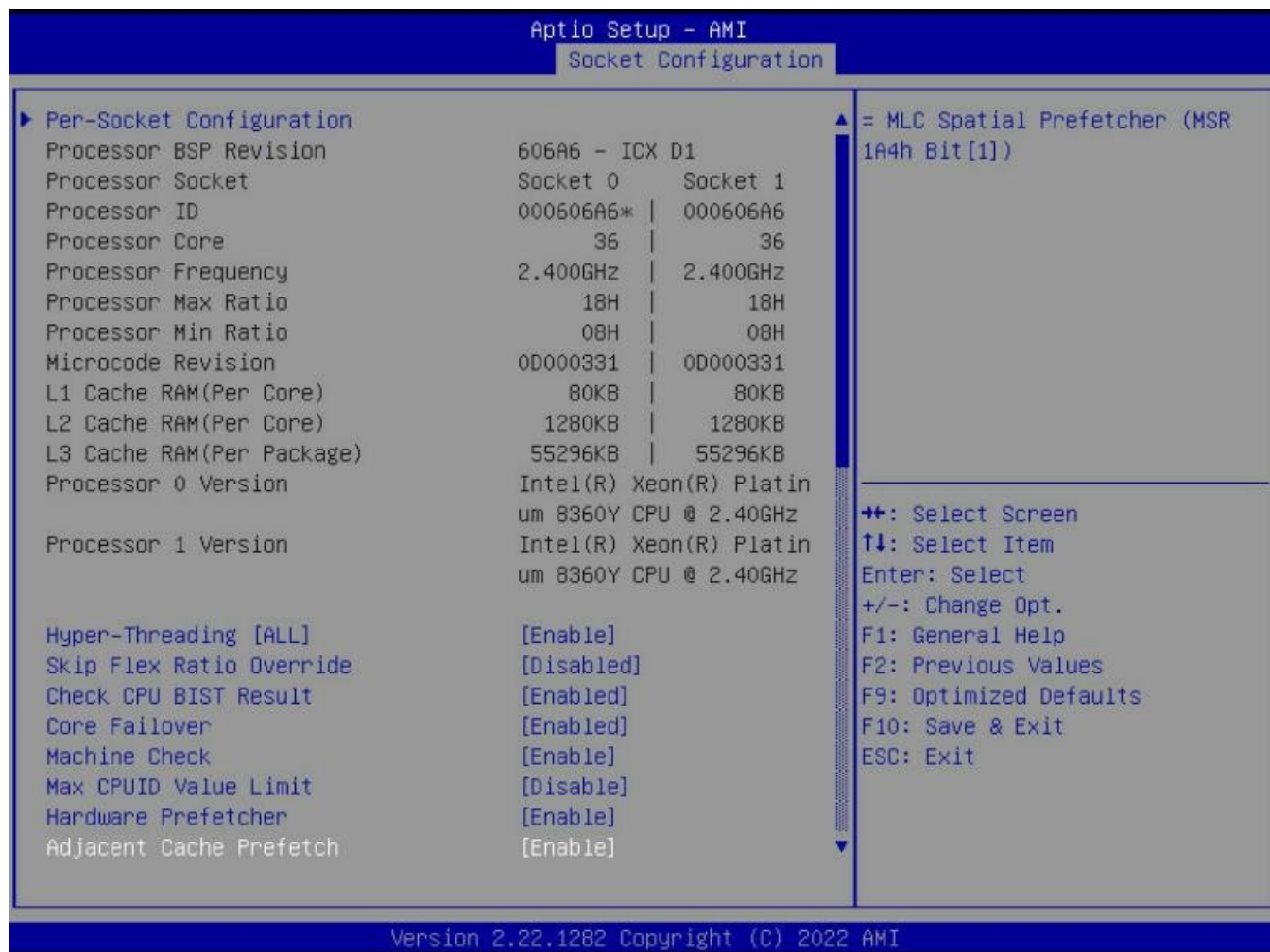


Рисунок 0-39 Socket Configuration

Настройка BIOS	Опции	Описание
Processor Configuration	Processor Configuration	Конфигурация процессора
Per-Socket Configuration	См. подробнее.	Изменить настройки для каждого сокета.
Processor BSP Revision	Read Only	Ревизия BSP
Processor Socket	Read Only	Сокет процессора
Processor ID	Read Only	ID процессора
Processor Core	Read Only	
Processor Frequency	Read Only	Частота процессора
Processor Max Ratio	Read Only	Максимальный коэффициент процессора
Processor Min Ratio	Read Only	Минимальный коэффициент процессора
Microcode Revision	Read Only	Ревизия микрокода
L1 Cache RAM	Read Only	Размер кэш-памяти L1
L2 Cache RAM	Read Only	Размер кэш-памяти L2

Настройка BIOS	Опции	Описание
L3 Cache RAM	Read Only	Размер кэш-памяти L3
Processor 0 Version	Read Only	Версия процессора 0
Processor 1 Version	Read Only	Версия процессора 1
Hyper-Threading [ALL]	Enable/Disable	Включает Hyper Threading (программный метод включения/отключения потоков логического процессора).
Skip Flex Ratio Override	Enable/Disable	Пропустить переопределения Flex Ratio для использования значений Flex Ratio по умолчанию при включении питания. В многопроцессорных системах это позволит использовать смешанные ограничения flex ratio.
Check CPU BIST Result	Enable/Disable	Отключить сбойное ядро BIST при включении, иначе игнорировать результат BIST.
Core Failover	Enable/Disable	Включить резервное ядро(а) вместо ядра(ер), не прошедших BIST.
Machine Check	Enable/Disable	Включить или отключить Machine Check.
Max CPUID Value Limit	Enable/Disable	Это должно быть включено для загрузки устаревших ОС, которые не поддерживают процессоры с расширенными функциями CPUID.
Hardware Prefetcher	Enable/Disable	= MLC Streamer Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefetcher	Enable/Disable	
DCU Streamer Prefetcher	Enable/Disable	
DCU IP Prefetcher	Enable/Disable	
LLC Prefetch	Enable/Disable	
DCU Mode	Normal/Mirror-Mode	
Bsp Selection	Auto/Socket 0/Socket 1/Socket 2/Socket 3/Socket 4/Socket 5/Socket 6/Socket 7	
Extended APIC	Enable/Disable	Включить/отключить расширенный APIC up port Примечание: Это автоматически включит VT-d, если включен x2APIC
APIC Physical Mode	Enable/Disable	
PECI	Enable/Disable	Включить бит доверия Peci

Настройка BIOS	Опции	Описание
Legacy Agent	Enable/Disable	Включить бит доверия устаревшего агента PECI.
SMBus Agent	Enable/Disable	Включить бит доверия агента SMBus PECI.
Smbus Error Recovery	Enable/Disable	Включить или отключить восстановление ошибок Smbus
Enable Intel(R) TXT	Enable/Disable	Включает Intel(R) TXT.
VMX	Enable/Disable	Включает технологию Vanderpool, вступает в силу после перезагрузки.
Enable SMX	Enable/Disable	Включает расширения Safer Mode Extensions.
Lock Chipset	Enable/Disable	Блокировать или разблокировать чипсет
MSR Lock Control	Enable/Disable	Enable - MSR 3Ah и CSR 80h будут заблокированы. Для снятия битов блокировки требуется сброс Power Good.
PPIN Control	Lock/Disable Unlock/Enable	Разблокировать и включить/отключить управление PPIN.
AES-NI	Enable/Disable	Включить/отключить поддержку AES-NI.
Total Memory Encryption (TME)	Enable/Disable	Включить/отключить полное шифрование памяти (TME)
Limit CPU PA to 46 bits	Enable/Disable	Ограничить физический адрес процессора до 46 бит для поддержки старых Hyper-v. Если включено, автоматически отключает TME-MT.

Таблица 0-40 Socket Configuration

6.4.1.1. Per-Socket Configuration



Рисунок 0-40 Per-socket Configuration

Настройка BIOS	Опции	Описание
CPU Socket 0/1 Configuration	CPU Socket 0/1 Configuration	Конфигурация сокета процессора 0/1
CPU Socket 0 Configuration	См. подробнее.	Количество ядер для включения. 0 означает все ядра. %d ядер доступно.
CPU Socket 1 Configuration	См. подробнее.	

Таблица 0-41 Per-socket Configuration

6.4.1.2. CPU Socket 0 Configuration

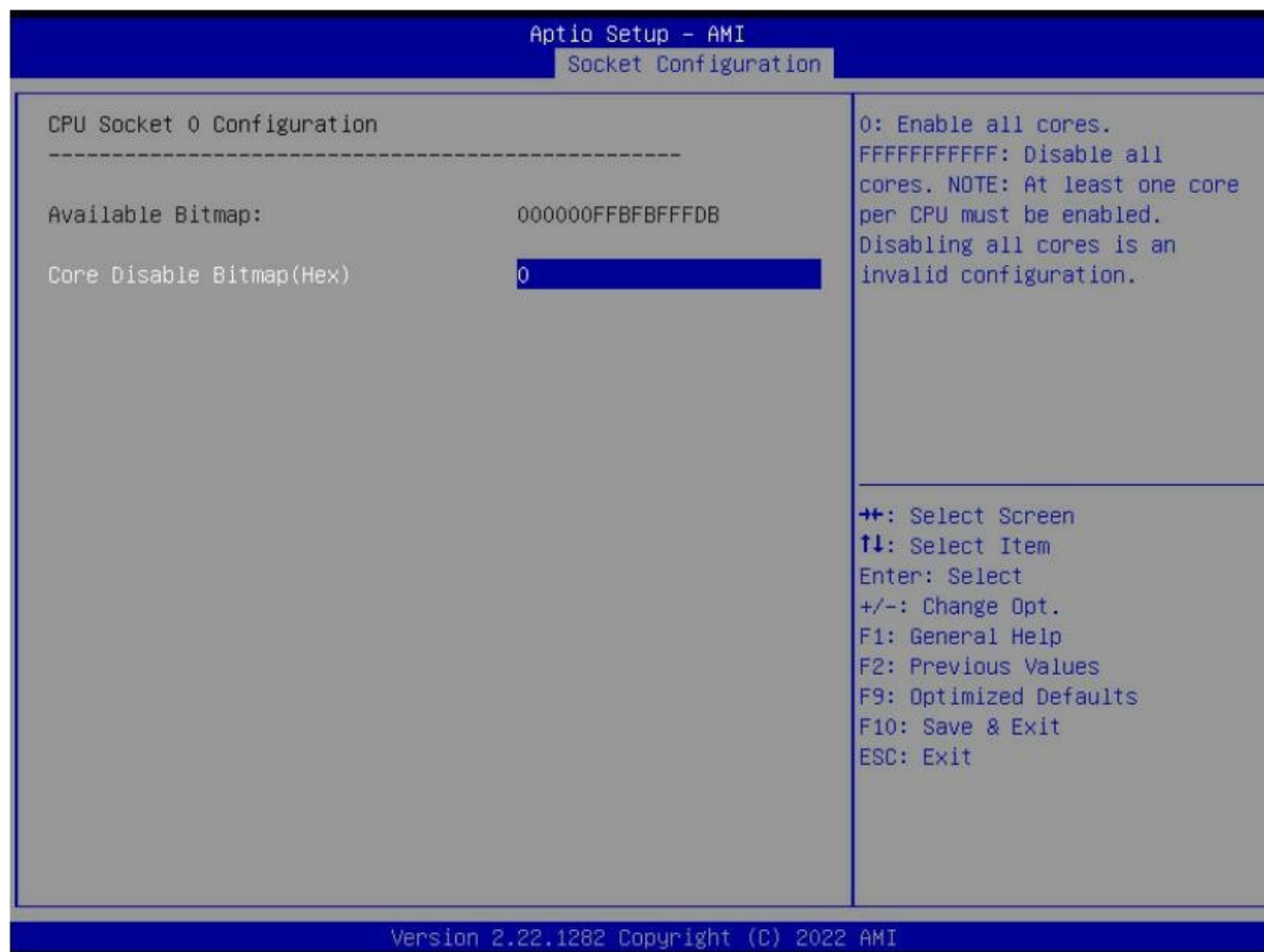


Рисунок 0-41 CPU Socket 0 Configuration

Настройка BIOS	Опции	Описание
CPU Socket 0 Configuration	CPU Socket 0 Configuration	Конфигурация сокета процессора 0
Available Bitmap:	000000FFBFBFFFDDB	Доступная битовая карта
Core Disable Bitmap (Hex)	0	0: Включить все ядра. FFFFFFFF: Отключить все ядра. ПРИМЕЧАНИЕ: Как минимум одно ядро на CPU должно быть включено. Отключение всех ядер является недопустимой конфигурацией.

Таблица 0-42 CPU Socket 0 Configuration

6.4.2. Common RefCode Configuration

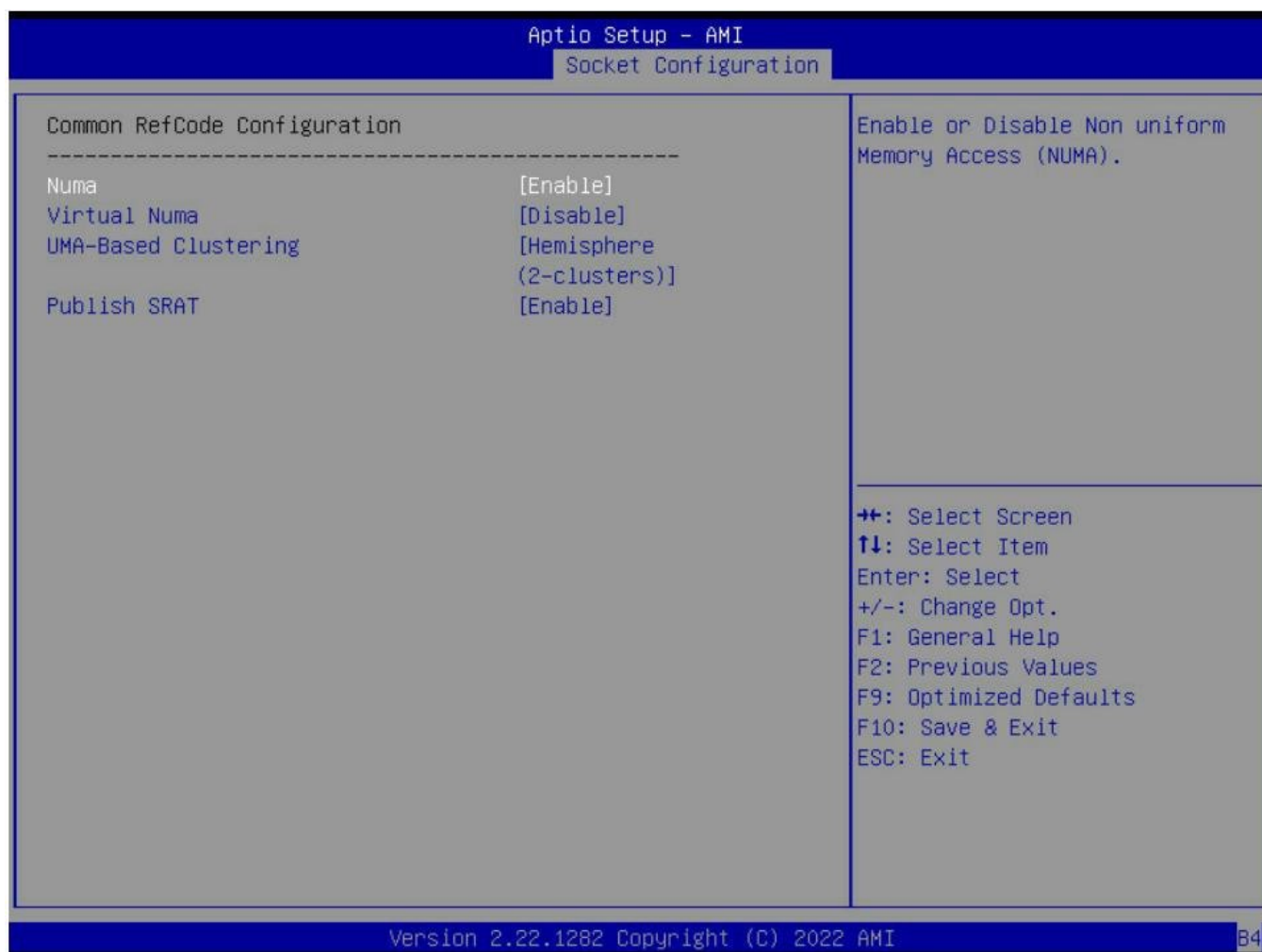


Рисунок 0-42 Common RefCode Configuration

Настройка BIOS	Опции	Описание
Common RefCode Configuration	Common RefCode Configuration	Общая конфигурация RefCode
Numa	Enable/Disable	Включить или отключить Non uniform Memory Access (NUMA).
Virtual Numa	Enable/Disable	Разделить физические узлы NUMA на узлы виртуальной NUMA равного размера в таблице ACPI. Это может улучшить производительность Windows на процессорах с более чем 64 логическими процессорами.
UMA-Based Clustering	Disable(All2All)/Hemisphere(2-clusters)	Опции кластеризации на основе UMA включают Disable (ALL2ALL), Hemisphere (2 кластера). Эти опции

Настройка BIOS	Опции	Описание
		действительны только когда отключен SNC. Если SNC включен, кластеризация на основе UMA автоматически отключается BIOS.
Publish SRAT	Enable/Disable	Опубликовать таблицу SRAT ACPI для ОС.

