БУЛАТ

РОССИЙСКИЙ ПРОИЗВОДИТЕЛЬ
ТЕЛЕКОММУНИКАЦИОННОГО
И ИТ-ОБОРУДОВАНИЯ

Инструкция по работе с BIOS

Сервер BS-202

В настоящей инструкции описаны сведения, необходимые для настройки и администрирования базовой системы ввода-вывода BIOS (Basic Input/Output System), и установлен порядок работы с BIOS для сервера BS-202.

Выпуск 1.0 / 11.2023

www.opk-bulat.ru

Товарные знаки

Логотип «БУЛАТ» БУЛАТ и другие товарные знаки ООО «БУЛАТ» являются зарегистрированными товарными знаками ООО «БУЛАТ».

Остальные товарные знаки, наименования изделий, услуг и компаний, упомянутые в настоящем документе, принадлежат их владельцам.

Примечание

Приобретаемое оборудование, услуги и конструктивные особенности обуславливаются договором, заключенным между ООО «БУЛАТ» и клиентом. Все или отдельные части оборудования, услуг и конструктивных особенностей, описываемых в данном документе, могут не входить в объем покупки или объем эксплуатации. Если иное не указано в договоре, все утверждения, рекомендации и иная содержащаяся в данном документе информация предоставляется «как есть» без каких-либо дополнительных гарантий или обязательств, явных или подразумеваемых.

Документ содержит текущую информацию на момент его издания, которая может быть изменена без предварительного уведомления. При подготовке документа были приложены все усилия для обеспечения достоверности информации, но все утверждения, сведения и рекомендации, приводимые в данном документе, не являются явно выраженной или подразумеваемой гарантией (истинности или достоверности). Внешний вид изделий может отличаться от представленного в настоящем документе.

ООО «БУЛАТ»

Адрес: Россия, 121471,
г. Москва, ул. Рябиновая, дом 26, строение 2

+7 (495) 870-30-44

sales@opk-bulat.ru

www.opk-bulat.ru

Содержание

1. Общие сведения

BIOS — система, предоставляющая API для работы с изделием и подключаемыми устройствами. Одним из основных назначений BIOS является инициализация и тестирование изделия при запуске.

У BIOS есть специальное меню настройки — InsydeH20 Setup Utility, которое представляет интерфейс для настройки.

1.1. Содержание «InsydeH20 Setup Utility»

«InsydeH20 Setup Utility» состоит из следующих основных разделов и подразделов:

- «Main»:

  1) «System Time»;
  2) «System Date»;

- «Advanced»:

  1) «Peripheral Configuration»;
  2) «Video Configuration»;
  3) «OEMBOARD Function»;
  4) «S10 AST2500»;
  5) «Socket Configuration»;
  6) «ME Configuration»;
  7) «Pch Configuration»;
  8) «H2O IPMI Configuration»;
  9) «APEI Configuration»;
  10) «H20 Event log Config Manager»;
  11) «Console Redirection»;
  12) «H2oUve Configuration»;

- «Security»:

  1) «Current TPM Device»;
  2) «TPM State»;
  3) «TPM Active PCR Hash Algorithm»;
  4) «TPM Hardware Supported Hash Algorithm»;
  5) «TrEE Protocol Version»;
  6) «TPM Availability»;
  7) «TPM Operation»;
  8) «Clear TPM»;
  9) «Supervisor Password»;
  10) «Set Supervisor Password»;
  11) «Platform Hierarchy Policy»;

- «Power»:

  1) «Wake on PME»;

- «Boot»:

  1) «Boot Type»;
  2) «Quick Boot»;

3) «Quiet Boot»;
4) «Network Stack»;
5) «PXE Boot capability»;
6) «Add Boot Options»;
7) «ACPI Selection»;
8) «USB Boot»;
9) «EFI Device First»;
10) «Timeout Automatic Failover»;
11) «EFI»;
12) «Legacy»;

- «Exit»:

1) «Exit Saving Changes»;
2) «Save Change Without Exit»;
3) «Exit Discarding Changes»;
4) «Load Optimal Defaults»;
5) «Load Custom Defaults»;
6) «Save Custom Defaults»;
7) «Discard Changes».

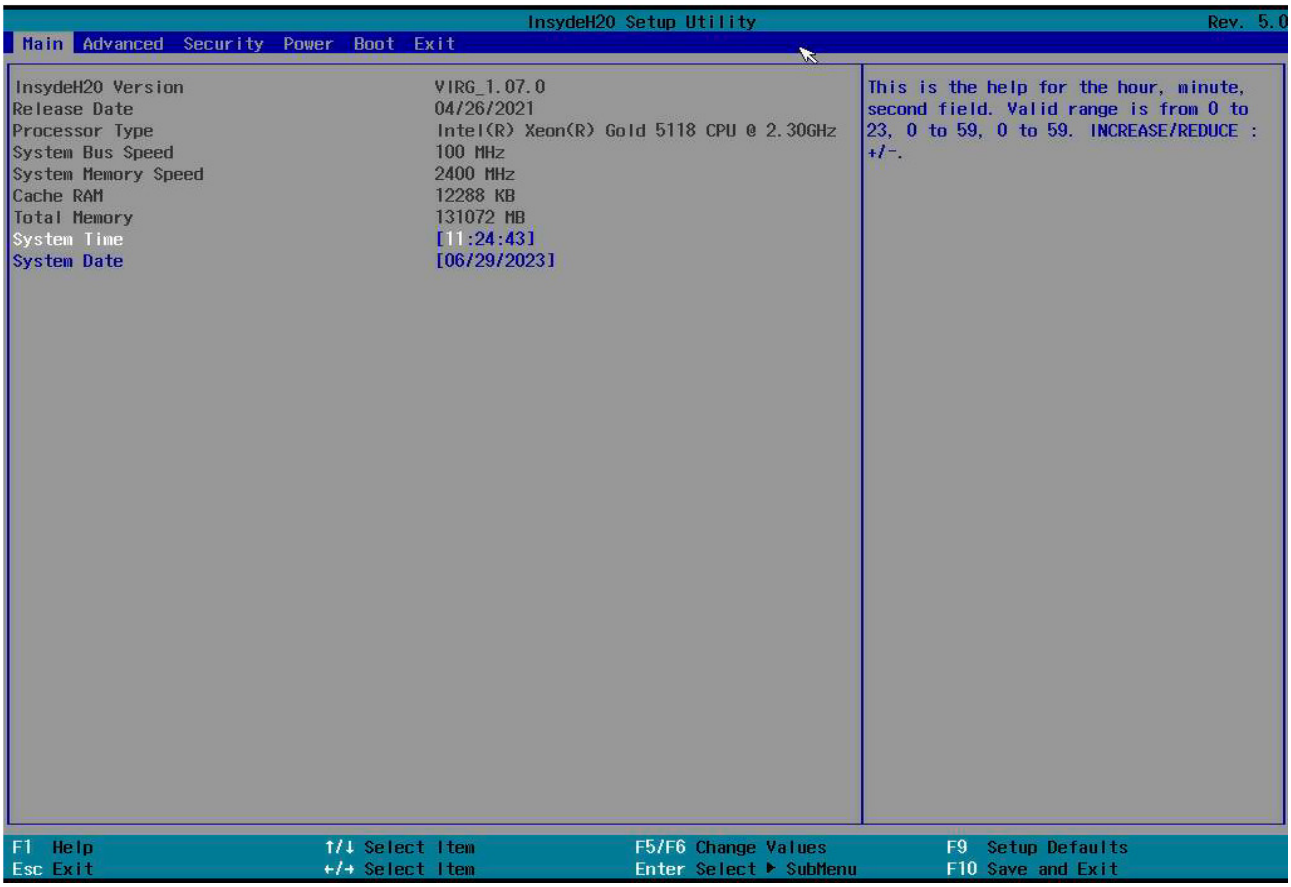
2. Описание функций и настроек

2.1. «Main»

Вкладка «Main» содержит следующую основную информацию о системе и позволяет установить настройки (рисунок 2.1):

- «InsydeH20 Version» — версия BIOS;
- «Release Date» — установленная дата;
- «Processor Type» — тип процессора;
- «System Bus Speed» — скорость шины;
- «System Memory Speed» — скорость памяти;
- «Cache RAM» — объем оперативной памяти;
- «Total Memory» — объем доступного хранилища;
- «System Time» — установка времени системы в формате [чч:мм:сс];
- «System Date» — установка даты системы в формате [мм/дд/гггг].