Таблица 0-43 Common RefCode Configuration

6.4.3. Uncore Configuration

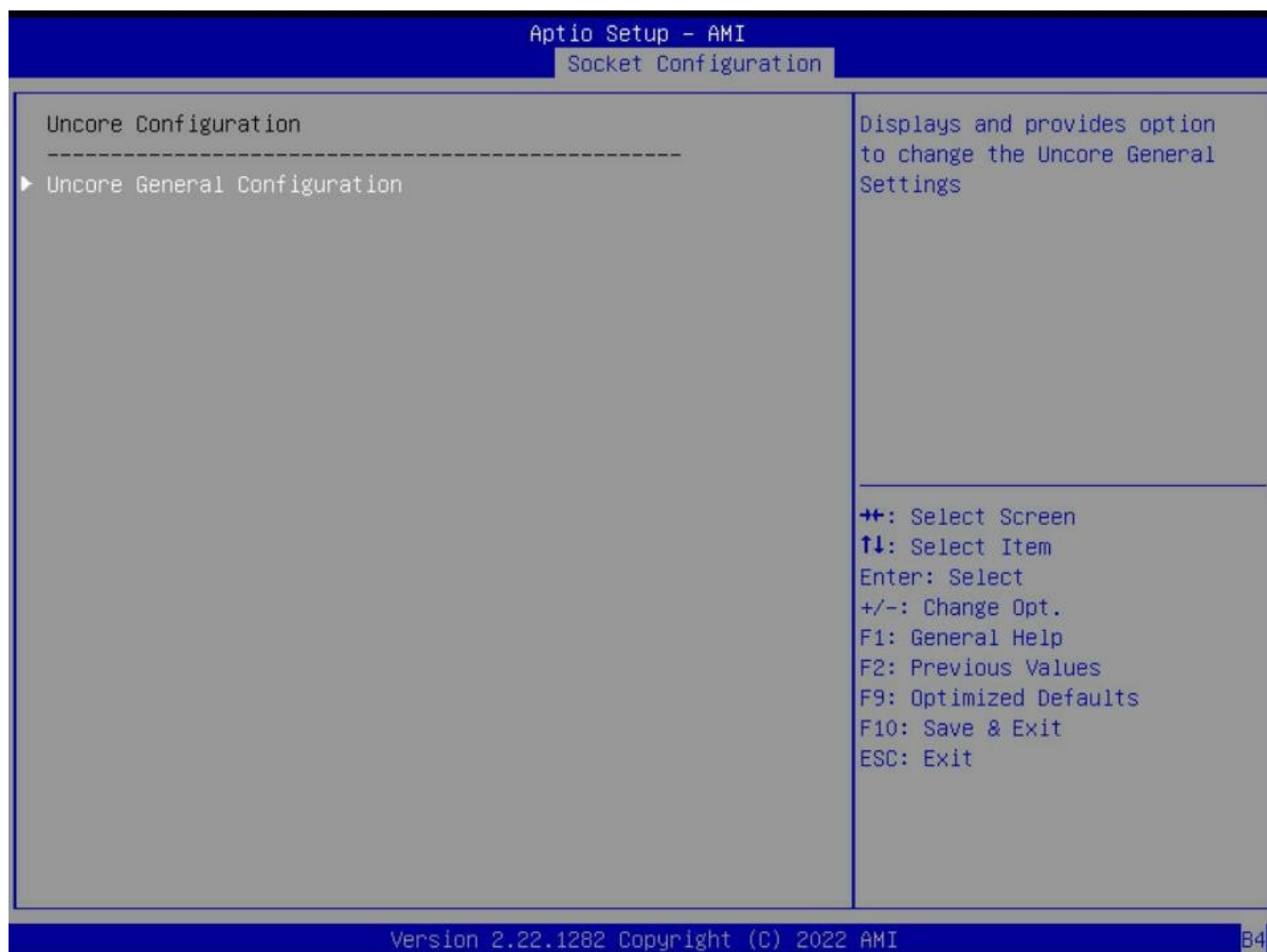


Рисунок 0-45 Uncore Configuration

Настройка BIOS	Опции	Описание
Uncore Configuration	Uncore Configuration	Конфигурация Uncore
Uncore General Configuration	См. подробнее.	Отображает и предоставляет опцию для изменения общих настроек

Настройка BIOS	Опции	Описание
		Uncore.

Таблица 0-45 Uncore Configuration

6.4.4. Uncore General Configuration

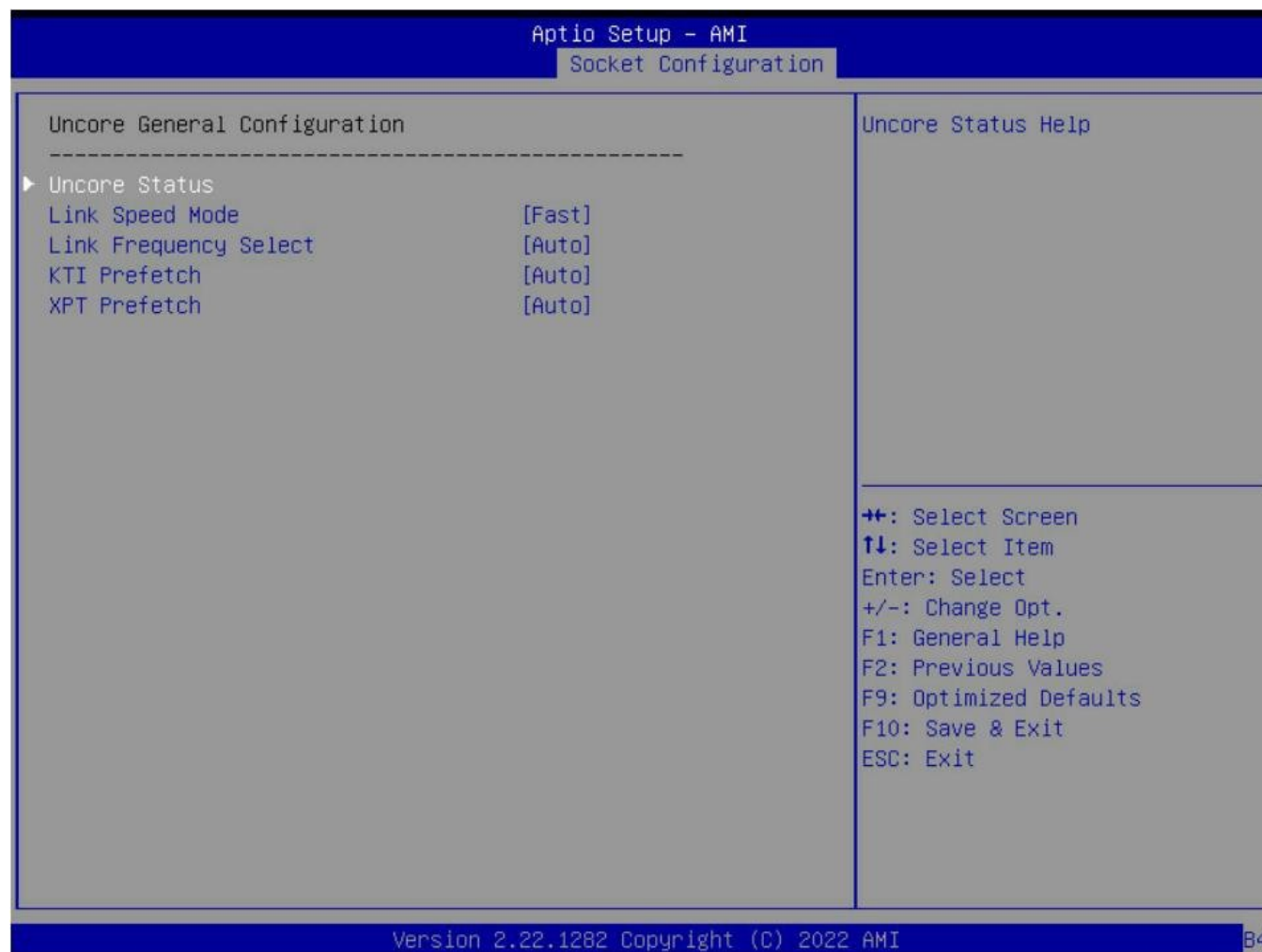


Рисунок 0-46 Uncore General Configuration

Настройка BIOS	Опции	Описание
Uncore General Configuration	Uncore General Configuration	Общая конфигурация Uncore
Uncore Status	См. подробнее.	Uncore Status Help
Link Speed Mode	Slow/Fast	Выберите скорость канала UPI: POR speed (Fast) или default speed (Slow)
Link Frequency Select	9.6GT/s /10.4GT/s/11.2GT/s /Auto /Use Per Link Setting	Позволяет выбрать частоту канала UPI
KTI Prefetch	Disable/Enable /Auto	KTI Prefetch

Настройка BIOS	Опции	Описание
XPT Prefetch	Disable/Enable /Auto	XPT Prefetch

Таблица 0-46 Uncore General Configuration

6.4.4.1. Uncore Status

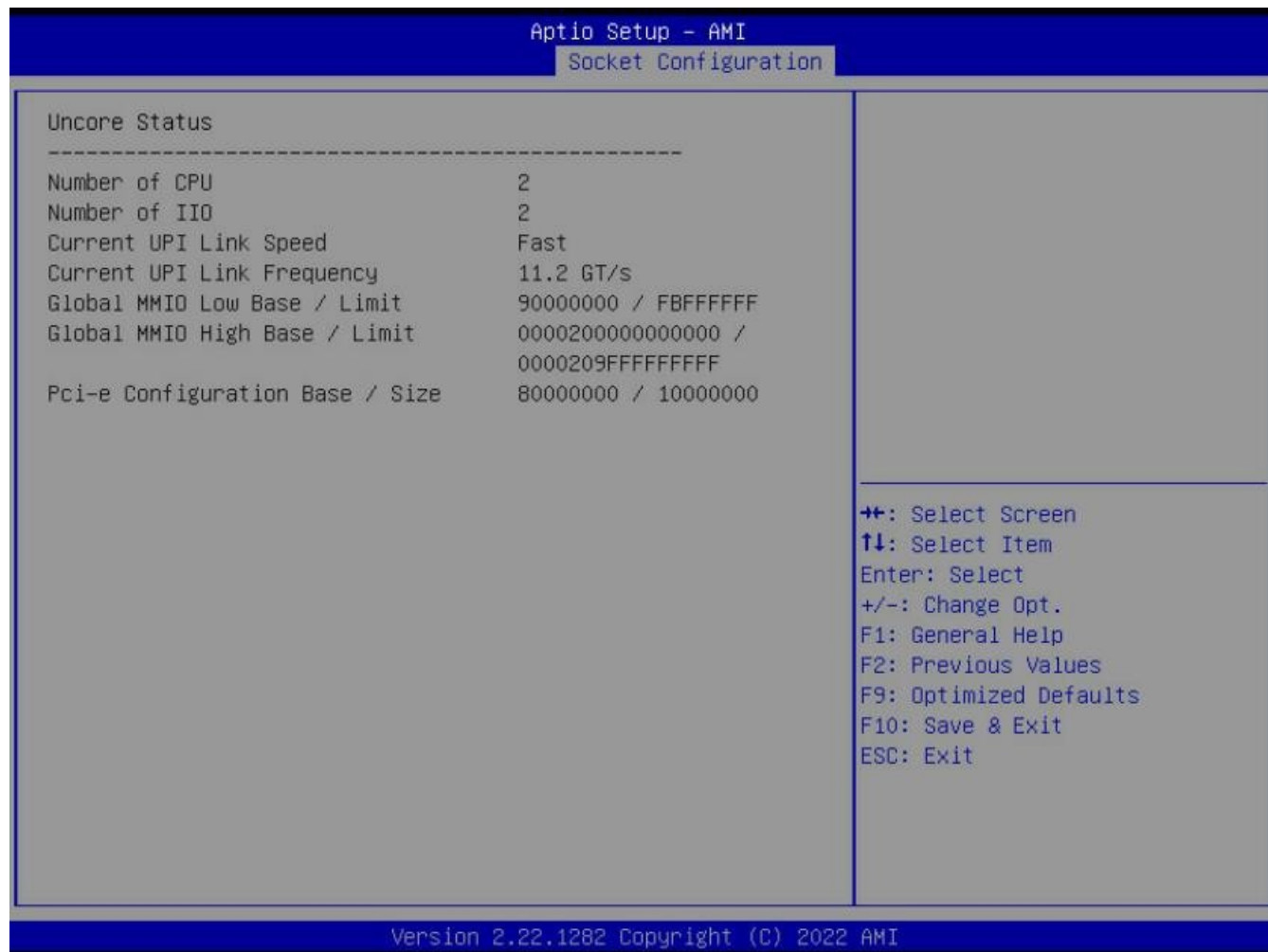


Рисунок 0-47 Uncore Status

Настройка BIOS	Опции	Описание
Uncore Status	Uncore Status	Статус Uncore
Number of CPU	Read Only	Справка о статусе Uncore
Number of IIO		
Current UPI Link Speed		
Current UPI Link Frequency		
Global MMIO Low Base / Limit		
Global MMIO High Base / Limit		
PCle Configuration Base / Size		

Таблица 0-47 Uncore Status

6.4.5. Memory Configuration

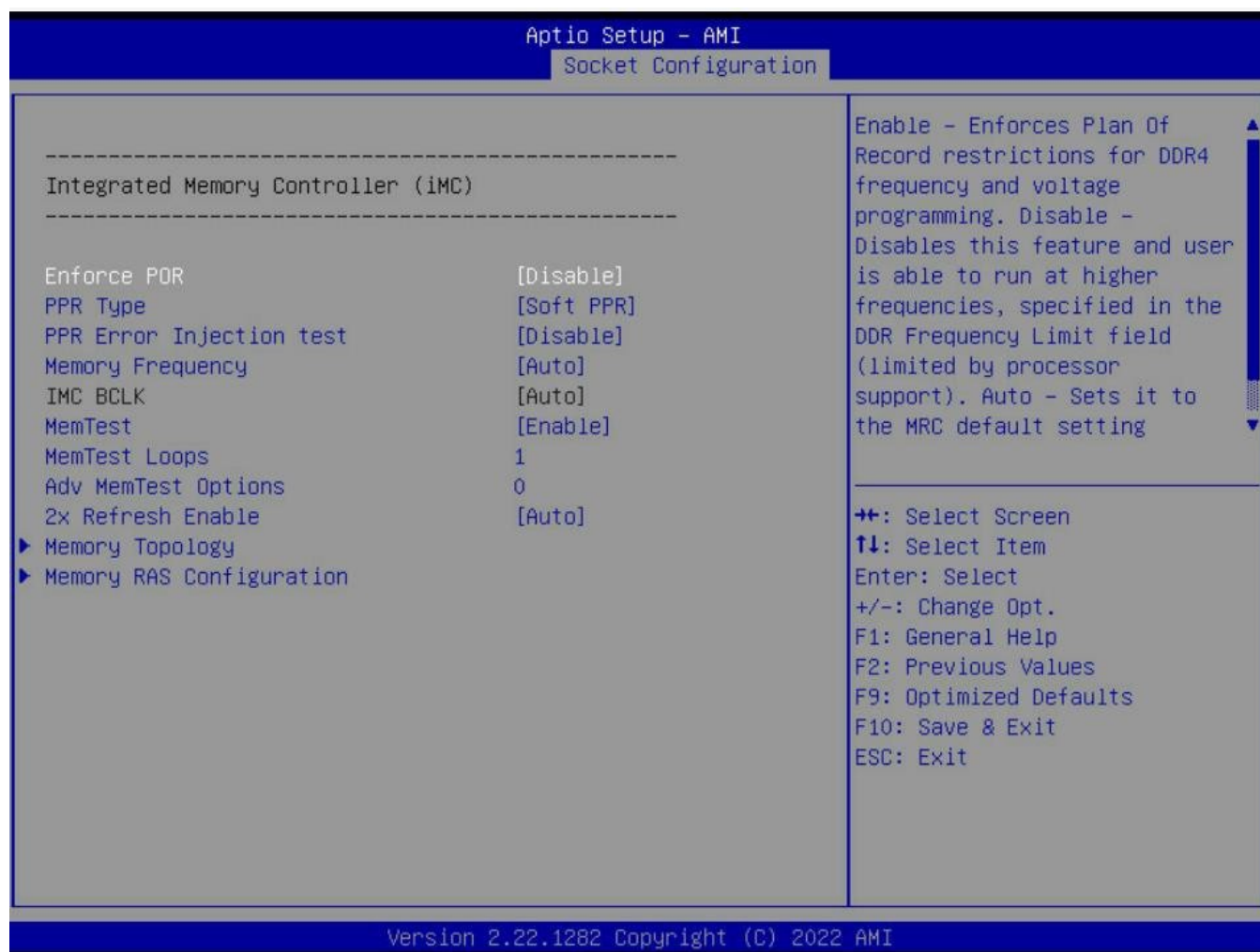


Рисунок 0-48 Memory Configuration

Настройка BIOS	Опции	Описание
Integrated Memory Controller (iMC)	Integrated Memory Controller (iMC)	Интегрированный контроллер памяти (iMC)
Memory Frequency	[Auto]/1200/1333/1400/1600/1800/1866/2000/2133/2200/2400/2600/2666/2800/2933/3000/3200/3400-OvrClk/3466-OvrClk/3600-OvrClk/3733-OvrClk/3800-OvrClk/4000-OvrClk/4200-OvrClk/4266-OvrClk/4400-OvrClk/4800-OvrClk	Выбор максимальной частоты памяти в МГц. Если Enforce POR отключено, пользователь сможет запускать на более высоких частотах, чем поддерживается памятью (ограничено поддержкой процессора). Не выбирайте "Reserved"
Enforce POR	Disable/POR	Enable - Принудительно применять ограничения Plan Of Record для частоты DDR4

Настройка BIOS	Опции	Описание
		и программирования напряжения. Disable - Отключает эту функцию, и пользователь может работать на более высоких частотах, указанных в поле Limit DDR Frequency (ограничено поддержкой процессора). Auto - Устанавливает значение MRC по умолчанию
PPR Type	Soft PPR/PPR Disabled/Hard PPR	Выбирает Post Package RepairType-Hard/Soft/Disabled . Auto-Sets it to the MRC default setting; current default is Soft PPR.
PPR Error Injection test	Disable/Enable	Включить/отключить поддержку теста c-script error inject
IMC BCLK	Auto/100MHz /133MHz	Auto, 100MHz или 133MHz

MemTest	Disable/Enable	Enable - Включает тест памяти во время обычной загрузки. Disable - Отключает эту функцию.
MemTest Loops	1	Количество циклов теста памяти во время обычной загрузки, установите 0 для бесконечного теста
Adv MemTest Options	0	Эта опция представляет собой битовую маску [19:0]: Все 0 = отключено: bit-0=XMATS8, bit-1=XMATS16, bit-2=XMATS32, bit-3=XMATS64, bit-4=WCMATS8, bit-5=WCMCH8, bit-6=GNDB64, bit-7=MARCHCM64, bits[8:10]=Reserved, bit-11=TWR, bit-12=DATARET, bit-13=MATS8TC1, bit-14=MATS8TC2, bit-15=MATS8TC3, bit-16=SK-HYNIX, bit-17=SAMSUNG, bit-18=MICRON, bit-19=SCRAM_X2
2x Refresh Enable	[Auto]/Enable/Disable	Включить/отключить 2x Refresh
Memory Topology	См. подробнее.	Отображает топологию памяти с информацией о заполнении DIMM.