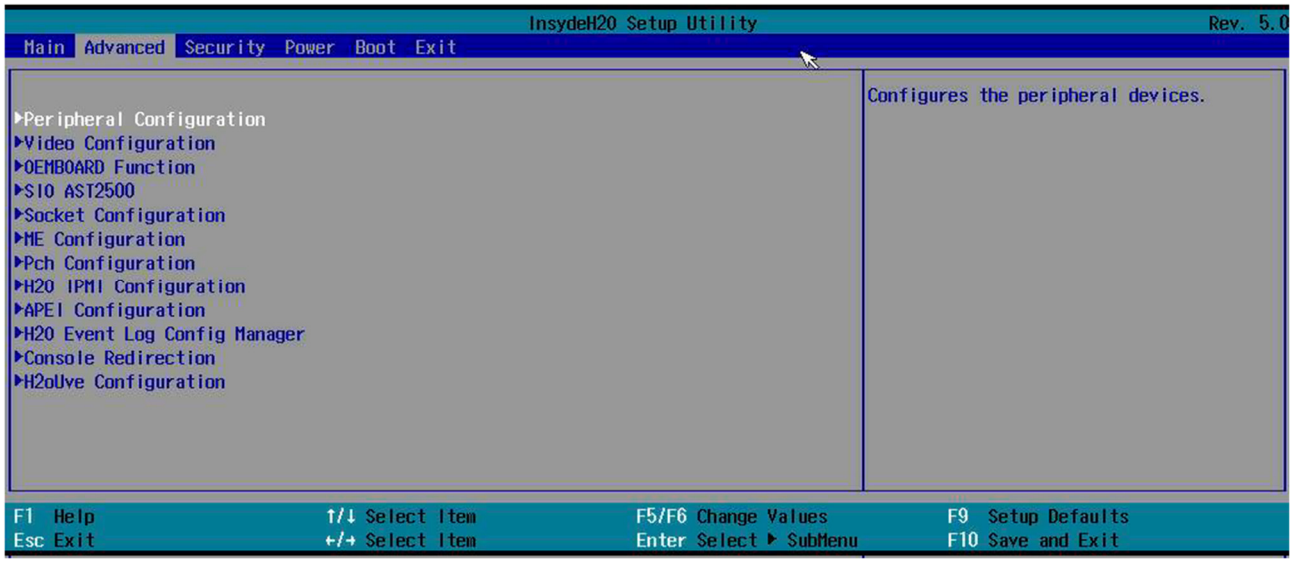
Рисунок 2.1. Вкладка «Main»



2.2. «Advanced»

Вкладка «Advanced» содержит расширенные настройки. Общий вид окна вкладки приведен на рисунке 2.2.

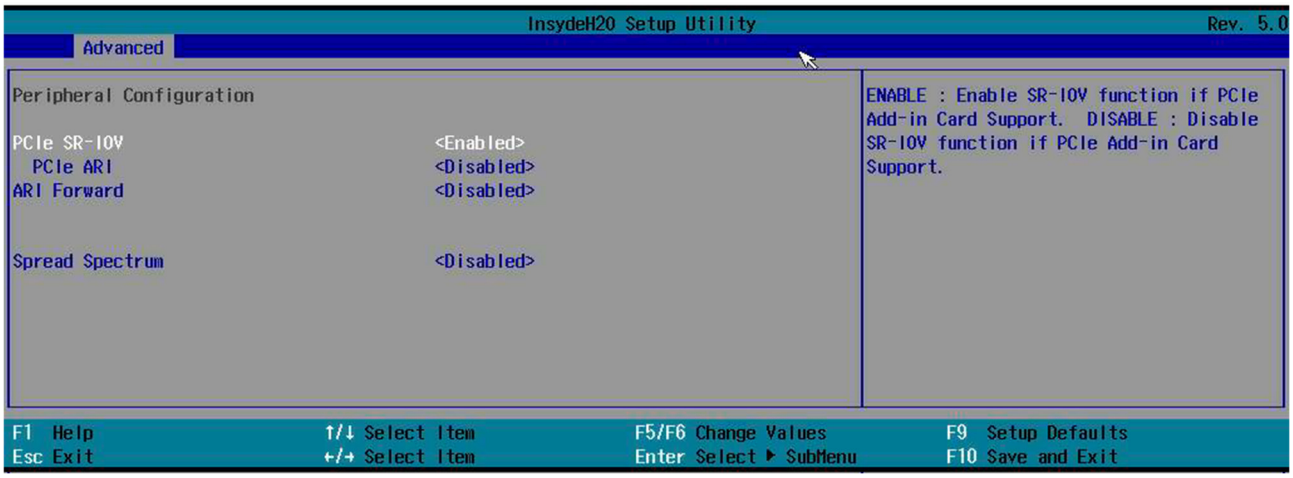
Рисунок 2.2. Вкладка «Advanced»



2.2.1. «Peripheral Configuration»

Настройка периферийных устройств (рисунок 2.3).

Рисунок 2.3. «Peripheral Configuration»



В окне на рисунке 2.3:

- «PCIe SR-IOV». SR-IOV — виртуализация ввода-вывода с единым корнем. Включить: включить функцию SR-IOV, если поддерживается карта расширения PCIe. Отключить: отключить функцию SR-IOV, если поддерживается карта расширения PCIe;
- «PCIe ARI». Alternate Routing ID позволяет изменить представление устройства PCIe для операционной системы (ОС) — вместо одного физического может быть представлено до 256 виртуальных, каждое из которых программой виртуализации будет восприниматься как полноценное физическое устройство. Позволяет включить или выключить возможность альтернативного идентификатора маршрута;
- «ARI Forward» — позволяет включить или выключить проброс альтернативного идентификатора маршрута;

- «Spread Spectrum» — распределение спектра электромагнитного излучения. Предназначено для регулирования уровня электромагнитного излучения, испускаемого различными компонентами, прежде всего генератором тактового сигнала. Включение данной опции может быть оправдано лишь в том случае, если есть серьезные проблемы с высоким уровнем электромагнитного излучения, исходящего от электронных компонентов, и необходимо уменьшить уровень помех, влияющих на окружающие электронные приборы и устройства.

2.2.2. «Video Configuration»

Настройка устройств вывода видеосигнала (рисунок 2.4).