MemTest	Disable/Enable	Enable - Включает тест памяти во время обычной загрузки. Disable - Отключает эту функцию.
Memory RAS Configuration	См. подробнее.	Отображает и предоставляет опцию для изменения настроек Memory RAS

Таблица 0-48 Memory Configuration

6.4.5.1. Memory Topology

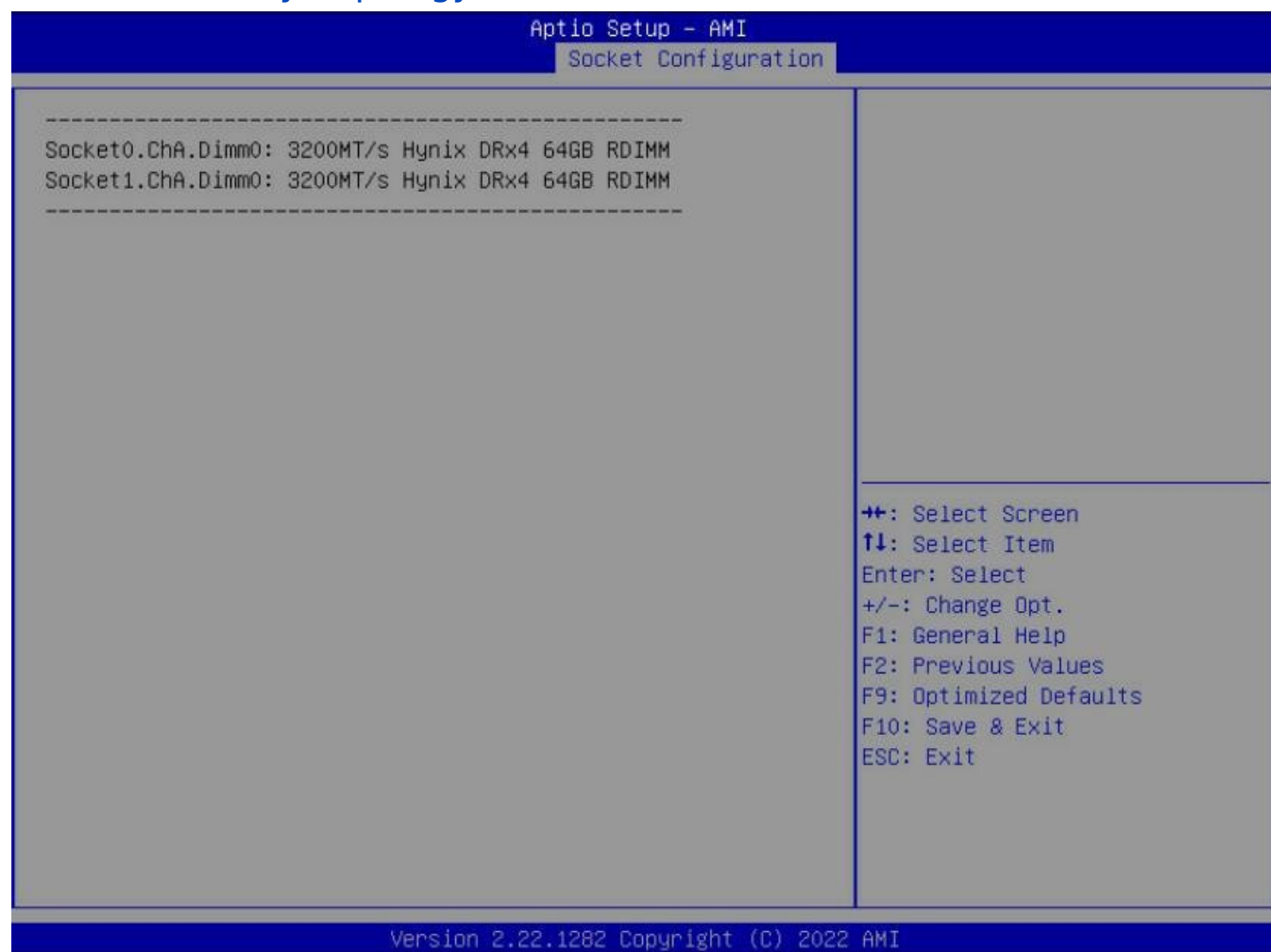


Рисунок 0-49 Memory Topology

Настройка BIOS	Опции	Опции	Опции	Описание	Описание
Socket0.ChA.Dimm0:	3200MT/s	Hynix	DRx4 64GB	DRx4 64GB	RDIMM
Socket1.ChA.Dimm0:	3200MT/s	Hynix	DRx4 64GB	DRx4 64GB	RDIMM

Таблица 0-49 Memory Topology

6.4.5.2. Конфигурация RAS памяти

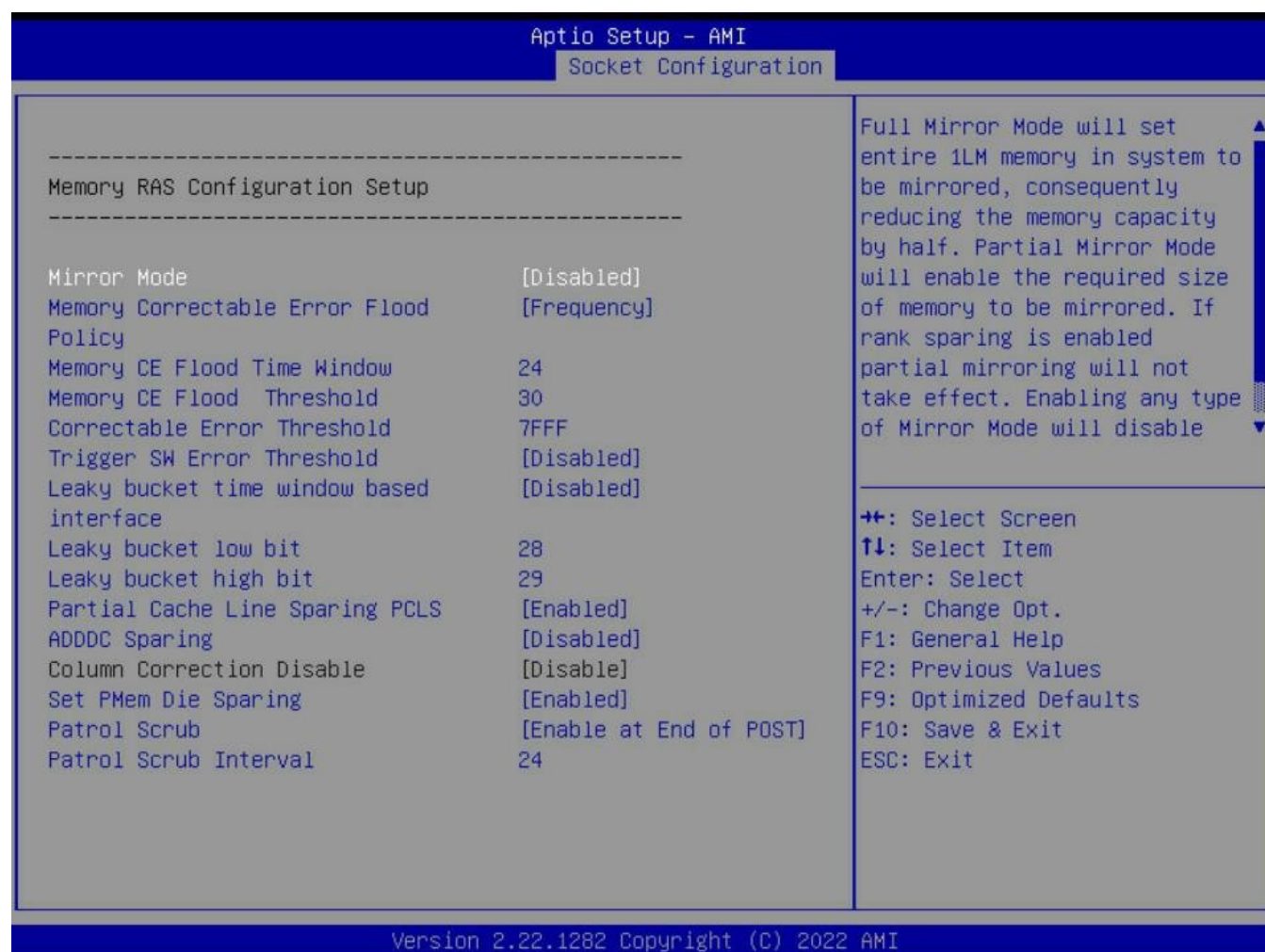


Рисунок 0-50 Memory RAS Configuration

Настройка BIOS	Опции	Описание
Mirror Mode	Disable/Full Mirror Mode/Partial Mirror Mode	Full Mirror Mode установит всю память 1LM в системе как зеркалируемую, что уменьшит объем памяти вдвое. Partial Mirror Mode позволит зеркалировать требуемый объем памяти. Если включено rank sparing, частичное зеркалирование не будет работать. Включение любого режима зеркалирования отключит
Memory Correctable Error Flood Policy	Disable/ Once/ Frequency	Политика флуда корректируемых ошибок

Настройка BIOS	Опции	Описание
		памяти
SW Correctable Error Time Window	24	Временное окно SW корректируемых ошибок
Memory CE Flood Threshold	30	Порог флуда корректируемых ошибок памяти
Correctable Error Threshold	7FFF	Порог корректируемых ошибок (0x01 - 0x7fff), используемый для sparing и leaky bucket
Trigger SW Error Threshold	Disable/Enable	Включить или отключить SW Per Bank Threshold
Leaky bucket time window based interface	Disable/Enable	Включить/отключить интерфейс leaky bucket time window-based
Leaky bucket low bit	28	Leaky bucket low bit (1 - 63)
Leaky bucket high bit	29	Leaky bucket high bit (1 - 63)
Partial Cache Line Sparing PCLS	Disable/Enable	Включить/отключить PCLS Sparing
Column Correction Disable	Disable	Отключить коррекцию колонок
ADDDC Sparing	Disable/Enable	Включить/отключить ADDDC Sparing
Set PMem Die Sparing	Disable/Enable	Включить/отключить PMem Die Sparing
Patrol Scrub	Disabled/Enabled/ Enable at End of POST	Включить/отключить Patrol Scrub
Patrol Scrub Interval	24	Выбирает количество часов (1-24), необходимых для завершения полного scrub. Значение 0 означает авто.

Таблица 0-50 Memory RAS Configuration

6.4.6. IIO Configuration

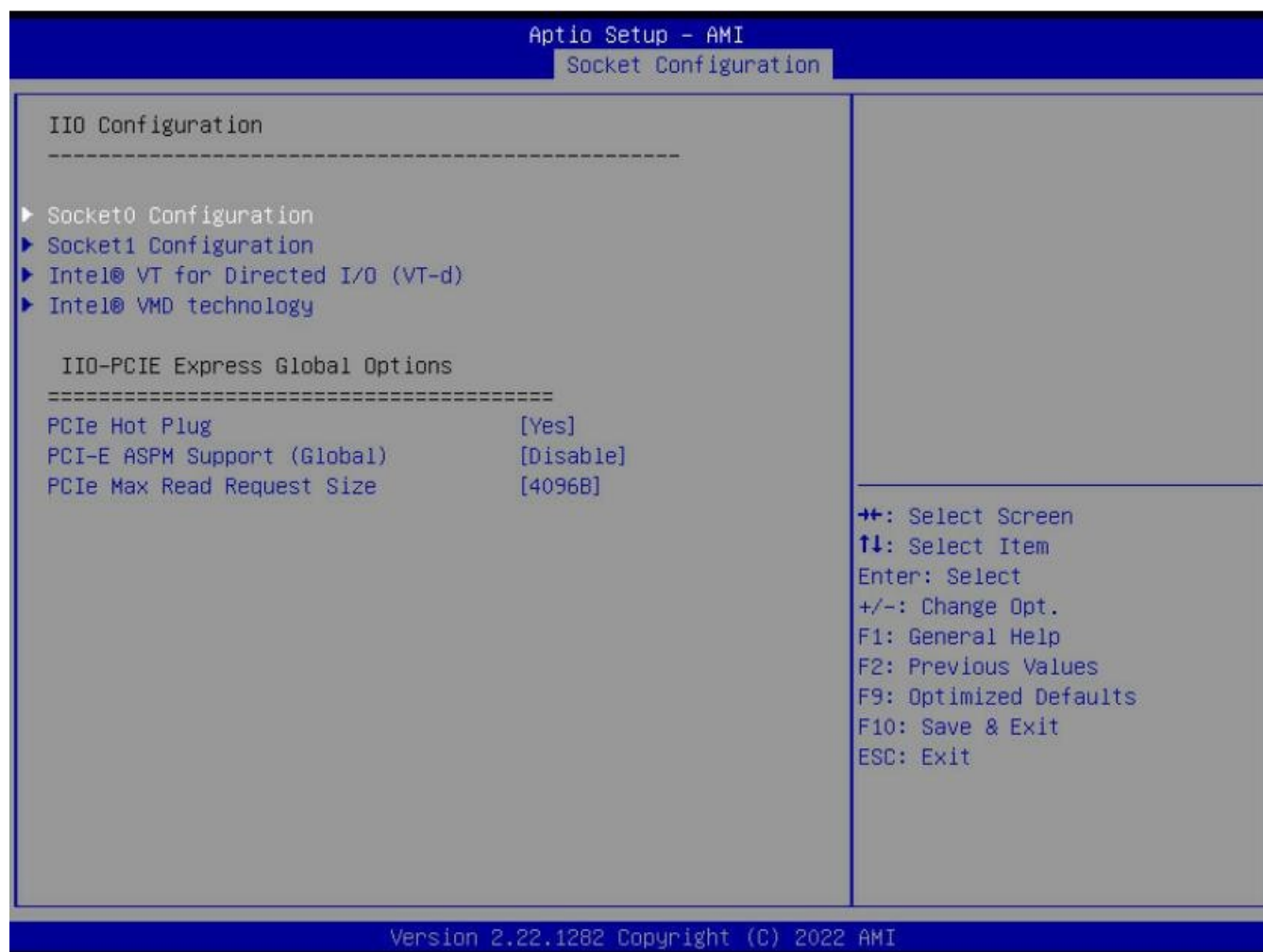


Рисунок 0-51 IIO Configuration

Настройка BIOS	Опции	Описание
IIO Configuration	IIO Configuration	Конфигурация IIO
Socket 0/1 Configuration	См. подробнее.	Опции конфигурации IIO.
Intel(R) VT for Directed I/O (VT-d)	См. подробнее.	Опции конфигурации Intel(R) VT-d.
Intel(R) VMD technology	См. подробнее.	Опции Intel(R) VMD для управления томами.
IIO-PCIe Express Global Options	IIO-PCIe Express Global Options	Глобальные настройки IIO-PCIe Express
PCIe Hot Plug	No / Yes	Глобальное включение/отключение PCIe Hot Plug
PCI-E ASPM Support (Global)	Disable/Per-Port	Эта опция включает/отключает поддержку ASP для всех нисходящих устройств.

Настройка BIOS	Опции	Описание
PCIe Max Read Request Size	Keep Default / 128B / 256B / 512B / 1024B / 2048B / 4096B	Установить запрошенный MRRS в иерархии PCI или сохранить значение HW по умолчанию.

Таблица 0-51 IIO Configuration

6.4.6.1. Socket 0/1 Configuration

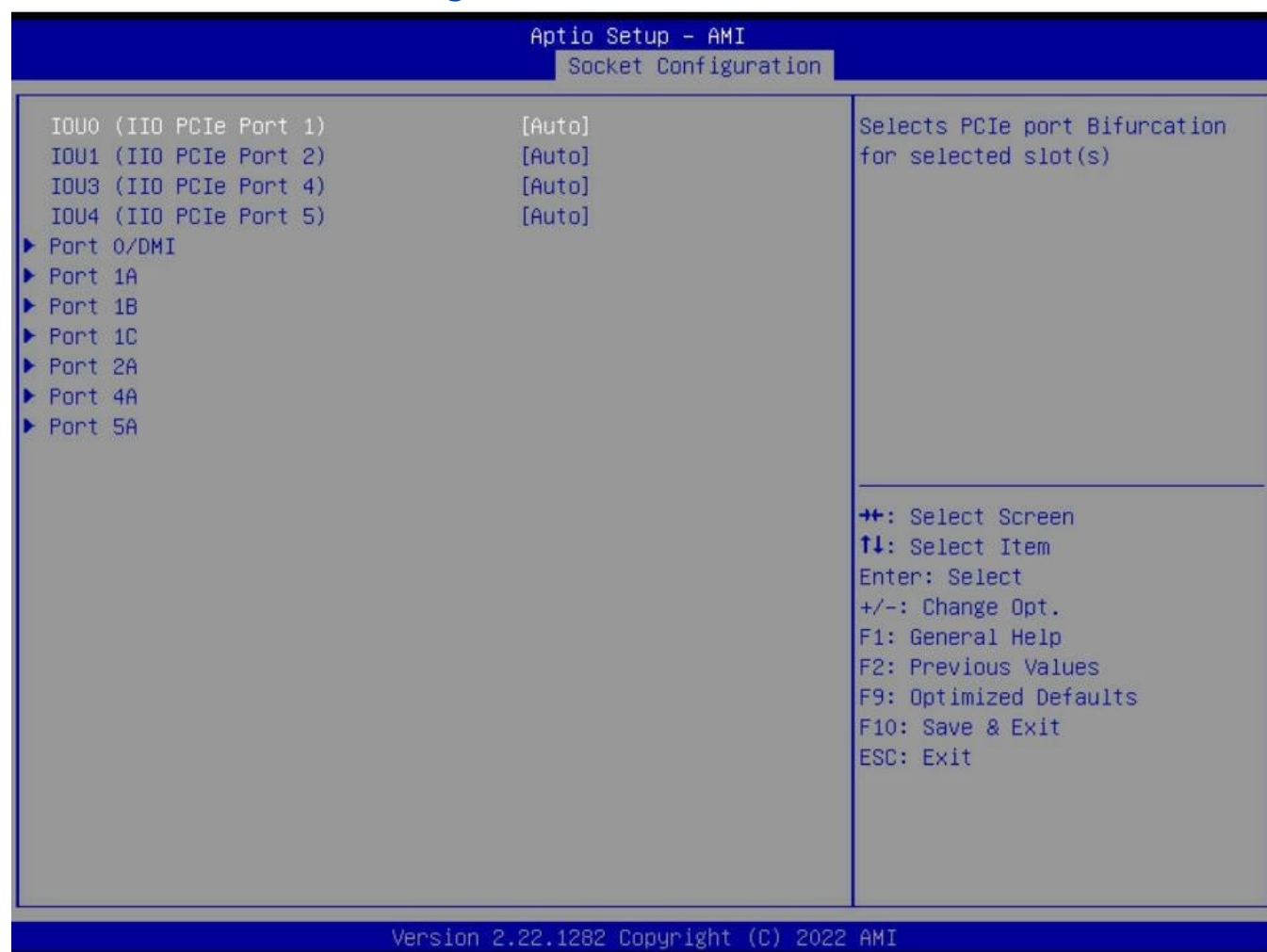


Рисунок 0-52 Socket 0/1 Configuration

Настройка BIOS	Опции	Описание
IOU0 (IIO PCIe Port 1)	X4x4x4x4/x4x4x8/x8x4x4/x8x8/x16/Auto	Выберите бифуркацию порта PCIe для выбранного слота(ов)
IOU1 (IIO PCIe Port 2)	X4x4x4x4/x4x4x8/x8x4x4/x8x8/x 16/Auto	Выберите бифуркацию порта PCIe для выбранного слота(ов)
IOU3 (IIO PCIe Port 4)	X4x4x4x4/x4x4x8/x8x4x4/x8x8/x 16/Auto	Выберите бифуркацию порта PCIe для выбранного

Настройка BIOS	Опции	Описание
		слота(ов)
IOU4 (IIO PCIe Port 5)	X4x4x4x4/x4x4x8/x8x4x4/x8x8/x 16/Auto	Выберите бифуркацию порта PCIe для выбранного слота(ов)
Port 0/DMI	См. подробнее.	Настройки, относящиеся к портам PCI Express(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).
Port 1A	См. подробнее.	Настройки, относящиеся к портам PCI Express(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).
Port 2A	См. подробнее.	Настройки, относящиеся к портам PCI Express(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).
Port 4A	См. подробнее.	Настройки, относящиеся к портам PCI Express(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).
Port 5A	См. подробнее.	Настройки, относящиеся к портам PCI Express(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).

Таблица 0-52 Socket 0/1 Configuration

6.4.6.2. Port 0/DMI

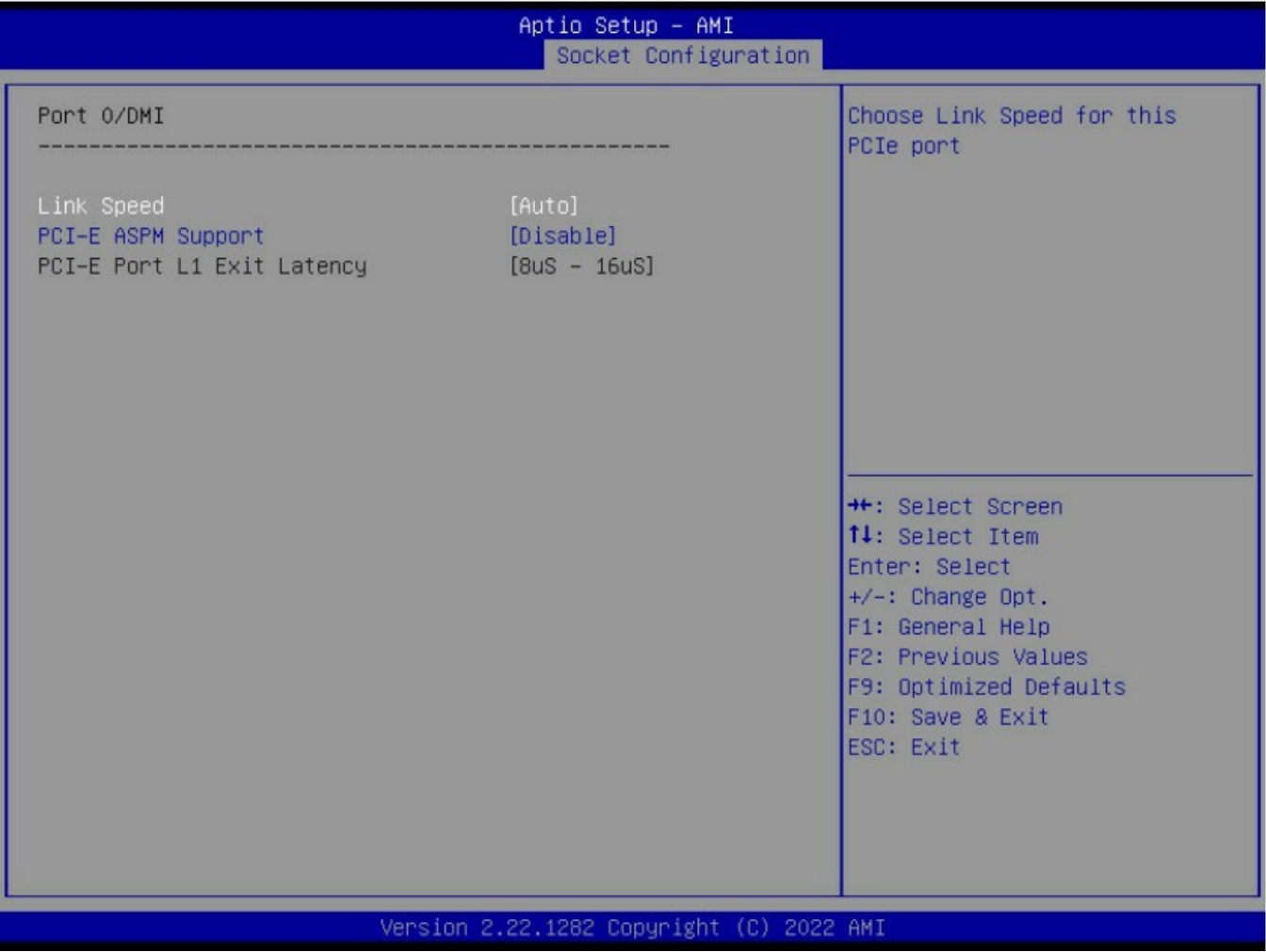


Рисунок 0-53 Port 0/DMI

Настройка BIOS	Опции	Описание
Port 0/DMI	Port 0/DMI	Порт 0/DMI
Link Speed	Auto/Gen 1 (2.5 GT/s)/Gen 2 (5 GT/s)/Gen 3 (8 GT/s)	Выберите скорость канала для этого порта PCIe.
PCI-E ASPM Support	Auto/L1 Only/Disable	Эта опция включает/отключает поддержку ASPM (L1) для нисходящих устройств.

PCI-E Port L1 Exit Latency 8us-16us

Таблица 0-53 Port 0/DMI

6.4.6.3. Port XX



Рисунок 0-54 Port 1A

Настройка BIOS	Опции	Описание
Port XX	Port XX	Порт XX
PCI-E Port	Auto/Enable /Disable	В автоматическом режиме BIOS отключит порт EXP, если на этом устройстве нет устройства или ошибок, и устройство не поддерживает HP. Disable используется для отключения порта и скрывания его пространства CFG.
Hot Plug Capable	Auto/Enable /Disable	Эта опция указывает, считается ли канал поддерживающим горячую замену.
Surprise Hot Plug Capable	Auto/Enable /Disable	Эта опция указывает, считается ли канал

Настройка BIOS	Опции	Описание
PCI-E Port Link Disable	No/Yes	поддерживающим внезапную горячую замену. Эта опция отключает канал, так что обучение не происходит, но пространство CFG остается активным.
Link Speed	Auto/Gen 1 (2.5 GT/s)/Gen 2 (5 GT/s)/Gen 3 (8 GT/s)/Gen 4 (16 GT/s)	Выберите скорость канала для этого порта PCIe.
PCI-E Port Link Status	Read Only	Статус канала порта PCI-E
PCI-E Port Link Max	Read Only	Максимум канала порта PCI- E
PCI-E Port Link Speed	Read Only	Скорость канала порта PCI-E
PCI-E Port Clocking	Distinct /Common	Настройка синхронизации порта через LNKCON[6]. Это относится к этому компоненту и нисходящему компоненту.
PCI-E Port Clock Gating	Enable /Disable	Включить/отключить Clock Gating для этого порта PCIe
Data Link Feature Exchange	Enable /Disable	Включить/отключить согласование функций канала данных в регистре Data Link Feature Capabilities (DLFCAP).
PCI-E Port MPSS	128B/256B/512B/Auto	Настройка максимального поддерживаемого размера полезной нагрузки в регистре PCIe Device Capabilities.
PCI-E Port D-state	D0 /D3Hot	Установите D0 для нормальной работы, D3Hot для перехода в состояние низкого энергопотребления
PCI-E ASPM Support	Auto/L1 Only/Disable	Эта опция включает/отключает поддержку ASPM (L1) для нисходящих устройств.
PCI-E Completion Timeout	260ms to 900ms	Таймаут завершения PCI-E
PCI-E Port L1 Exit Latency	8us-16us	Задержка выхода L1 порта PCI-E

Таблица 0-54 Port 1A

6.4.6.4. Intel(R) VT for Directed I/O (VT-d)



Рисунок 0-55 Intel(R) VT for Directed I/O (VT-d)

Настройка BIOS	Опции	Описание
Intel. VT for Directed I/O (VT-d) Intel. VT for Directed I/O	Intel. VT for Directed I/O (VT-d) Enable /Disable	Intel. VT for Directed I/O (VT-d) Включить/отключить Intel. Virtualization Technology for Directed I/O (VT-d), сообщая о назначении устройства ввода-вывода VMM через таблицы DMAR ACPI.
Interrupt Remapping	Auto/Enable/Disable	Включить/отключить поддержку переназначения прерываний VT-d.

Таблица 0-55 Intel(R) VT for Directed I/O (VT-d)

6.4.6.5. VMD Configuration



Рисунок 0-56 VMD Configuration

Настройка BIOS	Опции	Описание
Intel. VMD technology	Intel. VMD technology	Технология Intel. VMD
Intel. VMD for Volume Management Device on Socket 0	См. подробнее.	
Intel. VMD for Volume Management Device on Socket 1	См. подробнее.	

Таблица 0-56 VMD Configuration

6.4.6.6. VMD for Volume Management Device on Socket 0

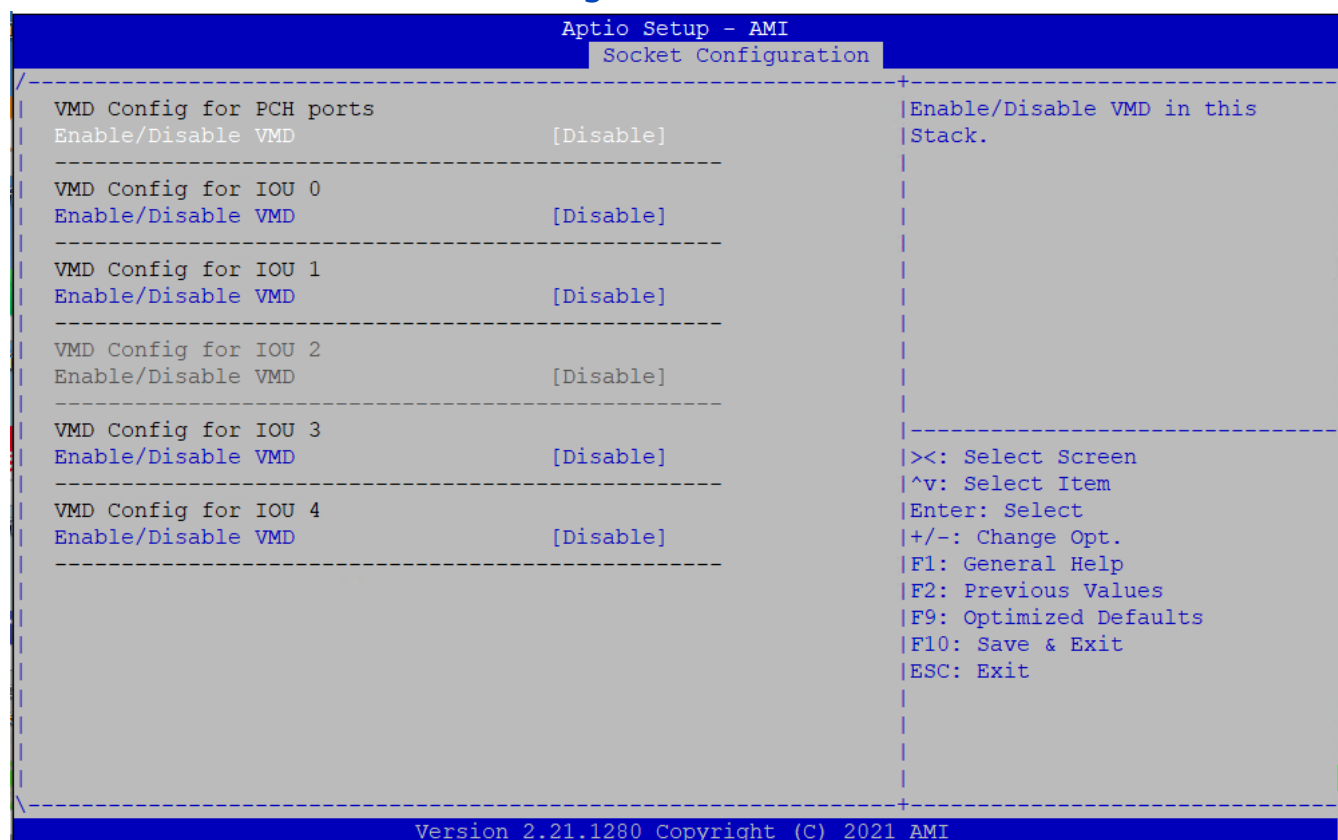


Рисунок 0-57 VMD for Volume Management Device on Socket 0

Настройка BIOS	Опции	Описание
VMD Config for PCH ports	VMD Config for PCH ports	Конфигурация VMD для портов PCH
Enable/Disable VMD	Enable /Disable	Включить / Отключить VMD
VMD Config for IOU 0/1/3/4	VMD Config for IOU 0/1/3/4	Конфигурация VMD для IOU 0/1/3/4
Enable/Disable VMD	Enable /Disable	Включить / Отключить VMD

Таблица 0-57 VMD for Volume Management Device on Socket 0

6.4.7. Advanced Power Management Configuration

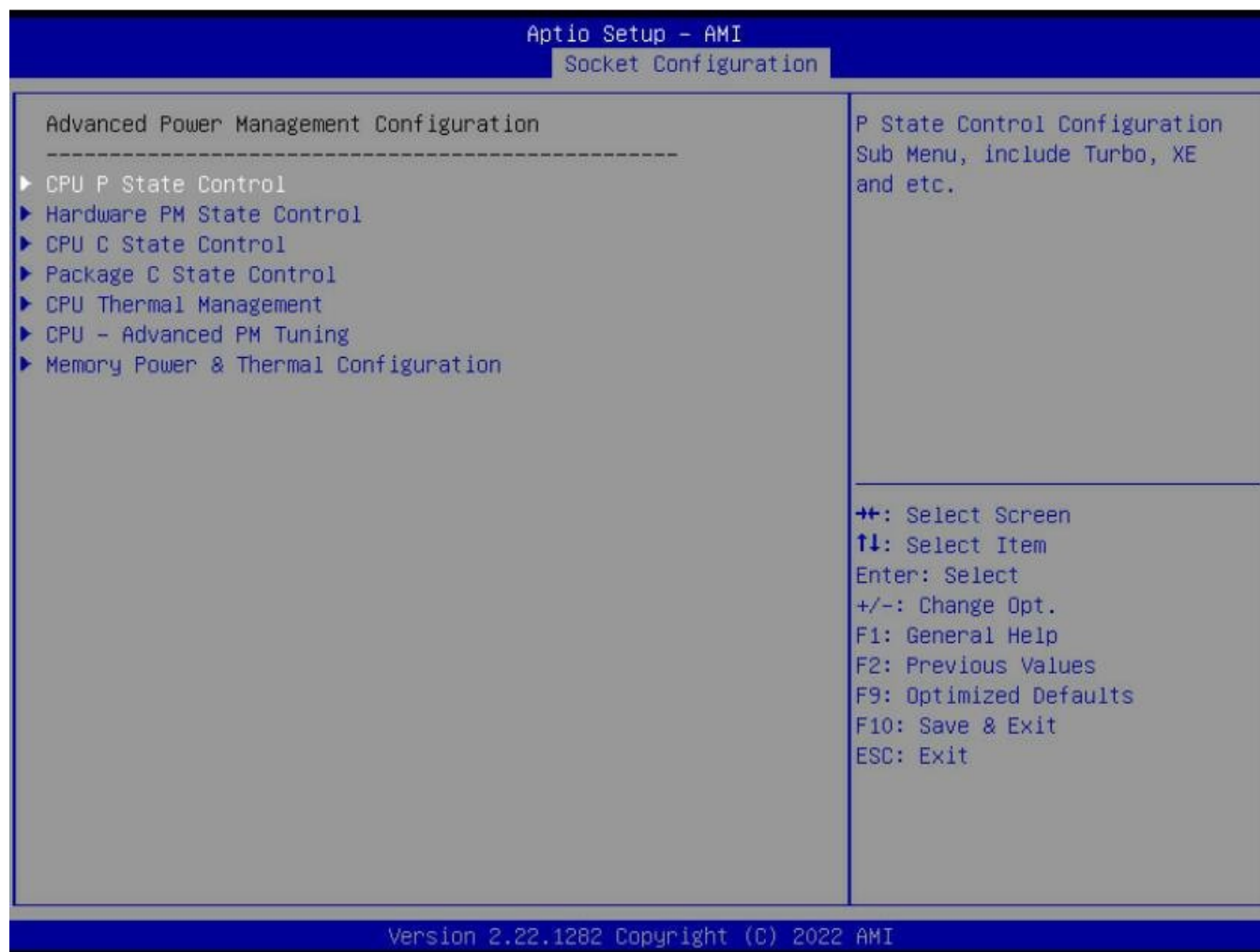


Рисунок 0-58 Advanced Power Management Configuration

Настройка BIOS	Опции	Описание
Advanced Power Management Configuration	Advanced Power Management Configuration	Расширенная конфигурация управления питанием
CPU P State Control	См. подробнее.	Подменю конфигурации управления P-состояниями, включая Turbo, XE и т.д.
Hardware PM State Control	См. подробнее.	Настройка аппаратного P-состояния
CPU C State Control	См. подробнее.	Настройки C-состояний процессора.
Package C State Control	См. подробнее.	Настройка C-состояния пакета.
CPU Thermal Management	См. подробнее.	Настройки, связанные с тепловыделением процессора.
CPU - Advanced PM Tuning	См. подробнее.	Настройка Energy Per Bias, Pwr_Ctl, PPO Current SWLTD,

Настройка BIOS	Опции	Описание
Memory Power & Thermal Configuration	См. подробнее.	SAPM и т.д. Отображает и предоставляет опцию для изменения настроек памяти

Таблица 0-58 Advanced Power Management Configuration

6.4.7.1. CPU P State Control



Рисунок 0-59 CPU P State Control

Настройка BIOS	Опции	Описание
CPU P State Control	CPU P State Control	Конфигурация P-состояний процессора
Speed Step (P states)	Enable / Disable	Включить/отключить EIST (P-States).
EIST PSD Function	HW_ALL/SW_ALL	Выбор HW_ALL/SW_ALL при возврате _PSD.
Boot performance mode	Max Performance/Max Efficient/Set by Intel Node Manager	Выбор режима производительности, который BIOS установит перед передачей управления ОС.
Energy Efficient Turbo	Enable / Disable	Energy Efficient Turbo Disable,

Настройка BIOS	Опции	Описание
Turbo Mode	Enable / Disable	MSR 0x1FC [19] Включить/отключить режим Turbo процессора (требуется включения EMTTM).