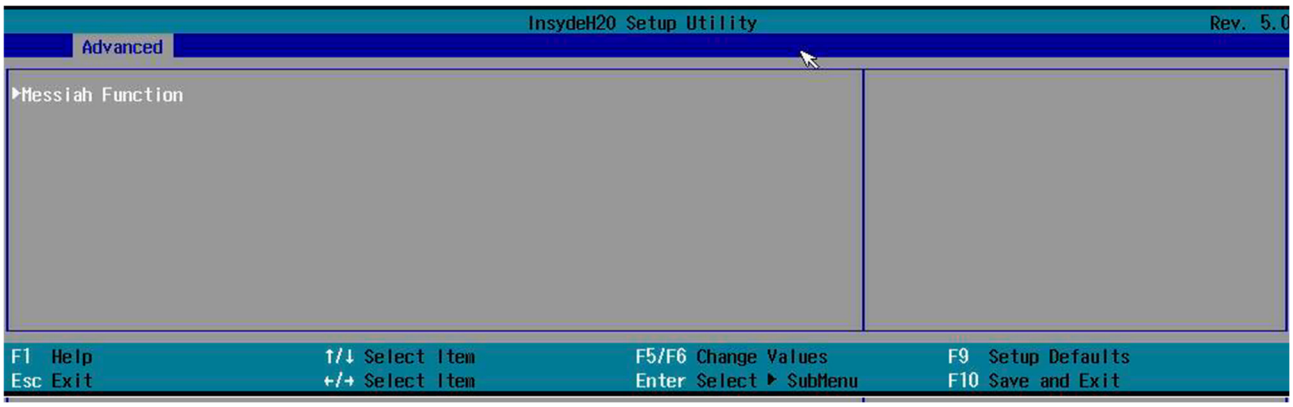
Рисунок 2.4. «Video Configuration»

2.2.2.1. «Display Mode» — выбор приоритета использования устройств.

2.2.3. «OEMBOARD Function»

Функции платы от оригинального производителя оборудования (рисунок 2.5).

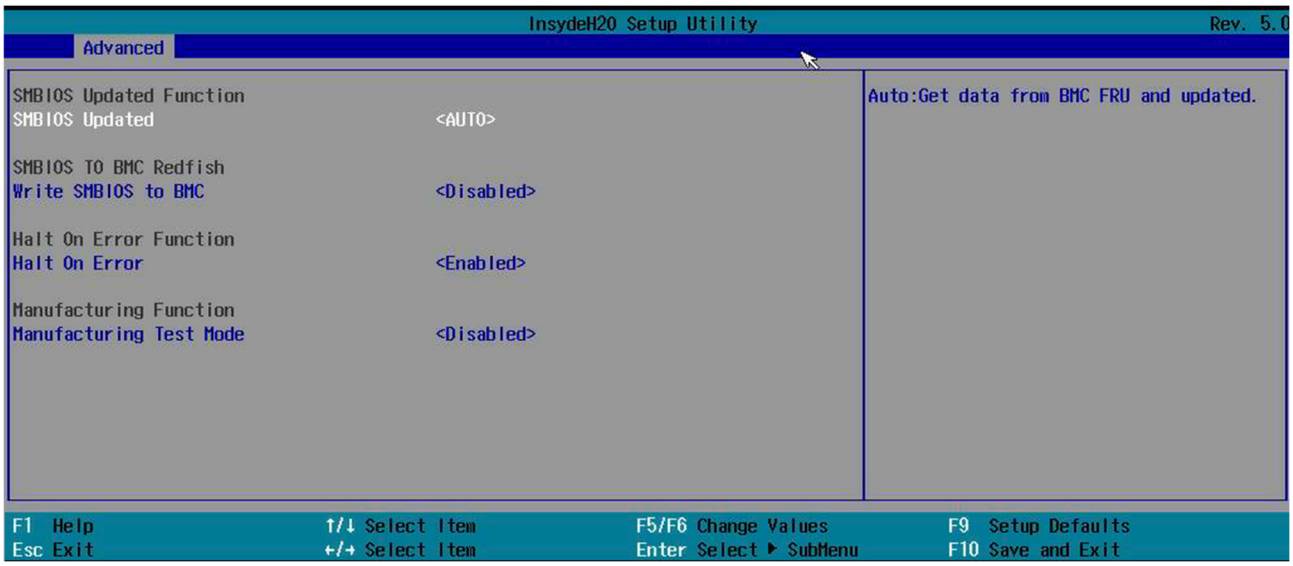
Рисунок 2.5. «OEMBOARD Function»



2.2.3.1. «Messiah Function» — системное управление BIOS (рисунок 2.6):

- «SMBIOS Updated Function» — обновление системного управления BIOS;
- «SMBIOS TO BMC Redfish» — перенаправление вывода системного управления в BMC;
- «Halt On Error Function» — управление поведением системы в случае возникновения некритической ошибки во время загрузки персонального компьютера (ПК).

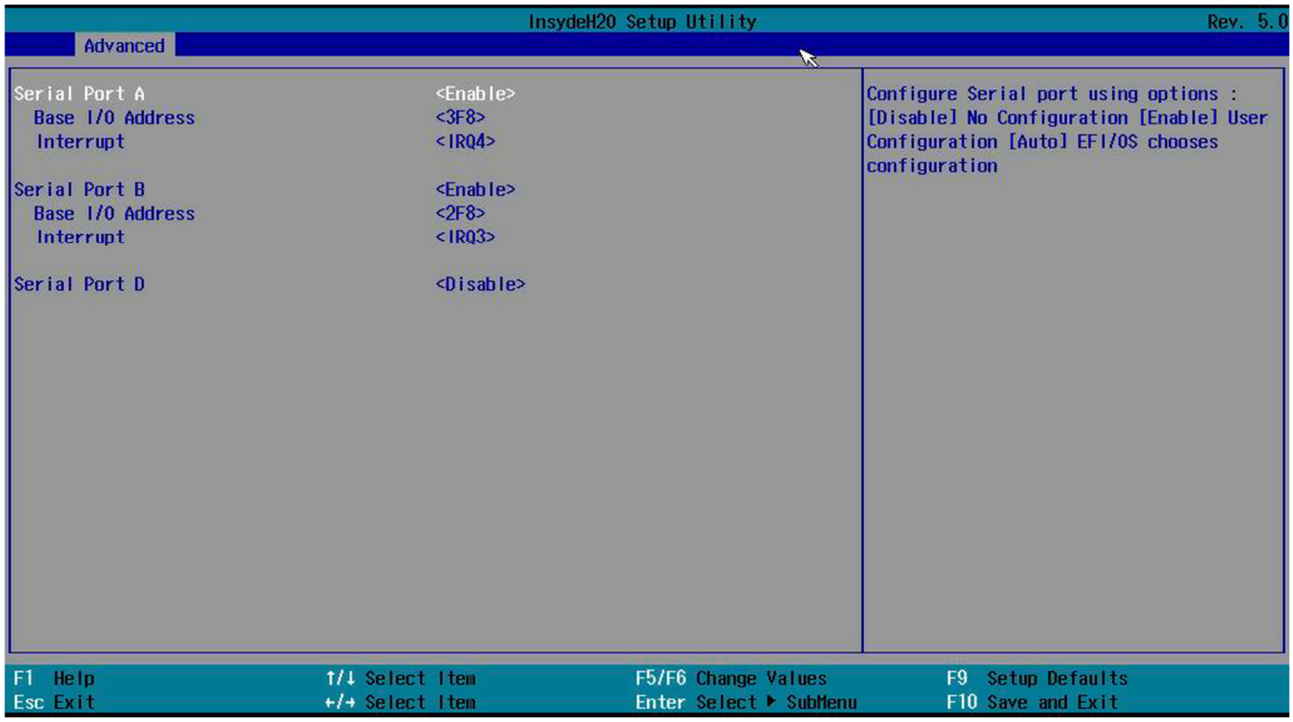
Рисунок 2.6. «Messiah Function»



2.2.4. «SI0 AST2500»

Настройка контроллера ввода-вывода (рисунок 2.7).