Таблица 0-59 CPU P State Control

6.4.7.2. Hardware PM State Control

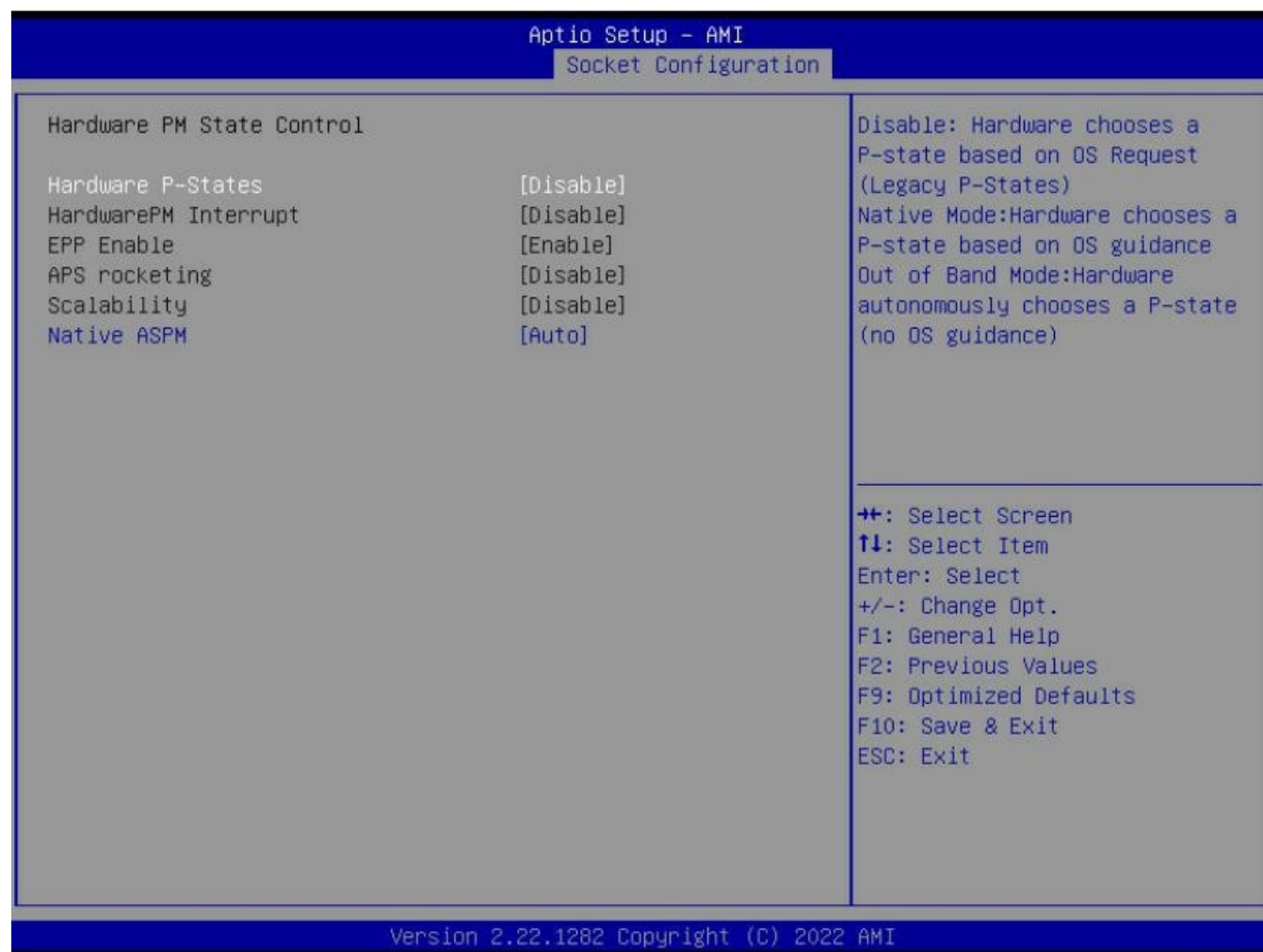


Рисунок 0-60 Hardware PM State Control

Настройка BIOS	Опции	Описание
Hardware PM State Control	Hardware PM State Control	Конфигурация аппаратного управления питанием
Hardware P-States	Disable/ Native Mode/ Out of Band Mode / Native Mode with No Legacy Support	Disable: Аппаратное обеспечение выбирает P-состояние на основе запроса ОС (Legacy P-States) Native Mode: Аппаратное

Настройка BIOS	Опции	Описание
		обеспечение выбирает P-состояние на основе рекомендаций ОС. Out of Band Mode: Аппаратное обеспечение автономно выбирает P-состояние (без указаний ОС).
HardwarePM Interrupt	Enable / Disable	Включить/отключить прерывание аппаратного управления питанием.
EPP Enable	Enable / Disable	При отключении, HW маскирует EPP в CPUID[6] .10 и использует EPB для EPP.
APS rocketing	Enable / Disable	Включить/отключить механизм rocketing в алгоритме выбора P-состояния HWP.Rocketing позволяет коэффициенту ядра мгновенно подскакивать до максимального турбо, в отличие от плавного нарастания.
Scalability	Enable / Disable	Включить/отключить оптимизации масштабирования производительности ядра к частоте в процессоре.
Native ASPM	Auto /Enable / Disable	Enabled - ASPM управляется ОС, Disabled - ASPM выключен, AUTO - ASPM управляется BIOS.

Таблица 0-60 Hardware PM State Control

6.4.7.3. CPU C State Control

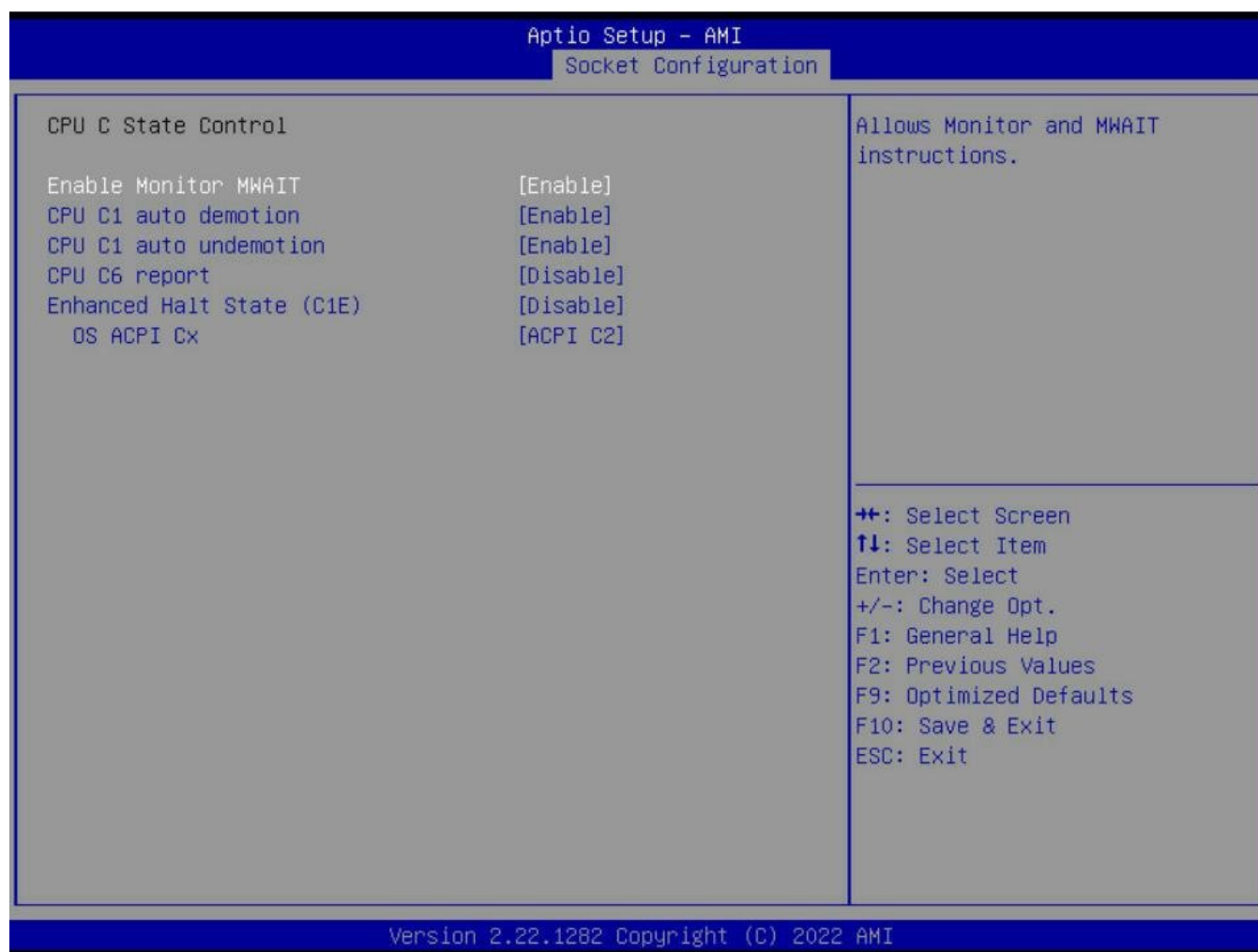


Рисунок 0-61 CPU C State Control

Настройка BIOS	Опции	Описание
CPU C State Control	CPU C State Control	Конфигурация C-состояний процессора
Enable Monitor MWAIT	Enable / Disable	Разрешает инструкции Monitor и MWAIT.
CPU C1 auto demotion	Enable / Disable	Разрешает процессору автоматически понижать уровень до C1. Вступает в силу после перезагрузки.
CPU C1 auto undemotion	Enable / Disable	Разрешает процессору автоматически повышать уровень из C1. Вступает в силу после перезагрузки.
CPU C6 report	Auto / Enable / Disable	Включить/отключить отчет CPU C6 (ACPI C3) для ОС.
Enhanced Halt State (C1E)	Enable / Disable	Управление автоматическим

Настройка BIOS	Опции	Описание
		продвижением Core C1E. Вступает в силу после перезагрузки.
OS ACPI Cx	ACPI C2/ ACPI C3	Сообщать CC3/CC6 OC как ACPI C2 или ACPI C3.

Таблица 0-61 CPU C State Control

6.4.7.4. Package C State Control



Рисунок 0-62 Package C State Control

Настройка BIOS	Опции	Описание
Package C State Control	Package C State Control	Конфигурация C-состояний пакета
Package C State	C0/C1 state/C2 state/C6(non-Retention) state/Auto	Лимит C-состояния пакета.

Таблица 0-62 Package C State Control

6.4.7.5. CPU Thermal Management



Рисунок 0-63 CPU Thermal Management

Настройка BIOS	Опции	Описание
CPU Thermal Management	CPU Thermal Management	Управление охлаждением процессора
PROCHOT Modes	Output-only / Disable / Both Input and Output / Input-only	Когда срабатывает термодатчик процессора (любое ядро), запускается PROCHOT#. Если включено двунаправленное действие, внешние агенты могут управлять PROCHOT# для снижения частоты процессора.
Thermal Monitor	Enable/Disable	Включить/отключить Thermal Monitor

Таблица 0-63 CPU Thermal Management

6.4.7.6. CPU-Advanced PM Tuning

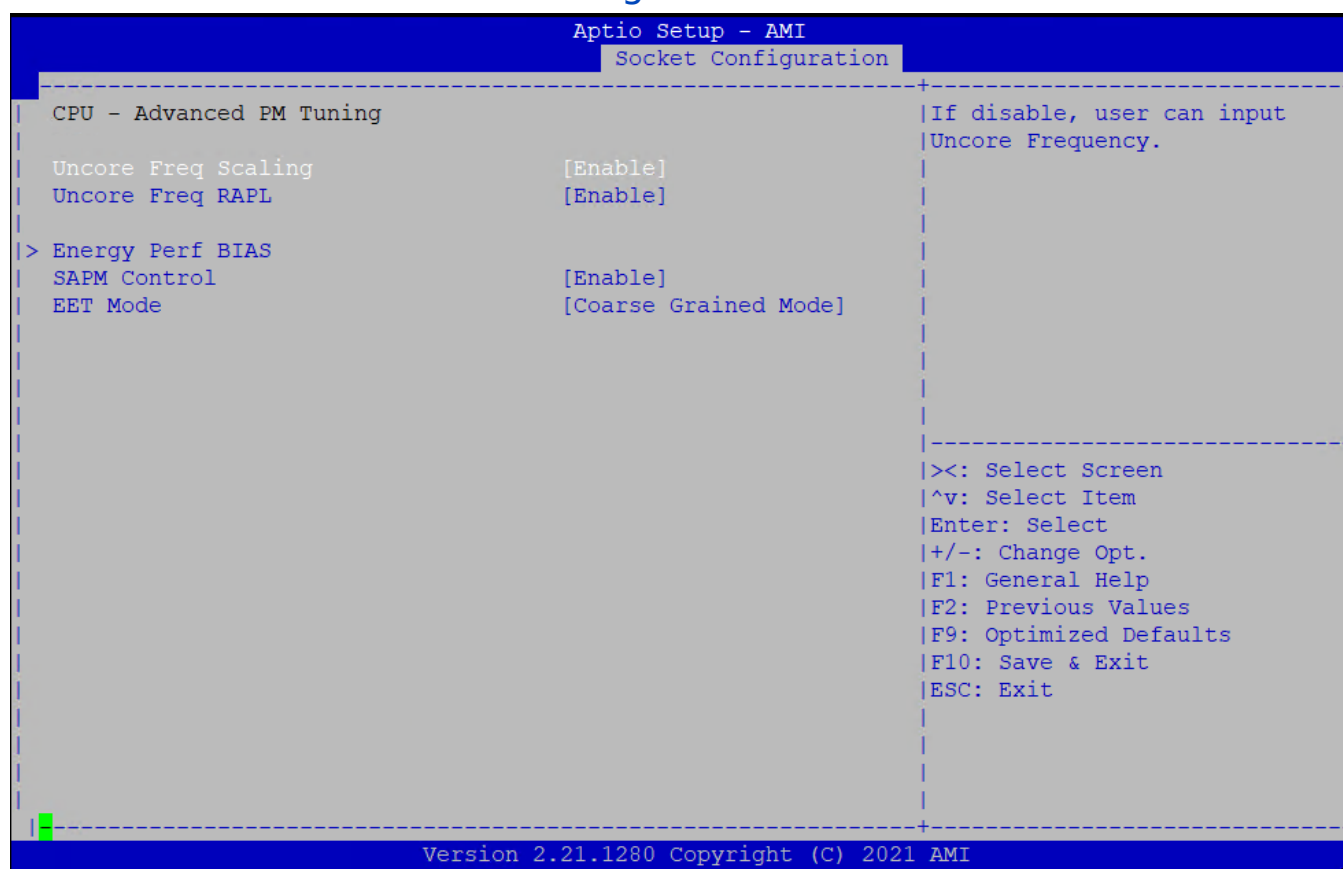


Рисунок 0-64 CPU-Advanced PM Tuning

Настройка BIOS	Опции	Описание
CPU-Advance PM Tuning	CPU-Advance PM Tuning	Расширенная настройка питания CPU
Uncore Freq Scaling	Enable/Disable	Если отключено, пользователь может ввести частоту Uncore.
Uncore Freq RAPL	Enable/Disable	Enable: BYPASS_CLM_RAPL_LIMIT = 0 Disable: BYPASS_CLM_RAPL_LIMIT= 1
Energy Perf BIAS	См. подробнее.	Подменю Energy Perf BIAS
SAPM Control	Enable/Disable	MSR 1FCh Bit [22] = PWR_PERF_TUNING_DISABLE_S APM_CT RL.
EET Mode	Coarse Grained Mode/Fine Grained Mode	Coarse Grained Mode решает, предоставить ли пользователю запрос турбо или P1. Fine Grained Mode решает, сколько турбо предоставить. Более полезно при включенном масштабировании

Настройка BIOS	Опции	Описание
		(Scalability).