Рисунок 2.7. «SI0 AST2500»



В окне, представленном на рисунке 2.7:

- «Serial Port A» — настройка порта, используя следующие опции:
  - отключено: настройки отключены;
  - включено: пользовательские настройки;
  - авто: EFI/OS выбирают настройки;
  - настройка адреса;
  - прерывание;
- «Serial Port B» — настройка порта, используя следующие опции:
  - отключено: настройки отключены;

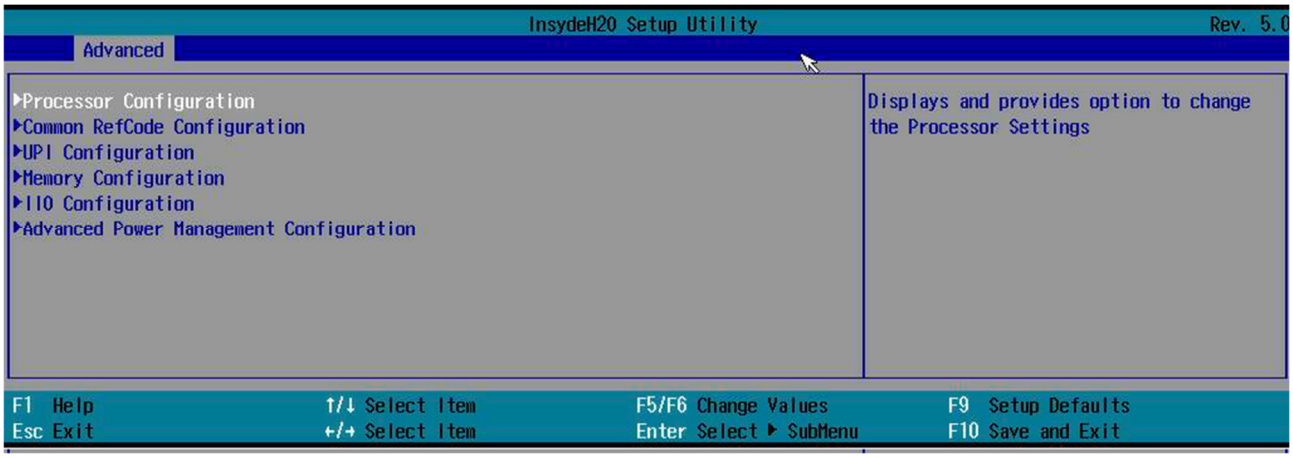
- включено: пользовательские настройки;
- авто: EFI/OS выбирают настройки;
- настройка адреса;
- прерывание;

- «Serial Port D».

2.2.5. «Socket Configuration»

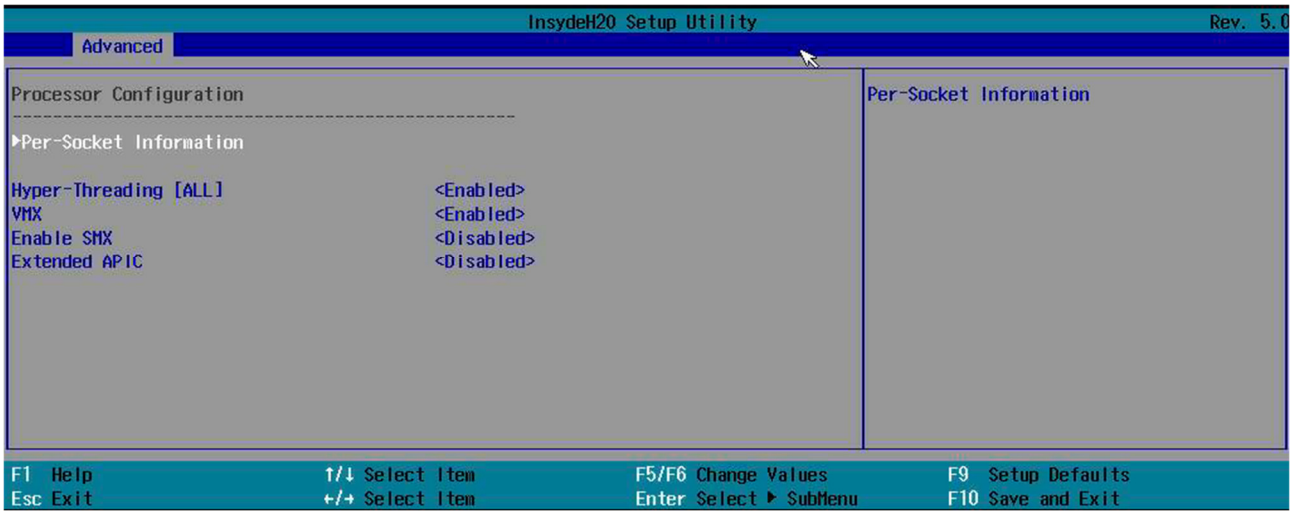
«Socket Configuration» показывает и дает возможность изменить настройки сокета (рисунок 2.8).

Рисунок 2.8. «Socket Configuration»



2.2.5.1. «Processor Configuration» — показывает и дает возможность изменить настройки процессора (рисунок 2.9).

Рисунок 2.9. «Processor Configuration»

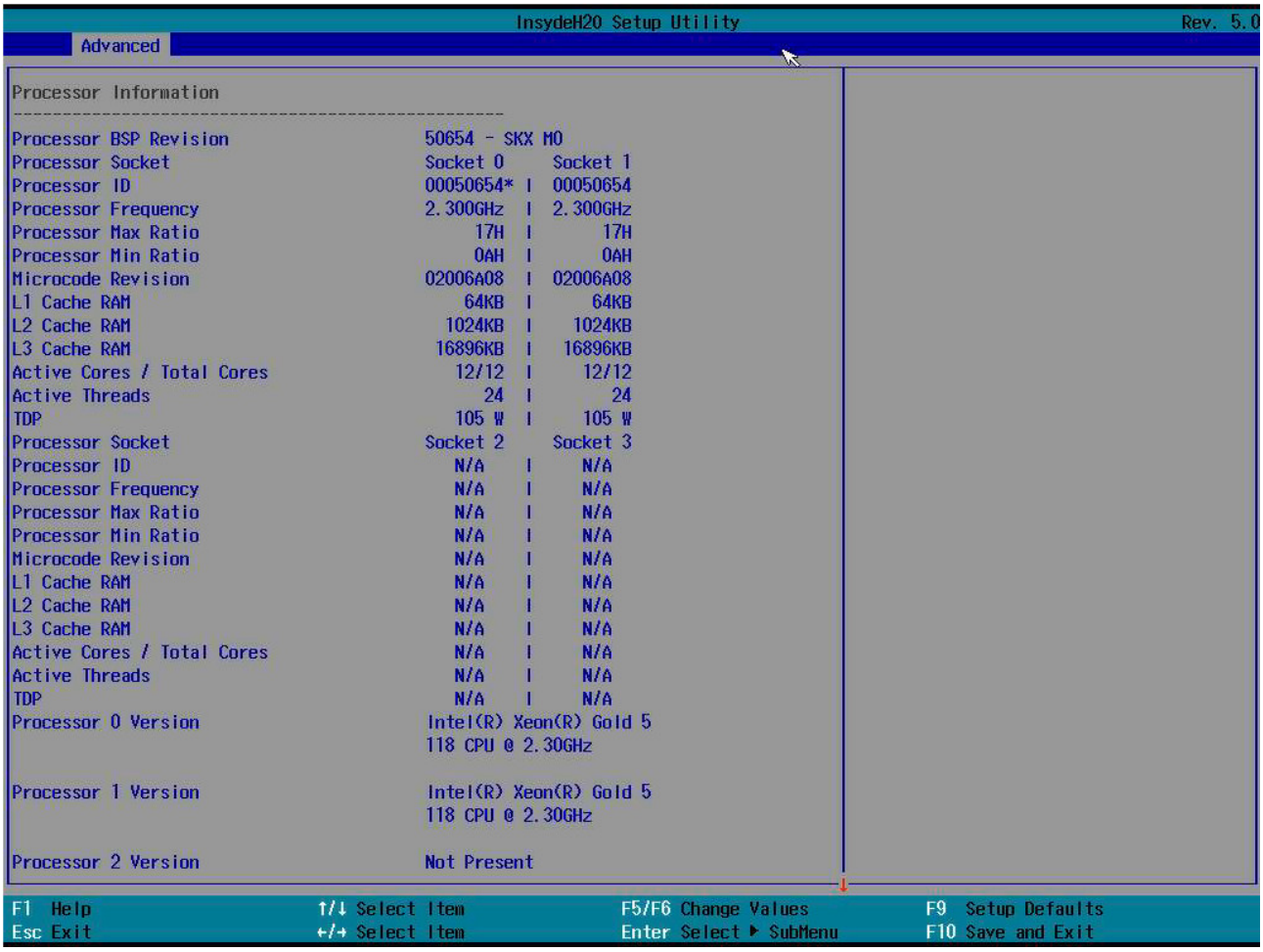


В окне на рисунке 2.9:

- «Per-Socket Information» — информация для каждого сокета (рисунок 2.10). Содержит следующие данные:
  - «Processor BSP Revision» — ревизия процессора;
  - «Processor Socket» — сокет;
  - «Processor ID» — идентификатор процессора;
  - «Processor Frequency» — частота процессора;
  - «L1 Cache RAM» — кэш первого уровня;

- «L2 Cache RAM» — кэш второго уровня;
- «L3 Cache RAM» — кэш третьего уровня;
- «Active Cores / Total Cores» — активные ядра/всего ядер;
- «Active Threads» — количество активных потоков;
- «TDP» — тепловыделение;

Рисунок 2.10. «Per-Socket Information»



- «Hyper-Threading [ALL]» — сверхпоточность или гиперпоточность. Опция позволяет включить или выключить в BIOS поддержку одноименной технологии Intel;
- «VMX» — аппаратная виртуализация. Виртуализация с поддержкой специальной процессорной архитектуры. В отличие от программной виртуализации с помощью данной техники возможно использование изолированных гостевых ОС, управляемых гипервизором напрямую. Гостевая ОС не зависит от архитектуры хостовой платформы и реализации платформы виртуализации;
- «Enable SMX» — расширения безопасного режима. Расширение системы команд 64- и 32-битных процессоров Intel (архитектур Intel 64 и IA-32), которое предоставляет интерфейс программирования для создания контролируемой доверенной среды у конечных пользователей;
- «Extended APIC» — расширенный контроллер прерываний. Опция отвечает за включение расширенного контроллера прерываний (APIC — Advanced Programmable Interrupt Controller). Следует учитывать, что расширенный контроллер прерываний является подсистемой расширенного конфигурирования и управления питанием (ACPI). Если отключить ACPI, придется отказаться и от использования расширенного контроллера прерываний.

2.2.5.2. «Common RefCode Configuration» — эталонный (референсный) код памяти (рисунок 2.11).

Это часть встроенного программного обеспечения (ПО) материнской платы на базе чипсета Intel, которая определяет, как в оперативной памяти компьютера будут проходить процедуры записи и чтения информации с учетом эффектов любых модификаций, установленных пользователем или компьютерным оборудованием.

MRC отвечает за инициализацию памяти как часть постпроцесса (POST) после включения питания компьютера, при его загрузке. Физически MRC является частью BIOS (UEFI) материнской платы на чипсете Intel.

MRC является частью эталонного кода BIOS, который относится к инициализации памяти в BIOS. Он включает в себя информацию о настройках памяти, частоте, времени, управлении и подробных операциях контроллера памяти.

Рисунок 2.11. «Common RefCode Configuration»

В окне на рисунке 2.11:

- «MMCFG Size» — MM — memory mapped. Устройства, регистры которых адресуются как ячейки памяти;
- «MMIO High Base» — количество сегментов, размер которых устанавливается MMIO High Granularity Size. Если параметр MMIO High Base будет установлен в 56T, то нельзя будет установить параметр MMIO High Granularity Size равным 1024G, поскольку адресация выйдет за пределы диапазона;
- «MMIO High Granularity Size» — количество гигабайт на 1 сегмент, который устанавливается MMIO High Base. Если параметр будет установлен в 1024G, то нельзя будет установить параметр MMIO High Base равным 56T, поскольку адресация выйдет за пределы диапазона;
- «Serial Debug Message Level» — параметр устанавливает уровень сообщений об ошибках, которые направляются через последовательный порт:
  - Disabled — никаких сообщений об ошибках отправляться не будет;
  - Minimum — будут отправляться сообщения только о критических ошибках;
  - Normal — будут отправляться информационные и критические сообщения;
  - Maximum — будут отправляться все типы сообщений.

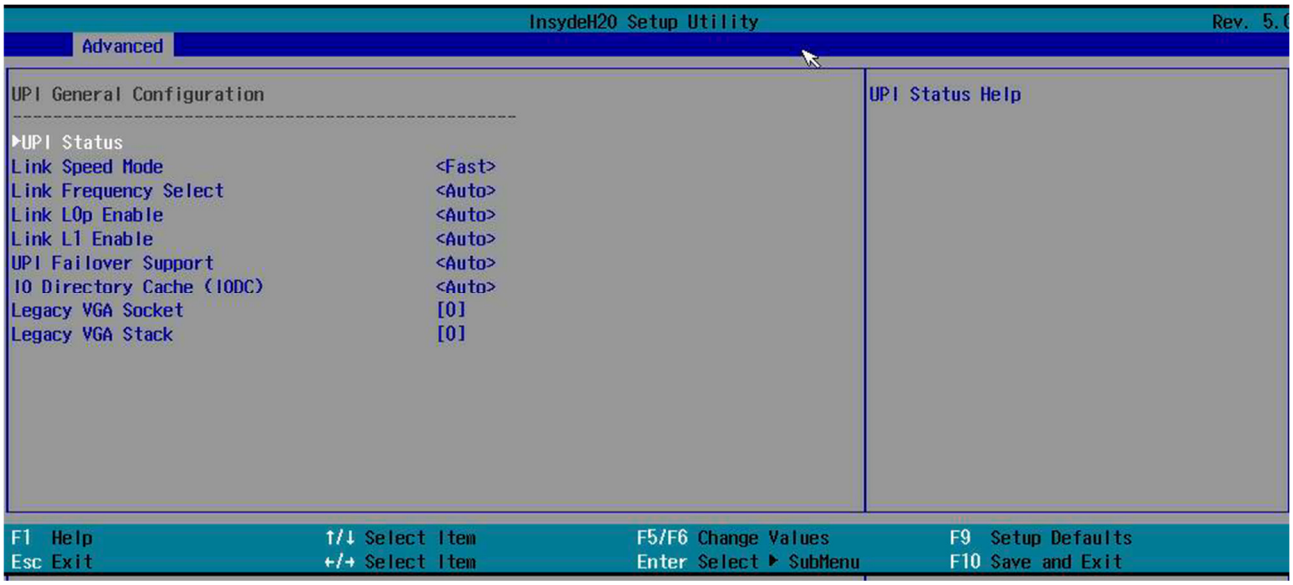
2.2.5.3. «UPI Configuration» — раздел параметров, отвечающих за настройку UPI.

Ultra Path Interconnect — сверхбыстрая межпроцессорная связь (шина, предназначенная для обеспечения взаимодействия между процессорами). Используется в серверных платформах на базе процессоров Intel.