Таблица 0-64 CPU-Advanced PM Tuning

6.4.7.7. Energy Perf BIAS

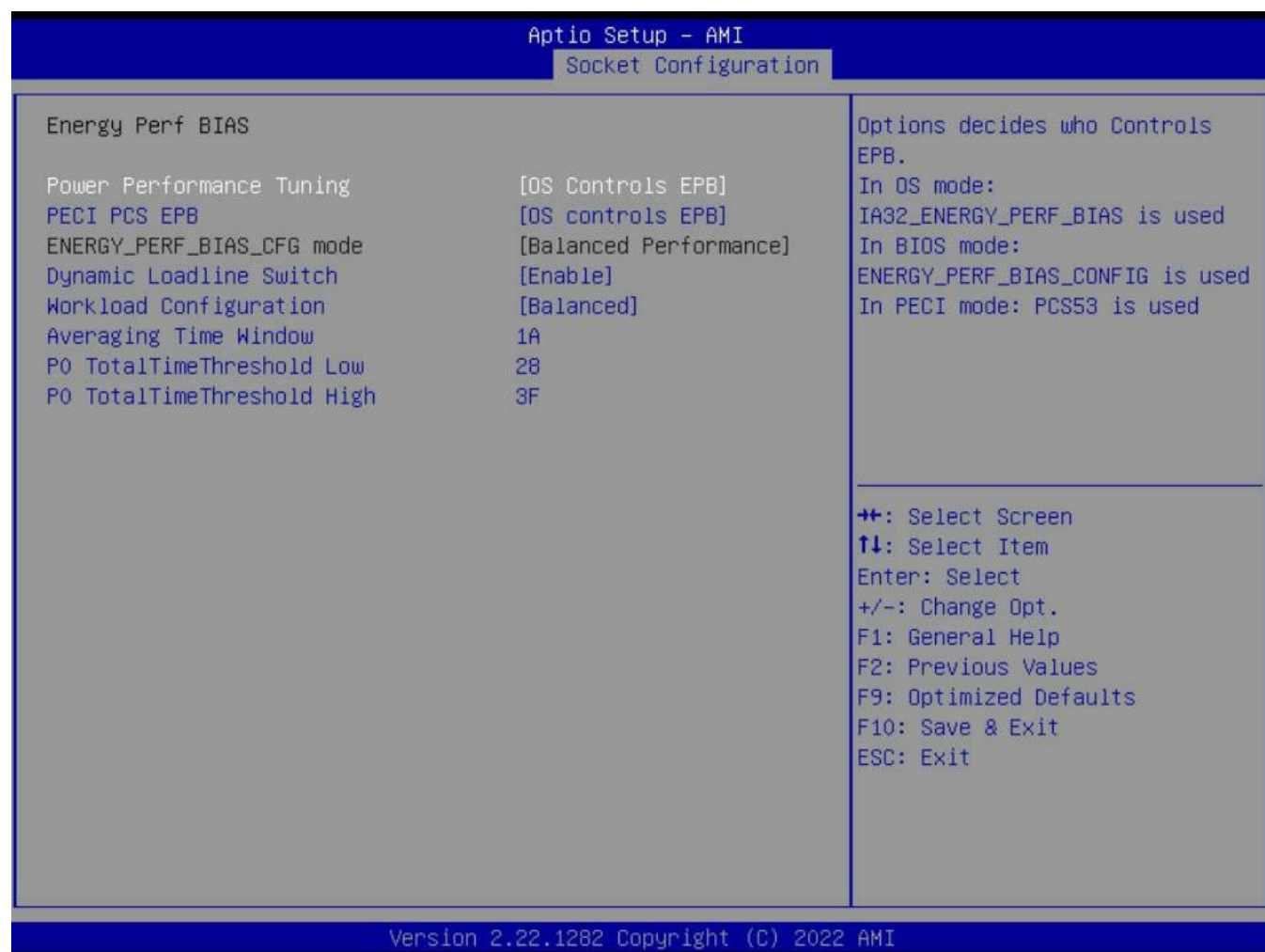


Рисунок 0-65 Energy Perf BIAS

Настройка BIOS	Опции	Описание
Energy Perf BIAS	Energy Perf BIAS	Energy Perf BIAS
Power Performance Tuning	OS Controls EPB / BIOS Controls EPB / PECI Controls EPB	Опция решает, кто управляет EPB.режиме OS: используется IA32_ENERGY_PERF_BIASрежи ме BIOS: используется ENERGY_PERF_BIAS_CONFIGре жиме PĒCI: используется PCS53.
PECI PCS EPB	OS controls EPB/ PECI controls	Управляет тем, имеет ли

Настройка BIOS	Опции	Описание
	EPB using PCS	PECI контроль над EPB
ENERGY_PERF_BIAS_CFG mode	Performance/ Balanced Performance/ Balanced Power/ Power	Использовать входные данные из выбора режима ENERGY_PERF_BIAS_CONFIG. PERF/Balanced Perf/Balanced Power/Power
Dynamic Loadline Switch	Enable/Disable	Управление переключателем Dynamic Loadline. MSR 0x1FC[Bit24]
Workload Configuration	Balanced/I/O sensitive	Это позволяет оптимизировать характеристику рабочей нагрузки. Три опции для выбора.
Averaging Time Window	1A	Это позволяет оптимизировать характеристику рабочей нагрузки. Три опции для выбора
P0 TotalTimeThreshold Low	2B	Механизм переключения HW ОТКЛЮЧАЕТ настройку производительности (0), когда общее время P0 меньше этого порога
P0 TotalTimeThreshold High	3F	Механизм переключения HW ВКЛЮЧАЕТ настройку производительности (0), когда общее время P0 больше этого порога

Таблица 0-65 Energy Perf BIAS

6.5. Server Mgmt

6.5.1. System Event Log

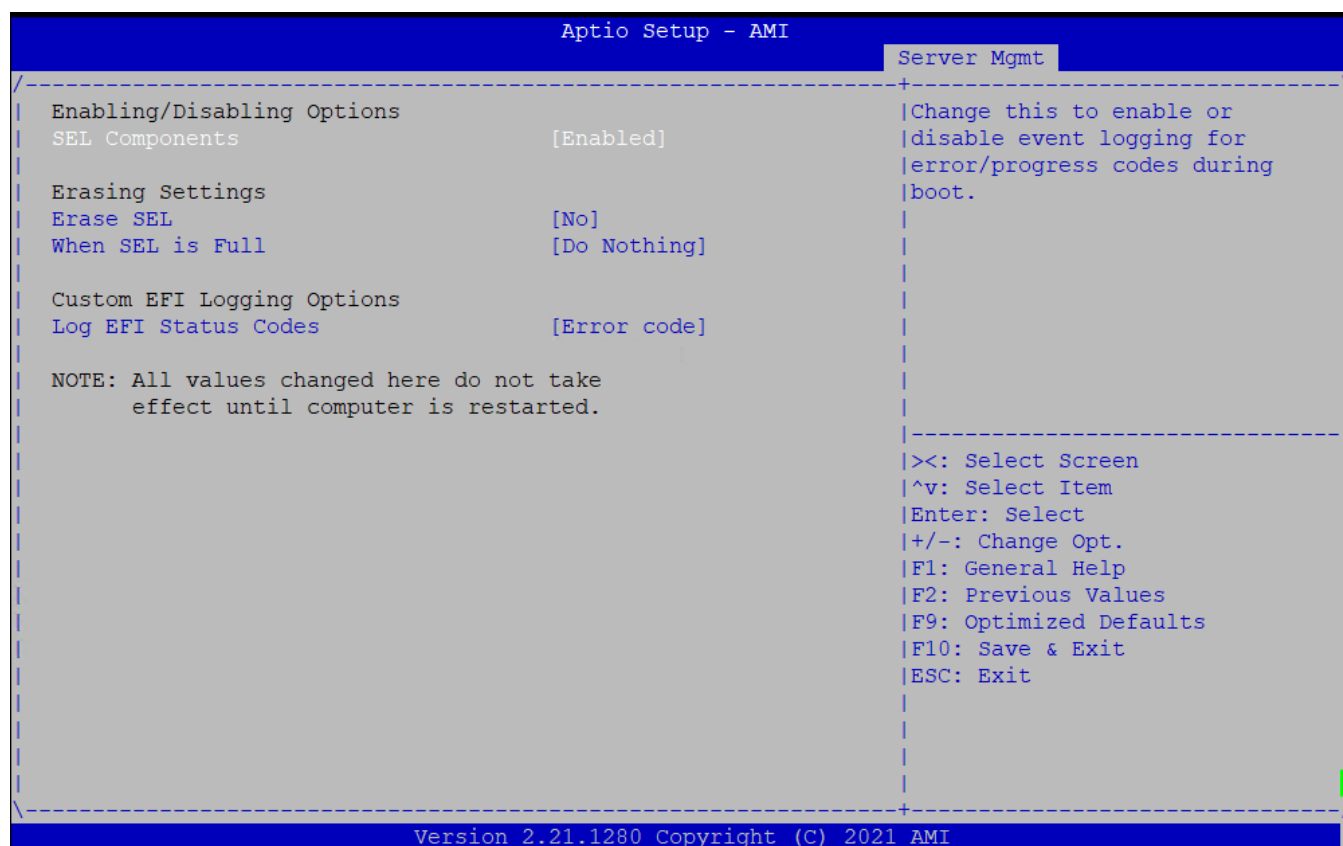


Рисунок 0-67 System Event Log

Настройка BIOS	Опции	Описание
Enabling/Disabling Options	Enabling/Disabling Options	Опции включения/отключения
SEL Components	Enabled/Disabled	Измените это, чтобы включить или отключить все функции логирования системных событий во время загрузки.
ErasingSettings	ErasingSettings	Настройки очистки
Erase SEL	No/Yes, On next reset/ Yes, On every reset	Выберите опции для очистки SEL.
When SEL is Full	Do Nothing/Erase Immediately/Delete Oldest Record	Выберите опции реакции на переполнение SEL.
Customer EFI Logging Options	Customer EFI Logging Options	Опции логирования EFI клиента
Log EFI Status Codes	Disabled/Both/Error	Отключить логирование

Настройка BIOS	Опции	Описание
	code/Progress code	статус-кодов EFI или логировать только коды ошибок, или только коды прогресса, или оба типа.

Таблица 0-67 System Event Log

6.5.2. View FRU information

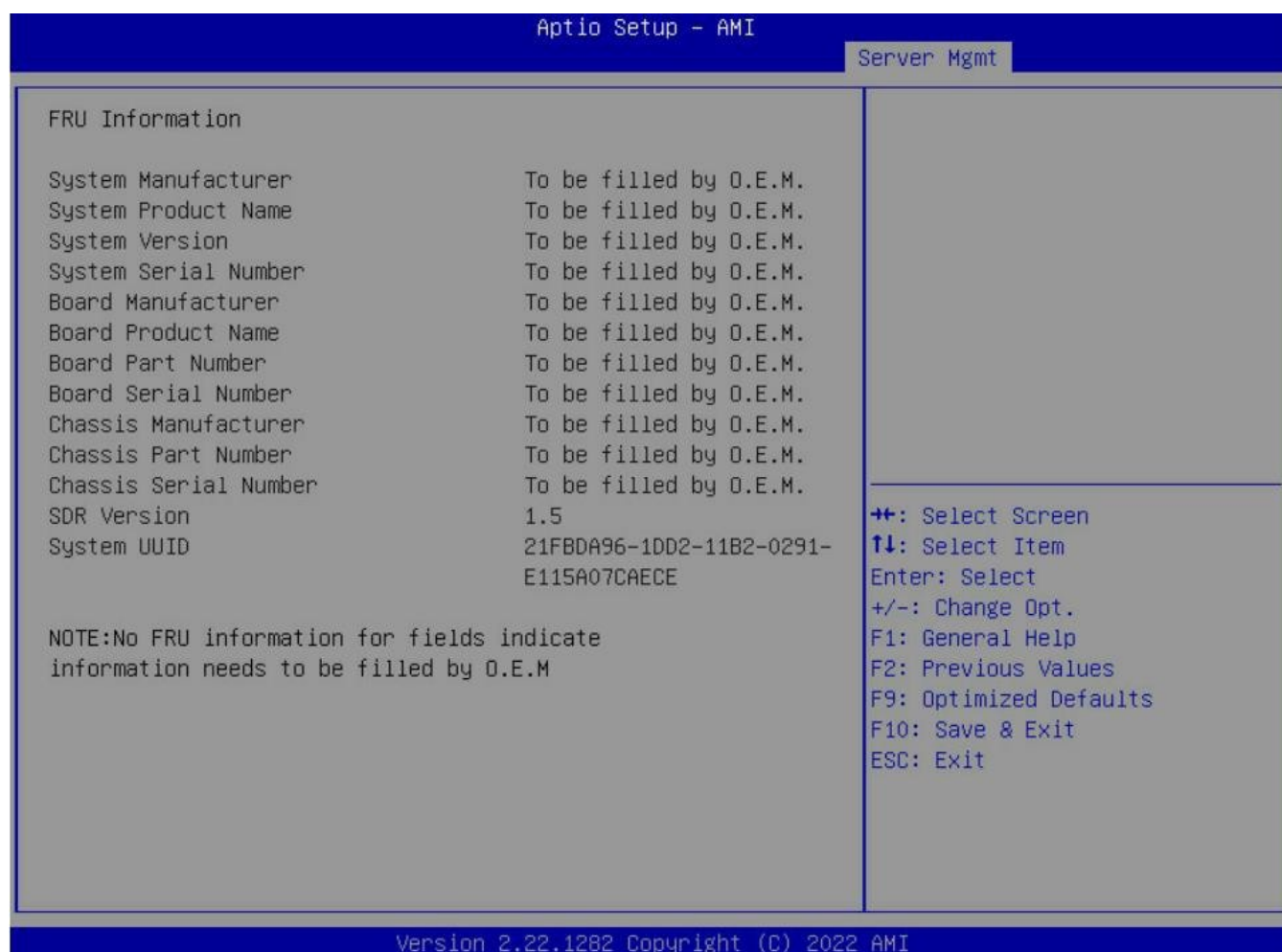


Рисунок 0-68 View FRU Information

6.5.3. BMC network configuration

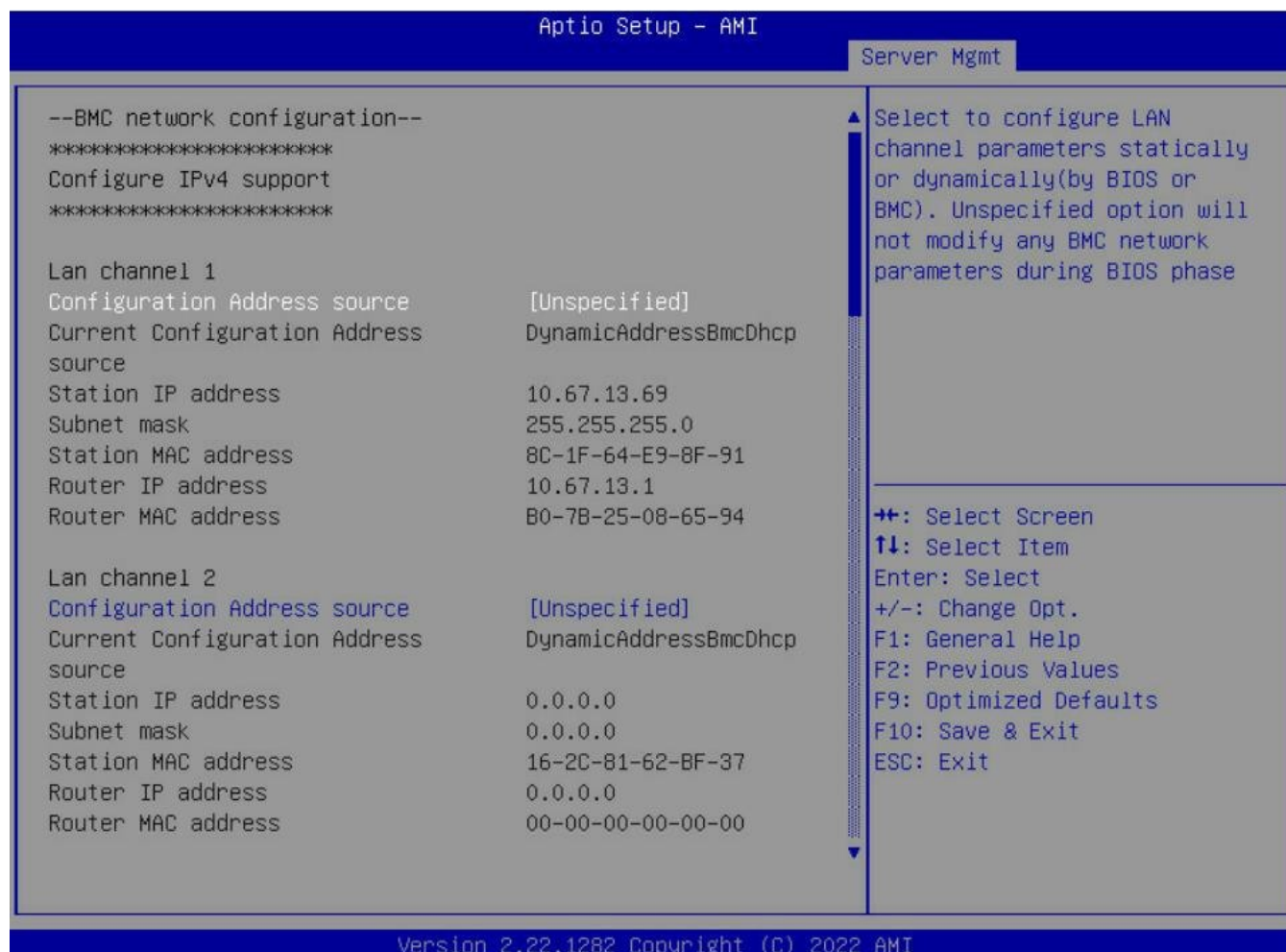


Рисунок 0-69 BMC network configuration

Настройка BIOS	Опции	Описание
BMC network configuration	BMC network configuration	Конфигурация сети BMC
Lan channel 1		
Configuration Address source	Unspecified/ Static/ DynamicBmcDhcp/DynamicBmcNonDhcp	Выберите для настройки параметров LAN канала статически или динамически (BIOS или BMC). Опция Unspecified не изменит сетевые параметры BMC на этапе BIOS
Current Configuration Address source		Текущая конфигурация LAN статическая или динамическая (BIOS или BMC). Unspecified для ненастроенного адресного пространства
Station IP address		Введите IP адрес станции

Настройка BIOS	Опции	Описание
Subnet mask		Введите маску подсети
Station MAC address		Введите MAC адрес станции
Router IP address		Введите IP адрес маршрутизатора
Router MAC address		Введите MAC адрес маршрутизатора
Lan channel 2		
Configuration Address source	Unspecified/Static/ DynamicBmcDhcp/ DynamicBmcNonDhcp	Выберите для настройки параметров LAN канала статически или динамически (BIOS или BMC). Опция Unspecified не изменит сетевые параметры BMC на этапе BIOS
Current Configuration Address source		Текущая конфигурация LAN статическая или динамическая (BIOS или BMC). Unspecified для ненастроенного адресного пространства
Station IP address		Введите IP адрес станции
Subnet mask		Введите маску подсети
Station MAC address		Введите MAC адрес станции
Router IP address		Введите IP адрес маршрутизатора
Router MAC address		Введите MAC адрес маршрутизатора

Таблица 0-68 BMC network configuration

6.5.4. View System Event Log

Aptio Setup - AMI			Server Mgmt
No. of log entries in SEL : 893			^ HEX:
DATE	TIME	SENSOR TYPE	* 01 00 02 E1 BF 17
02/01/21	08:46:25	Temperature	+ 60 20 00 04 01 50
02/01/21	08:46:53	Temperature	+ 01 57 5F 5F
02/01/21	08:53:47	Temperature	+ Generator ID: BMC - LUN #0
02/01/21	08:54:34	Temperature	+ (Channel #0)
02/01/21	08:59:25	Temperature	+ Sensor Number: 0x50 Reserved
02/01/21	09:00:08	Temperature	+ or Unknown
02/01/21	09:16:17	Temperature	+ Event Description: Record
02/01/21	09:16:50	Temperature	+ Type-0x02. Assertion Event.
02/01/21	09:17:56	Temperature	+
02/01/21	09:18:31	Temperature	+ -----
02/01/21	09:21:47	Temperature	+ ><: Select Screen
02/01/21	09:22:19	Temperature	+ ^v: Select Item
02/02/21	07:50:16	Temperature	+ Enter: Select
02/02/21	07:51:19	Temperature	+ +/-: Change Opt.
02/01/21	09:01:51	Temperature	+ F1: General Help
02/01/21	09:02:33	Temperature	+ F2: Previous Values
02/05/21	04:53:21	Temperature	+ F9: Optimized Defaults
02/05/21	04:53:53	Temperature	+ F10: Save & Exit
02/05/21	04:55:05	Temperature	+ ESC: Exit
02/05/21	04:55:39	Temperature	+
02/25/21	04:55:50	Temperature	v
Version 2.22.1282 Copyright (C) 2021 AMI			

Рисунок 0-70 View System Event Log

Настройка BIOS	Опции	Описание
System Event Log	System Event Log	Журнал системных событий
DATE	TIME	SENSOR TYPE (ДАТА / ВРЕМЯ / ТИП СЕНСОРА)

Таблица 0-69 View System Event Log

6.5.5. BMC User Settings



Рисунок 0-71 BMC User Settings

Настройка BIOS	Опции	Описание
BMC User Settings	BMC User Settings	Пользовательские настройки BMC
Add User	Gray Out	Нажмите для добавления, удаления и установки уровня привилегий пользователей.
Delete User	Gray Out	Нажмите для удаления пользователя.
Change User Settings	Gray Out	Нажмите для изменения настроек пользователя.