«UPI General Configuration» — основные настройки Ultra Path Interconnect (рисунок 2.12):

- «UPI Status» — раздел, показывающий информацию об интерфейсе UPI:
  - количество процессоров;
  - количество интерфейсов ввода-вывода;
  - текущая скорость соединения UPI;
  - текущая частота соединения UPI;
  - нижнее ограничение количества сегментов Memory Mapped Input Output;
  - верхнее ограничение количества сегментов Memory Mapped Input Output;
  - базовая настройка размера Ultra Path Interconnect PCIe;

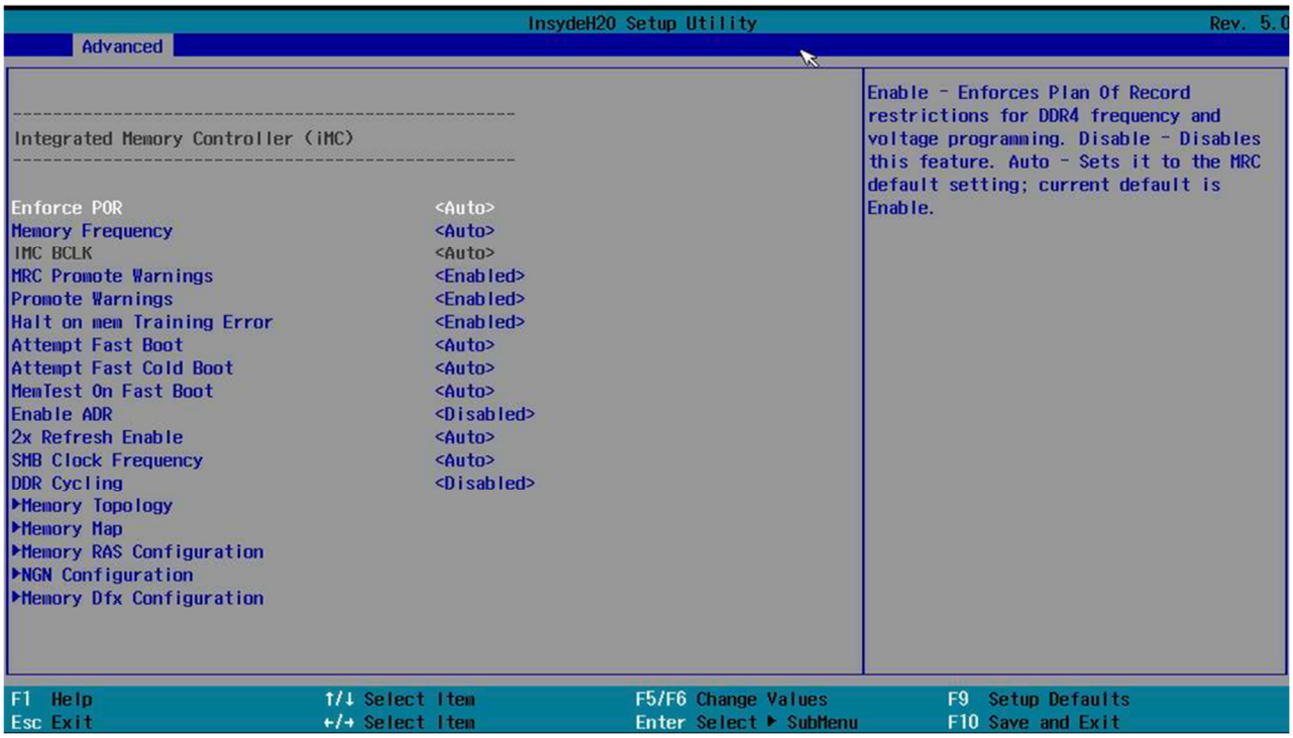
Рисунок 2.12. «UPI General Configuration»



- «Link Speed Mode» — настройка скорости соединения UPI;
- «Link Frequency Select» — настройка частоты соединения UPI;
- «Link L0p Enable» — параметр включает/выключает применение режима энергосбережения L0p для интерфейса UPI;
- «Link L1 Enable» — параметр включает/выключает применение режима энергосбережения L1p для интерфейса UPI;
- «UPI Failover Support» — поддержка отказоустойчивости UPI;
- «IO Directory Cache» (IODC) — параметр «IO Direct Cache» используется для настройки одноранговой сериализации PCI. В некоторых конфигурациях, например в системах с несколькими графическими процессорами на одном процессорном сокете, производительность может повыситься, если функция включена;
- «Legacy VGA Socket» — сокет, который устанавливает диапазон допустимых значений Legacy VGA;
- «Legacy VGA Stack» — множество, которое устанавливает диапазон допустимых значений Legacy VGA.

2.2.5.4. «Memory Configuration» — конфигурация памяти (рисунок 2.13).

Рисунок 2.13. «Memory Configuration»



«Enforce POR» — включение позволяет применить ограничения Plan Of Record для программирования частоты и напряжения DDR4. Скорость памяти будет ограничена рекомендациями Intel.

«Memory Frequency» — частота работы памяти.

«IMC BCLK» — Integrated Memory Controller Base Clock. Позволяет установить соотношение между частотой работы базовой шины и частотой оперативной памяти.

«MRC Promote Warnings» — определяет, передаются ли предупреждения MRC на системный уровень.

«Halt on mem Training Error» — управляет поведением системы в случае возникновения некритической ошибки во время загрузки.

«Attempt Fast Boot» — параметр ПО BIOS, который позволяет ускорить запуск ОС.

«Attempt Fast Cold Boot» — параметр ПО BIOS, который позволяет ускорить холодный запуск ОС (из выключенного состояния).

«MemTest On Fast Boot» — проверка памяти при быстром запуске.

«Enable ADR» — разрешение ускоренного восстановления баз данных.

«2x Refresh Enable» — частота обновления памяти. Относится к категории опций BIOS, предназначенных для настройки параметров работы оперативной памяти.

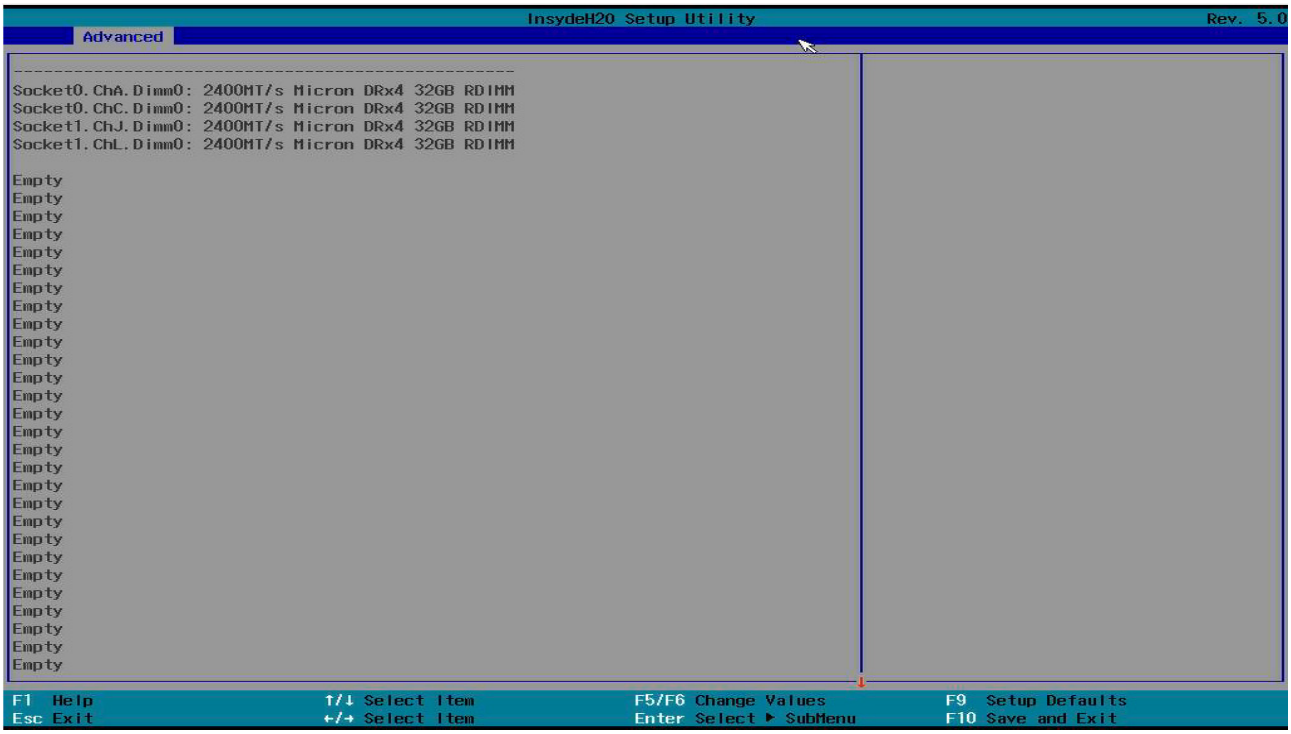
«SMB Clock Frequency» — тактовая частота системной шины определяется в диапазоне 10–100 кГц, тогда как I^2C может быть в диапазоне 0–100 кГц, 0–400 кГц, 0–1 МГц и 0–3,4 МГц в зависимости от режима. Это означает, что шина I^2C, работающая на частоте менее 10 кГц, не будет совместима с SMBus, поскольку время ожидания устройств SMBus может истечь.