Таблица 0-70 BMC User Settings

6.5.0.0.1. Use the Server Mgmt menu to configure the BMC through the sub-menu.

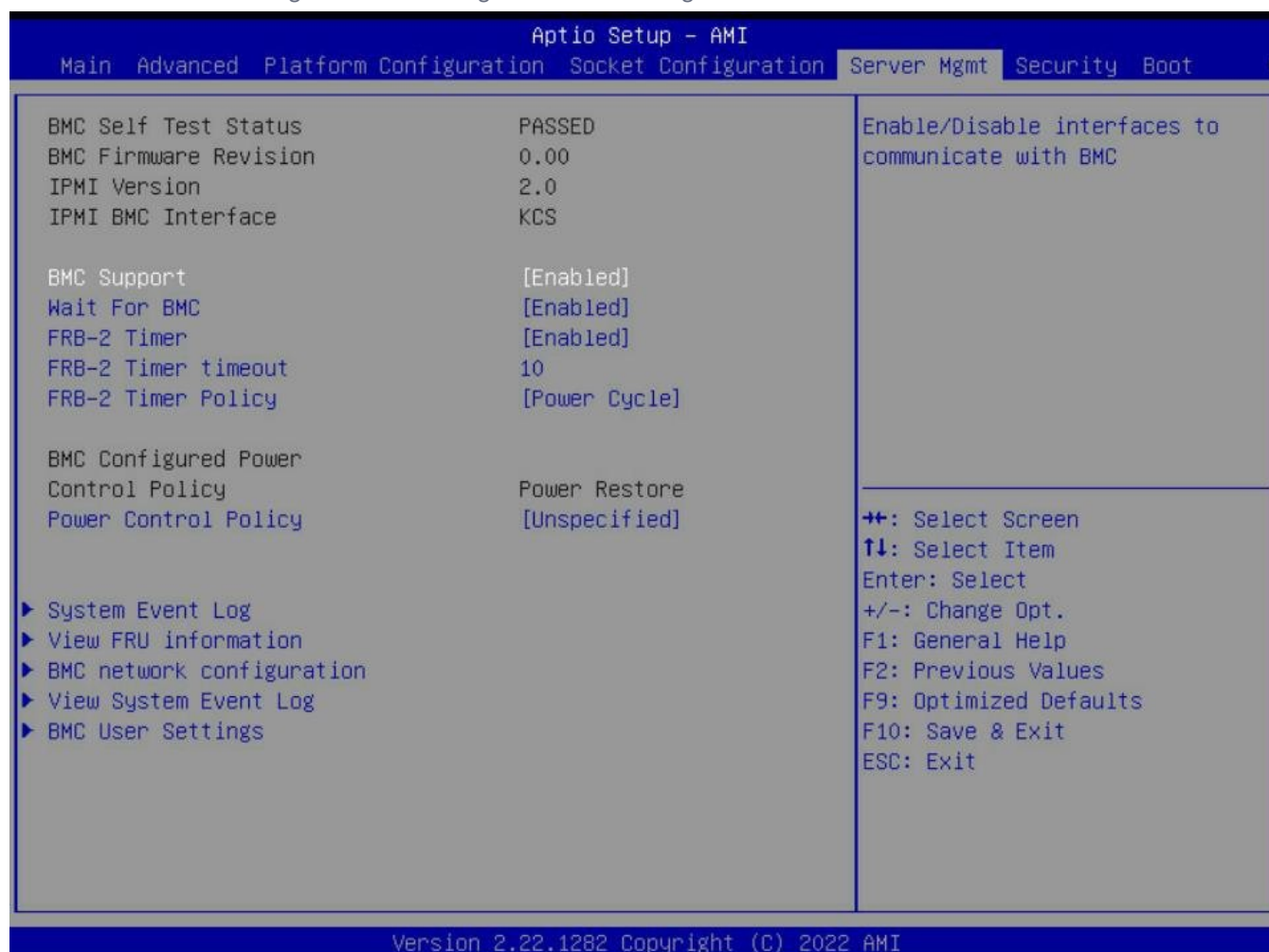


Figure 0-66 Server Mgmt

BIOS** ****Setting**	Options	Description
BMC Self-Test Status	Read Only	
BMC Device ID	Read Only	
BMC Device Revision	Read Only	

BMC Firmware Revision	Read Only	
IPMI Version	Read Only	
BMC Support	Enabled/Disabled	Enable/Disable interfaces to communicate with BMC
Wait For BMC	Enabled/Disabled	Wait For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.

BMC Firmware Revision	Read Only	
FRB-2 Timer	Enabled/Disabled	Enable or Disable FRB-2 timer (POST timer)
FRB-2 Timer timeout	10	Enter value Between 3 to 6 min for FRB-2 Timer Expiration value.
FRB-2 Timer Policy	Do Nothing/Reset/Power Down/Power Cycle	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.
BMC Configured Power Control Policy	Power Restore	
Power Control Policy	Unspecified/Do Not Power Up/Last Power State/Power Restore	Configure how the system should respond if AC Power is lost, Reset not required as selected Power policy will be set in BMC when policy is saved
System Event Log	Refer to for details.	Press F8 to change the SEL event log configuration.
View FRU information	Refer to for details.	Press F8 to view FRU information.
BMC network configuration	Refer to for details.	Configure BMC network parameters
View System Event Log	Refer to for details.	Press F8 to view the System Event Log Records.
BMC User Settings	Refer to for details.	Press F8 to Add, Delete and Set Privilege level for users.

Table 0-66 Server Mgmt

6.6. Security

6.6.1. Secure Boot



Рисунок 0-73 Secure Boot

Настройка BIOS	Опции	Описание
System Mode		Системный режим
Secure Boot	Enabled / Disabled	Функция Secure Boot активна, если Secure Boot включен (Enabled), Platform Key (PK) зарегистрирован, и система находится в режиме пользователя (User mode). Изменение режима требует сброса платформы.
Secure Boot Mode	Standard/Custom	Режим Secure Boot: Стандартный или Пользовательский. В

Настройка BIOS	Опции	Описание
		пользовательском режиме переменные политики Secure Boot могут быть настроены физически присутствующим пользователем без полной аутентификации.
Restore Factory Keys	См. подробнее	Принудительно перевести систему в User Mode. Установить заводские базы данных ключей Secure Boot по умолчанию.
Reset To Setup Mode		Сброс в режим настройки
Enter Audit Mode	См. подробнее	Войти в режим аудита (Audit Mode). Переход из User в Audit Mode приведет к стиранию переменной PK.
Key Management	См. подробнее	Позволяет опытным пользователям изменять переменные политики Secure Boot без полной аутентификации.
Image Execution Policy	См. подробнее	Управление политикой выполнения образов при нарушении безопасности.

Таблица 0-72 Secure Boot

6.6.2. Secure Flash Update



Рисунок 0-74 Secure Boot

6.6.0.0.1. Use the Security menu to set system and user passwords.

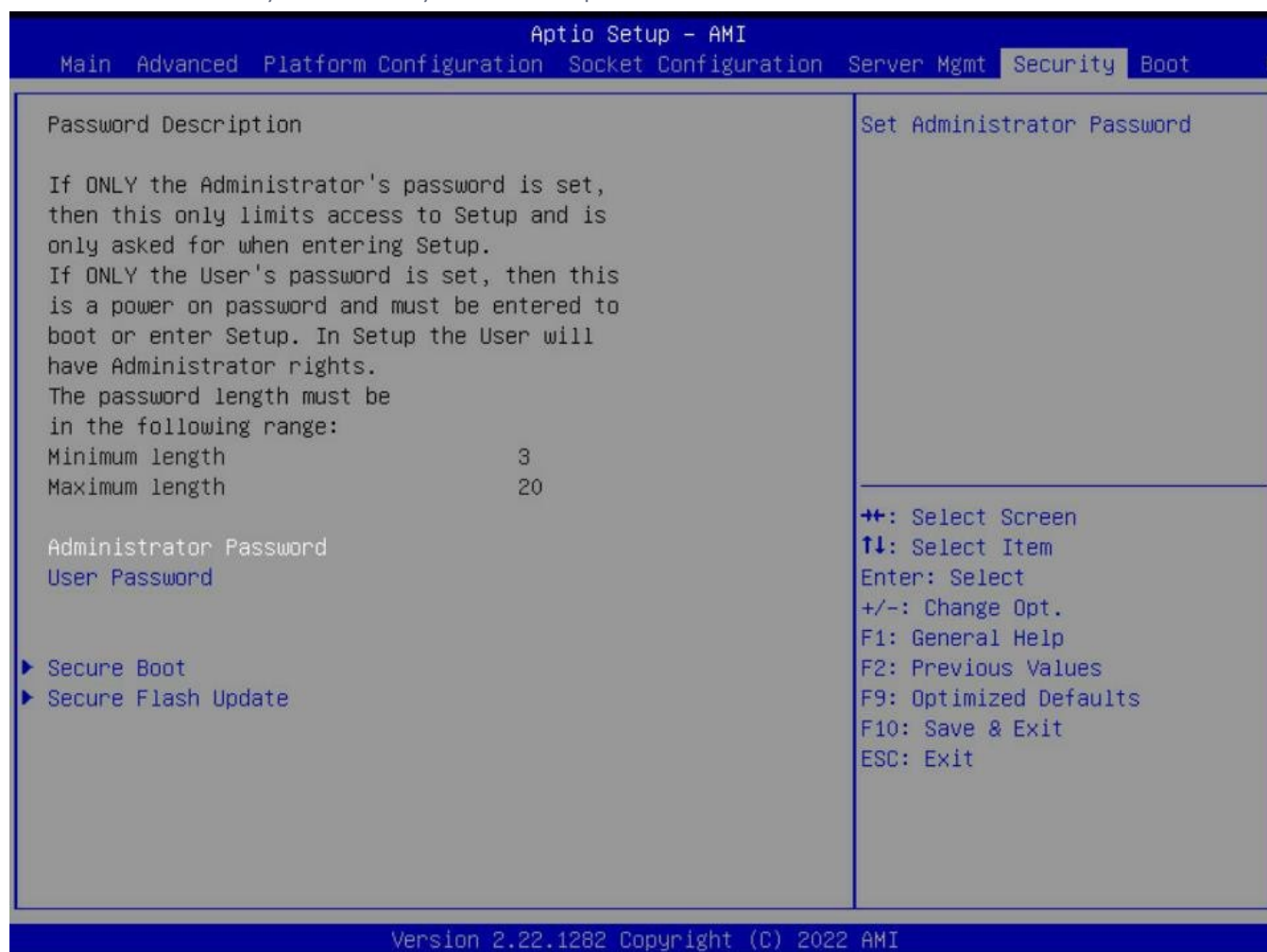


Figure 0-72 Security

BIOS** ****Setting**	Options	Description
Minimum length	Read Only	
Maximum length	Read Only	
Administrator Password		Set Administrator Password.
User Password		Set User Password.
Secure Boot	Refer to	Secure Boot configuration
Secure Flash Update	Refer to	Secure Flash Update support

Table 0-71 Security

6.7. Boot

6.7.0.0.1. Use the Boot menu to configure system boot options.

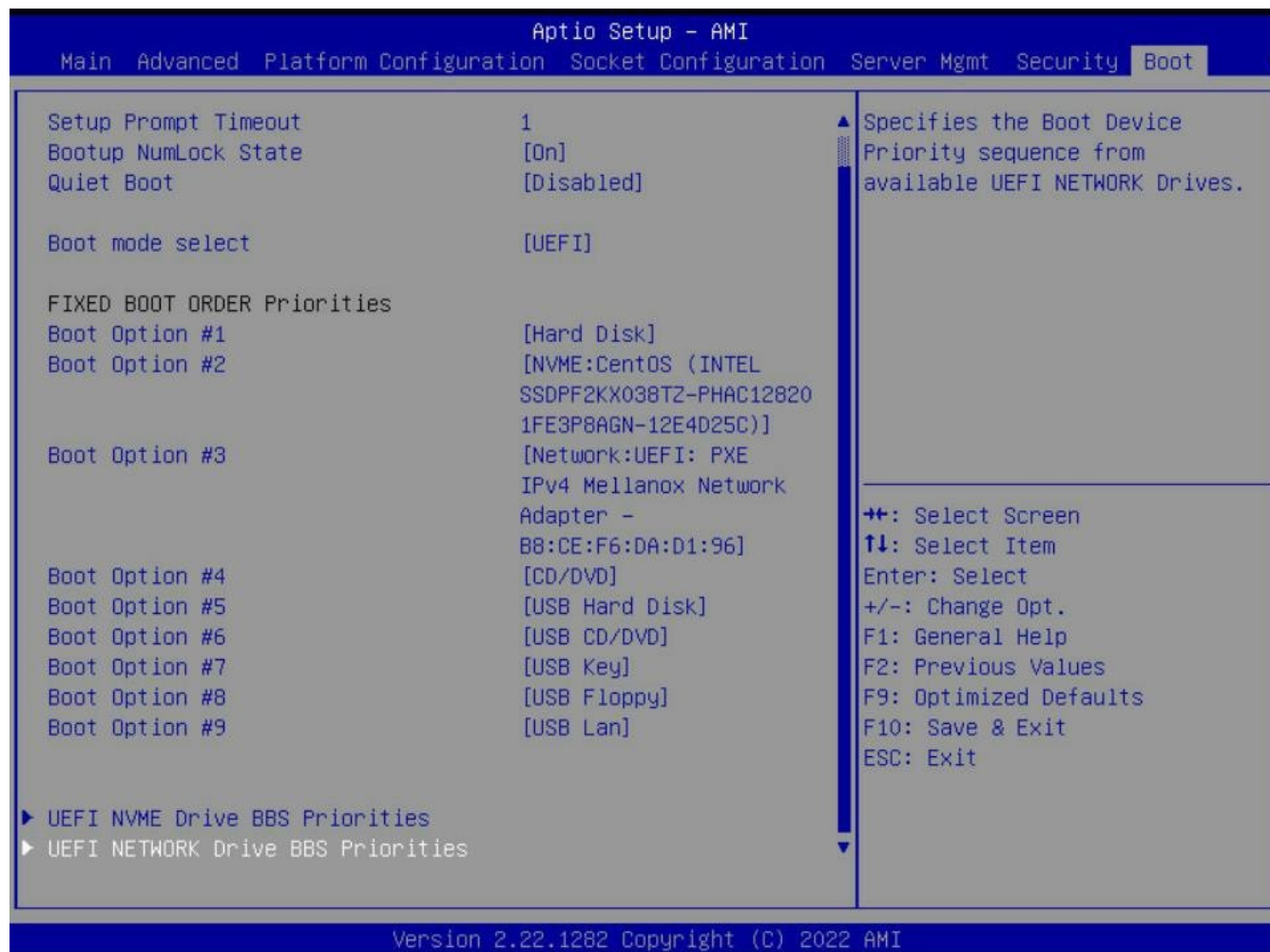


Figure 0-75 Boot

BIOS** ****Setting**	Options	Description
Boot Configuration	Boot Configuration	Boot Configuration
Setup Prompt Timeout	1	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	On/Off	Select the keyboard NumLock state.
Quiet Boot	Enabled/Disabled	Enables or disables Quiet Boot option.
Boot Mode Select	UEFI / Legacy	Select Boot Mode LEGACY Only/UEFI Only/UEFI and Legacy.
FIXED BOOT ORDERPriorities		
Boot Option #1Boot Option	[Hard Disk:CentOS Linux]	Sets the system boot order

BIOS** ****Setting**	Options	Description
#2Boot Option #3Boot Option #4	[Network] [CD/DVD] [OtherDevice]	
UEFI Hard Disk Drive BBS Priorities	Boot Option #1Boot Option #2	Specifies the Boot Device Priority sequence from available UEFI Hard Disk Drives.
UEFI Other Drive BBS Priorities	Boot Option #1Boot Option #2	Specifies the Boot Device Priority sequence from available UEFI Other Drives.

Table 0-73 Boot

6.8. Save & Exit

6.8.0.0.1. Use the Save & Exit menu to load default BIOS values, optimal failsafe values and to save configuration changes.

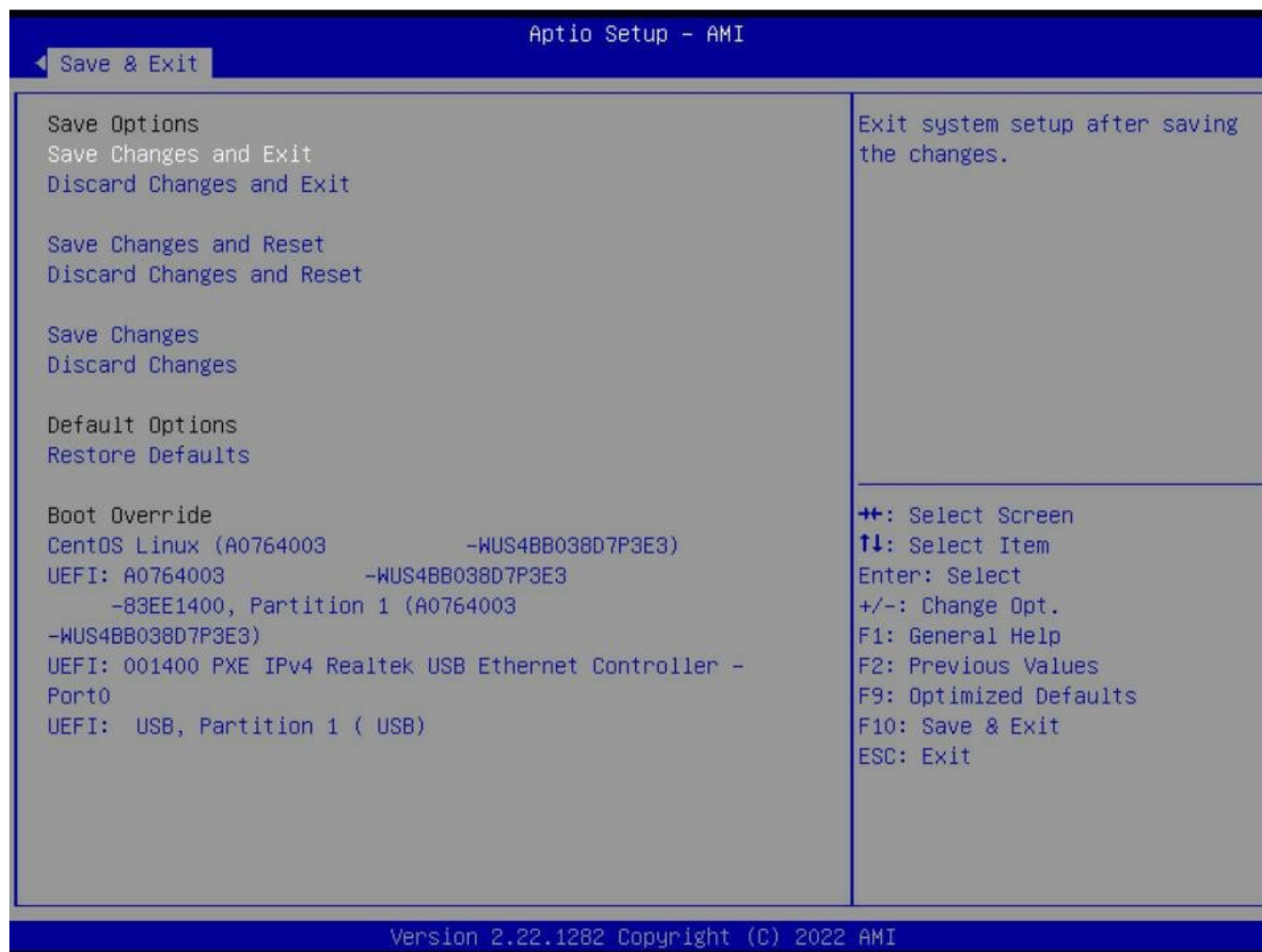


Figure 0-76 Save & Exit

BIOS** ****Setting**	Options	Description
Save Options	Save Options	Save Options
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Changes and Reset		Reset the system after saving the changes.
Discard Changes and reset		Reset system setup without saving any changes.
Save Changes		Save Changes done so far to any of the setup options.
Discard Changes		Discard Changes done so far to

BIOS** ****Setting**	Options	Description
		any of the setup options.
Default Options	Default Options	Default Options
Restore Defaults		Restore/Load Default values for all the setup options.
Boot Override:CentOS Linux(A0764003 - WUS4BB038D7P3E3)UEFI:A07 64003 -WUS4BB038D7P3E3 - 83EE1400,Partition 1(A0764003- WUS4BB038D7P3E3)	Boot Override:CentOS Linux(A0764003 - WUS4BB038D7P3E3)UEFI:A07 64003 -WUS4BB038D7P3E3 - 83EE1400,Partition 1(A0764003- WUS4BB038D7P3E3)	Boot Override:CentOS Linux(A0764003 - WUS4BB038D7P3E3)UEFI:A07 64003 -WUS4BB038D7P3E3 - 83EE1400,Partition 1(A0764003- WUS4BB038D7P3E3)

Table 0-74 Save & Exit

7. Обновление BIOS

7.1. Прошивка BIOS в UEFI Shell

Если система может загрузиться в UEFI shell, вы можете использовать инструмент AFU для прошивки BIOS в UEFI shell.

Скопируйте инструмент AMI Afuefi и прошивку BIOS в один каталог на USB-накопителе.

Проверьте расположение USB-накопителя, если расположение FS0, введите "FS0:"

Введите следующую команду для обновления: Afuefi BIOSFW.Bin /b /p /n /k.

Перезагрузите машину после завершения прошивки.

7.2. Прошивка BIOS в Windows

Загрузитесь в Windows.

Скопируйте Afuwin и прошивку BIOS в один каталог.

Введите следующую команду для обновления: Afuwin BIOSFW.Bin /b /p /n /k.

Перезагрузите машину после завершения прошивки.

7.3. Прошивка BIOS в Linux

Загрузитесь в Linux OS.

Скопируйте Afulnx и прошивку BIOS в один каталог.

Введите следующую команду для обновления: `Afulnx BIOSFW.Bin /b /p /n /k`.

Перезагрузите машину после завершения прошивки.

8. Контрольные точки

8.1. Фазы прошивки UEFI Framework

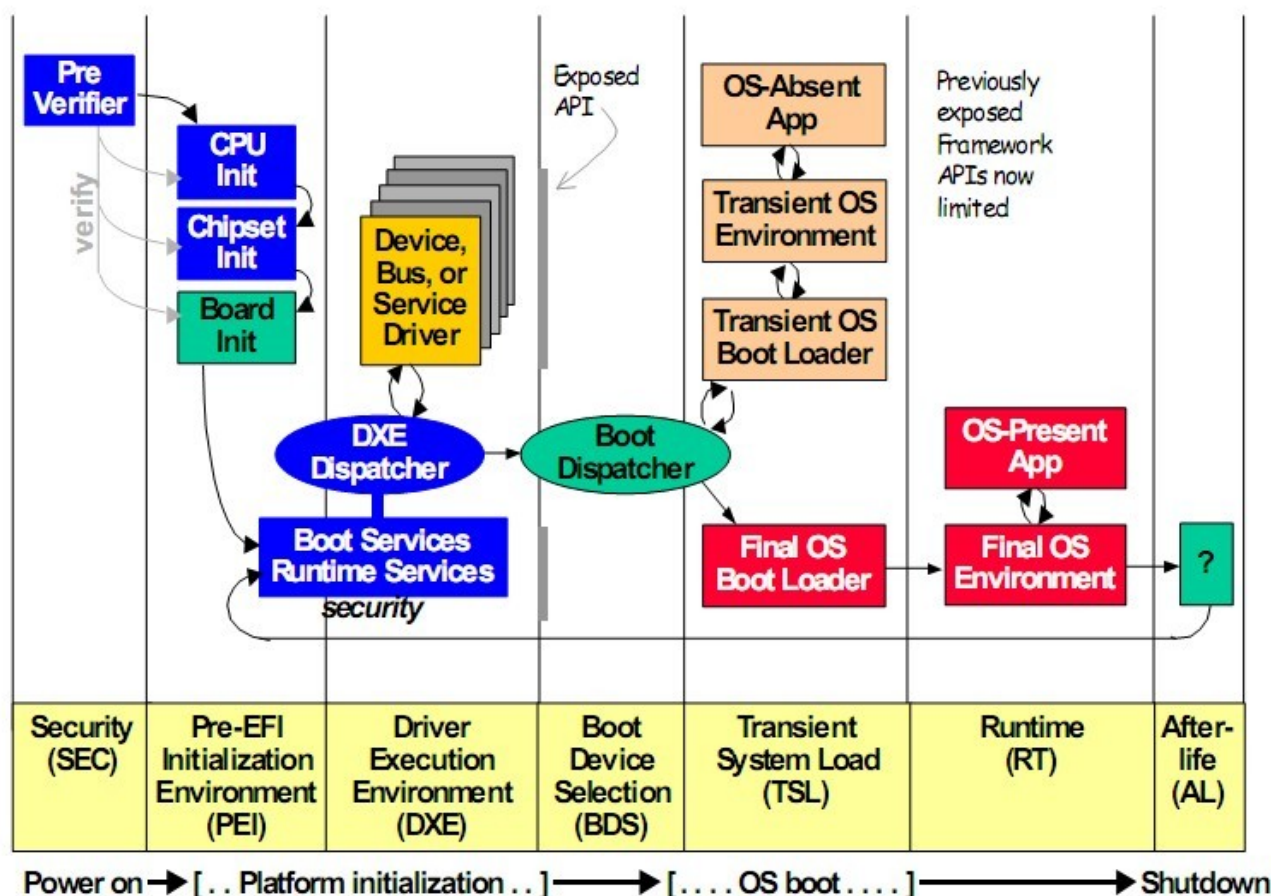


Рисунок 0-1

8.2. Контрольные точки AMI

8.2.1. Диапазоны контрольных точек AMI

Диапазон кода состояния	Описание
0x01 ~ 0x0B	Выполнение SEC
0x0C ~ 0x0F	Ошибка SEC
0x10 ~ 0x2F	Выполнение PEI до и включая обнаружение памяти
0x30 ~ 0x4F	Выполнение PEI после обнаружения памяти
0x50 ~ 0x5F	Ошибки PEI
0x60 ~ 0x8F	Выполнение DXE до BIOS
0x90 ~ 0xCF	Выполнение BDS
0xD0 ~ 0xDF	Ошибки DXE
0xE0 ~ 0xE8	Возобновление S3 (PEI)

8.2.2. AMI Security (SEC) Phase Initialization Code Checkpoints

Чекпойнт	Описание
Коды** ****прогресса**	Коды** ****прогресса**
0x01	Питание включено. Обнаружение типа сброса (мягкий/жесткий).
0x02	Инициализация AP до загрузки микрокода
0x03	Инициализация Северного моста до загрузки микрокода
0x04	Инициализация Южного моста до загрузки микрокода
0x05	Инициализация OEM до загрузки микрокода
0x06	Загрузка микрокода
0x07	Инициализация AP после загрузки микрокода
0x08	Инициализация Северного моста после загрузки микрокода
0x09	Инициализация Южного моста после загрузки микрокода
0x0A	Инициализация OEM после загрузки микрокода
0x0B	Инициализация кэша
Коды** ****ошибок**** ****SEC**	Коды** ****ошибок**** ****SEC**
0x0E	Микрокод не найден
0x0F	Микрокод не загружен
0xCA	Процессор не найден
0xCB	Сбой инициализации Un-core
0xCC	Не удалось включить доступ к CSRs
0xCD	Сбой загрузки микрокода

Чекпойнт	Описание
0xD0	Тест стека данных NEM не прошел

8.2.3. AMI Pre-EFI Initialization (PEI) Phase Initialization Code Checkpoints

Чекпойнт	Описание
Коды** ****прогресса**** ****PEI**	Коды** ****прогресса**** ****PEI**
0x10	PEI Core запущен
0x11	Начата инициализация CPU до памяти (Pre-memory)
0x12 ~ 0x14	Инициализация CPU до памяти (специфично для модуля CPU)
0x15	Начата инициализация NB/SB до памяти
0x16 ~ 0x18	Инициализация NB/SB до памяти (специфично для модуля NB/SB)
0x19	PEICAR_SB_INIT
0x1A ~ 0x1C	Зарезервировано для SB
0x1D ~ 0x2A	Зарезервировано для использования OEM
0x2B	PEI_MEMORY_SPD_READ
0x2C	PEI_MEMORY_PRESENCE_DETECT
0x2D	PEI_MEMORY_TIMING
0x2E	PEI_MEMORY_CONFIGURATION
0x2F	PEI_MEMORY_INIT
0x30	Зарезервировано для ASL
0x31	Память установлена
0x32	Начата инициализация CPU после памяти (Post-memory)
0x33	Инициализация CPU после памяти. Инициализация кэша
0x34	Инициализация CPU после памяти. Инициализация Application Processor(s) (AP)
0x35	Инициализация CPU после памяти. Выбор Boot Strap Processor (BSP)
0x36	Инициализация CPU после памяти. Инициализация System Management Mode (SMM)
0x37 ~ 0x3E	Инициализация NB/SB после памяти
0x3F ~ 0x4E	OEM коды инициализации после памяти
0x4F	DXE IPL запущен
Коды** ****ошибок**** ****PEI**	Коды** ****ошибок**** ****PEI**
0x50	Ошибка инициализации памяти. Неверный тип памяти или несовместимая скорость памяти

Чекпойнт	Описание
0x51	Ошибка инициализации памяти. Чтение SPD не удалось
0x52	Ошибка инициализации памяти. Неверный размер памяти или модули памяти не совпадают.
0x53	Ошибка инициализации памяти. Полезная память не обнаружена
0x54	Неспецифическая ошибка инициализации памяти.
0x55	Память не установлена
0x56	Неверный тип или скорость CPU
0x57	Несовпадение CPU
0x58	Самотестирование CPU не удалось или возможная ошибка кэша CPU
0x59	Микрокод CPU не найден или обновление микрокода не удалось
0x5A	Внутренняя ошибка CPU
0x5B	reset PPI недоступен
0x5C ~ 0x5F	Зарезервировано для будущих кодов ошибок AMI

Таблица 0-3 Коды чекпойнтов PEI

8.2.4. AMI Memory Reference Code Checkpoints

Чекпойнт	Описание
0xB0	STS_DIMM_DETECT: Обнаружение установки DIMM
0xB1	STS_CLOCK_INIT: Установка частоты DDR
0xB2	STS_SPD_DATA: Сбор оставшихся данных SPD
0xB3	STS_GLOBAL_EARLY: Программирование регистров на уровне контроллера памяти
0xB4	STS_RANK_DETECT: Оценка режимов RAS и сохранение информации о рангах
0xB5	STS_CHANNEL_EARLY: Программирование регистров на уровне канала
0xB6	STS_DDRIO_INIT: Последовательность инициализации DDRIO
0xB7	STS_DDR_CHANNEL_TRAINING: Тренировка DDR
0xB8	STS_INIT_THROTTLING: Инициализация CLTT/OLTT
0xB9	STS_MEMBIST: Аппаратный тест памяти и инициализация
0xBA	STS_MEMINIT: Выполнение инициализации памяти

Чекпойнт	Описание
0xBB	STS_DDR_MEMMAP: Программирование карты памяти и interleaving
0xBC	STS_RAS_CONFIG: Программирование конфигурации RAS
0xBD	STS_GET_MARGINS: Получение запасов (Margins)
0xBF	STS_MRC_DONE: MRC выполнен

Таблица 0-4 Коды чекпойнтов памяти

8.2.5. AMI Driver Execution Environment (DXE) Phase Initialization Code Checkpoints

Чекпойнт	Описание
Коды** ****прогресса**** ****DXE**	Коды** ****прогресса**** ****DXE**
0x60	DXE Core запущен
0x61	Инициализация NVRAM
0x62	Установка Runtime Services Южного моста
0x63 ~ 0x67	Инициализация CPU DXE (специфично для модуля CPU)
0x68	Инициализация PCI host bridge
0x69	Начата инициализация DXE Северного моста
0x6A	Начата инициализация DXE SMM Северного моста
0x6B ~ 0x6F	Инициализация DXE Северного моста (специфично для модуля Северного моста)
0x70	Начата инициализация DXE Южного моста
0x71	Начата инициализация DXE SMM Южного моста
0x72	Инициализация устройств Южного моста
0x73 ~ 0x77	Инициализация настроек DXE Южного моста (специфично для модуля Южного моста)
0x78	Инициализация модуля ACPI
0x79	Инициализация CSM
0x7A ~ 0x7F	Зарезервировано для будущих кодов AMI DXE
0x80 ~ 0x8F	ОЕМ коды инициализации DXE
0x90	Фаза выбора загрузочного устройства (BDS) начата
0x91	Подключение драйвера начато
0x92	Инициализация шины PCI начата
0x93	Инициализация контроллера Hot Plug шины PCI
0x94	Перечисление шины PCI (Enumeration)

Чекпойнт	Описание
0x95	Запрос ресурсов шины PCI
0x96	Назначение ресурсов шины PCI
0x97	Подключение устройств вывода консоли
0x98	Подключение устройств ввода консоли
0x99	Инициализация Super IO
0x9A	Инициализация USB начата
0x9B	Сброс USB
0x9C	Обнаружение USB
0x9D	Включение USB
0x9E ~ 0x9F	Зарезервировано для будущих кодов AMI
0xA0 ~ 0xA3	Инициализация IDE
0xA4 ~ 0xA7	Инициализация SCSI
0xA8	Проверка пароля Setup
0xA9	Начало Setup
0xAA	Зарезервировано для ASL
0xAB	Ожидание ввода Setup
0xAC	Зарезервировано для ASL
0xAD	Событие готовности к загрузке (Ready To Boot)
0xAE	Событие Legacy Boot
0xAF	Событие выхода из Boot Services
0xB0	Начало Runtime Set Virtual Address MAP
0xB1	Конец Runtime Set Virtual Address MAP
0xB2	Инициализация Legacy Option ROM
0xB3	Сброс системы (System Reset)
0xB4	Горячее подключение USB
0xB5	Горячее подключение шины PCI
0xB6	Очистка NVRAM
0xB7	Сброс конфигурации (сброс настроек NVRAM)
0xB8 ~ 0xBF	Зарезервировано для будущих кодов AMI
0xC0 ~ 0xCF	OEM коды инициализации BDS
Коды** ****ошибок**** ****DXE**	Коды** ****ошибок**** ****DXE**
0xD0	Ошибка инициализации CPU
0xD1	Ошибка инициализации Северного моста
0xD2	Ошибка инициализации Южного моста
0xD3	Некоторые архитектурные протоколы недоступны
0xD4	Ошибка выделения ресурсов PCI. Нет ресурсов
0xD5	Нет места для Legacy Option ROM
0xD6	Устройства вывода консоли не найдены

Чекпойнт	Описание
0xD7	Устройства ввода консоли не найдены
0xD8	Неверный пароль
0xD9	Ошибка загрузки Boot Option (LoadImage вернул ошибку)
0xDA	Сбой Boot Option (StartImage вернул ошибку)
0xDB	Сбой обновления прошивки (Flash update)
0xDC	Протокол сброса недоступен
0xDE ~ 0xDF	Зарезервировано для использования AMI

Таблица 0-5 Коды чекпойнтов DXE

8.2.6. AMI Recovery Code Checkpoints

Чекпойнт	Описание
0xF0	Условие восстановления вызвано прошивкой (Автоматическое восстановление)
0xF1	Условие восстановления вызвано пользователем (Принудительное восстановление)
0xF2	Процесс восстановления запущен
0xF3	Образ прошивки восстановления найден
0xF4	Образ прошивки восстановления загружен
Коды** ****ошибок**** ****восстановления**	Коды** ****ошибок**** ****восстановления**
0xF8	РРІ восстановления недоступен
0xF9	Капсула восстановления не найдена
0xFA	Неверная капсула восстановления
0xFB ~ 0xFF	Зарезервировано для будущих кодов ошибок AMI

Таблица 0-6 Коды чекпойнтов восстановления