«DDR Cycling» — устанавливает задержку в тактах между выдачей сигнала CAS и началом чтения данных (параметр tCL в диаграмме доступа). Для большинства качественных модулей

памяти типа SDRAM стандарта PC66, PC100 и PC133 можно установить значение 2. Если стабильная работа в этом случае не обеспечивается, необходимо снизить значение опции до 3. Для современных модулей памяти DDR SDRAM это значение равно 2,0; 2,5 или 3,0. Модули DDR2 SDRAM и DDR3 SDRAM характеризуется в среднем несколько большим значением: от 3,0 до 6,0 и от 6,0 до 10,0 соответственно. Если присутствует вариант Auto или By SPD, значение CAS Latency берется из микросхемы SPD. Установка большей задержки повышает стабильность работы компьютера, но отрицательно сказывается на быстродействии.

«Memory Topology» — показывает топологию оперативной памяти (рисунок 2.14).

Рисунок 2.14. «Memory Topology»



«Memory Map» (рисунок 2.15). Одной из основных обязанностей BIOS является программирование карты памяти.

Многие устройства, чтобы быть полезными, требуют, чтобы их интерфейсы были расширены до объема памяти. Кроме того, именно так BIOS может гарантировать, что информация о способе настройки системы будет передана ОС во время передачи обслуживания.

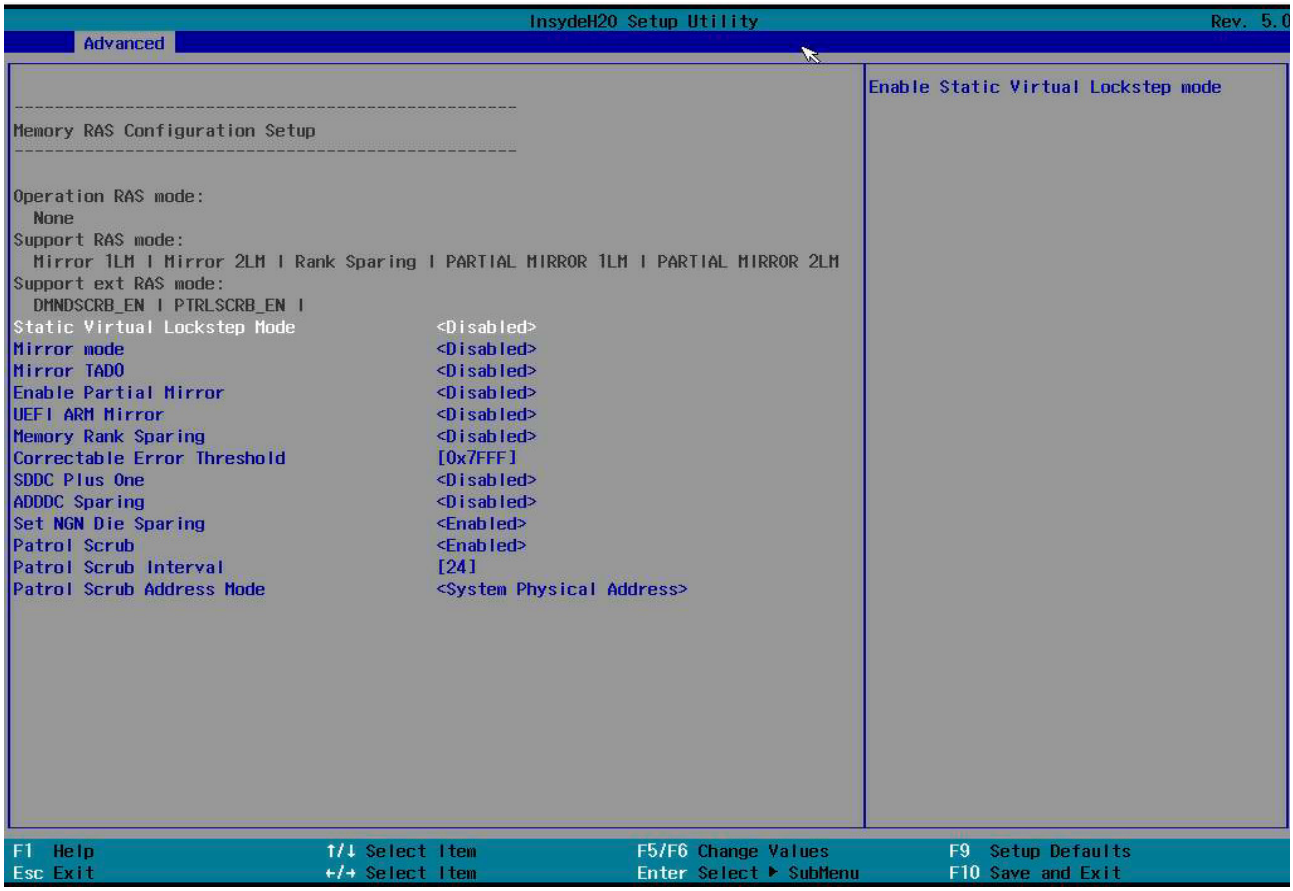
Рисунок 2.15. «Memory Map»

В окне «Memory Map»:

- «Volatile Memory Mode» — установка уровня кэша энергозависимой памяти;
- «AppDirect cache» — режим App Direct позволяет сохранять данные со скоростью, близкой к скорости памяти, сравнимой с энергонезависимыми Dimm (NVDIMMs), в соответствии с моделью программирования NVM Ассоциации индустрии сетей хранения данных, но при гораздо меньших затратах. Режим App Direct обрабатывает PMem как чрезвычайно быстрое энергонезависимое хранилище;
- «eADR Support» — Enhanced Asynchronous DRAM Refresh (eADR) позволяет сохранять в случае отказа электропитания изменчивые данные, находящиеся в кэшах DRAM и процессора, тем самым предотвращая потерю данных;
- «1LM Memory Interleave Granularity» — степень детализации чередования памяти;
- «IMC Interleaving» —эта опция используется для управления параметром чередования контроллера памяти;
- «Channel Interleaving». Более высокие значения разделяют блоки памяти и распределяют смежные части данных по чередующимся каналам, тем самым увеличивая потенциальную полосу пропускания чтения, поскольку запросы данных могут выполняться для всех чередующихся каналов с перекрытием. Для целей тестирования при использовании трех модулей памяти 4-стороннее чередование может превосходить оценку производительности установки 6-стороннего чередования в зависимости от используемого теста и ОС (32-разрядная или 64-разрядная). Однако обнаружено, что 6-стороннее чередование способно обеспечить более высокий общий BCLK для Super PI 32M, чем использование настройки 4-стороннего чередования (если, не используется одно- или двухканальное чередование и соответствующее чередование каналов, тем самым уменьшая нагрузку на контроллер памяти);
- «Rank Interleaving». Чередование физических рангов памяти так, чтобы к одному рангу можно получить доступ во время обновления другого. Прирост производительности снова зависит от рассматриваемого теста. Для круглосуточных систем, использующих трехканальную конфигурацию памяти, нет никаких преимуществ устанавливать это значение ниже 4, тогда как Channel Interleave следует оставить равным 6 для лучшей общей производительности системы;
- «Socket Interleave Below 4GB» — чередование сокетов менее 4 ГБ.

«Memory RAS Configuration» (рисунок 2.16). Row Address Strobe (RAS) — это сигнал на получение адреса строки, в которой находится ячейка памяти.

Рисунок 2.16. «Memory RAS Configuration»



В окне «Memory RAS Configuration»:

- «Operation RAS mode»;
- «Support RAS mode»;
- «Support ext RAS mode»;
- «Static Virtual Lockstep Mode» — режим Lockstep memory обеспечивает наилучшие функции RAS памяти.

Модули DIMM должны быть установлены попарно по каналам памяти (по два модуля DIMM в каждом канале памяти), чередуя каналы DDR4.

Каждая пара модулей DIMM в каналах DDR4 должна быть заполнена идентичными модулями DIMM. То есть модули DIMM должны быть идентичны по размеру, организации и т. д. Например, модули DIMM в слотах 9 (DDR4 канал 0) и 15 должны быть идентичными.

Канал памяти работает со скоростью передачи данных по каналам DDR4.

Объем памяти, установленный в режиме lockstep memory, — это объем памяти, доступный для использования;

- «Mirror mode» — зеркальное отображение памяти поддерживается в независимом режиме и пошаговом режиме блокировки;

🕮 ПРИМЕЧАНИЕ

При использовании функции зеркального отображения памяти необходимо учитывать следующую информацию:

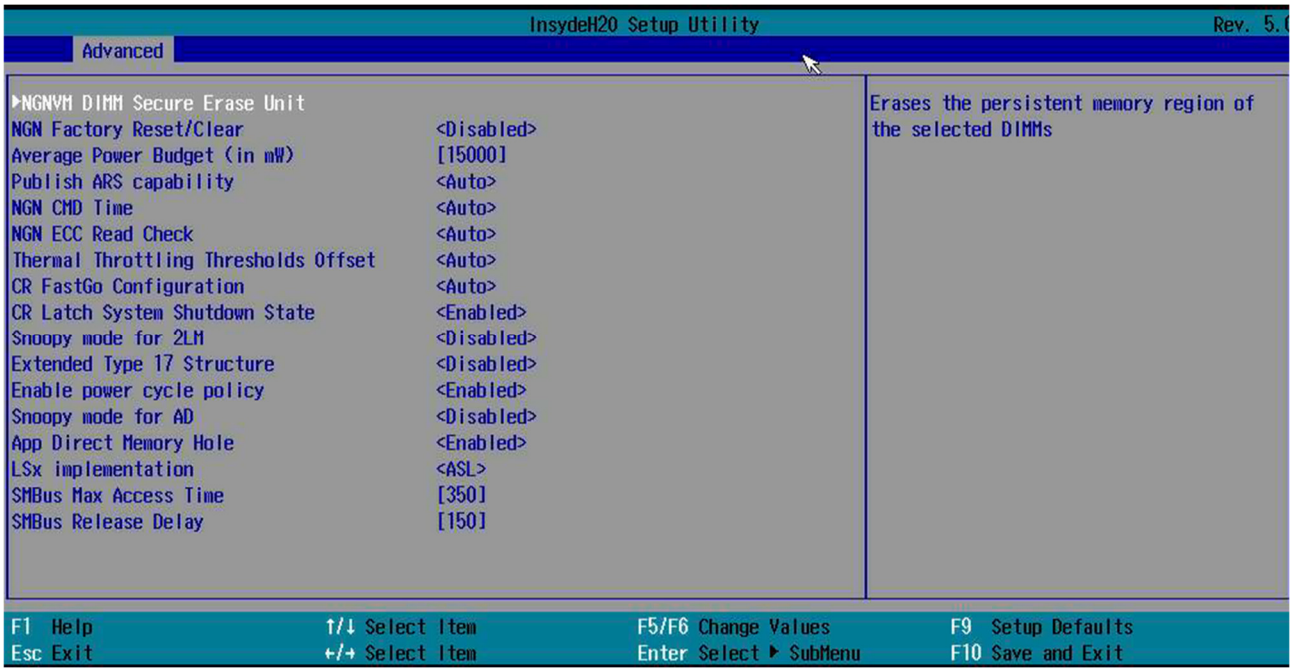
- сервер поддерживает зеркальное отображение памяти с одним сокетом. Канал памяти вычислительной книги 0 отражает канал памяти 1, а канал памяти 2 отражает

канал памяти 3. Такое зеркальное отображение обеспечивает избыточность памяти, но уменьшает общий объем памяти вдвое;
  - модули DIMM должны быть установлены попарно для каждой вычислительной книги при использовании функции зеркального отображения памяти;
  - набор модулей DIMM должен быть идентичным (размер, организация и т. д.) для канала памяти 0 и канала памяти 1 и идентичным для канала памяти 2 и канала памяти 3;
  - зеркальное отображение памяти уменьшает максимально доступный объем памяти наполовину от установленного объема памяти. Например, если на сервере установлено 64 ГБ оперативной памяти, при включенном зеркальном отображении памяти доступно только 32 ГБ адресуемой памяти.

- «Mirror TAD0». Процессор Intel Xeon с уровнем SKU выше, чем у Silver, поддерживает до двух зеркальных диапазонов, по одному зеркальному диапазону на интегрированный контроллер памяти (iMC). Диапазон определяется значением, запрограммированным в регистре декодера целевого адреса 0 (AD 0) для сервера. Параметр TAD0 определяет размер диапазонов первичного и вторичного зеркал. Диапазон вторичных зеркал зарезервирован для резервирования и не указывается в общем объеме памяти. При зеркальном отображении существует бит регистра управления и состояния (CSR), который позволяет использовать TAD0 для зеркального отображения;
- «Enable Partial Mirror». Режим частичного зеркального отображения позволит зеркалировать необходимый объем памяти. Если включено сохранение ранга, частичное зеркальное отображение не вступит в силу. Включение зеркального отображения отключит предварительную выборку XPT;
- «UEFI ARM Mirror» — инициирует поведение зеркала диапазона адресов на основе UEFI с помощью опции настройки;
- «Memory Rank Sparing». В режиме экономии разрядов один разряд DIMM памяти служит запасным для других разрядов на том же канале. Запасной ранг хранится в резерве и не используется в качестве активной памяти. Резервный разряд должен иметь идентичный или больший объем памяти, чем все остальные активные разряды DIMM на том же канале. После превышения порогового значения ошибки содержимое этого ранга копируется в запасной ранг. Вышедший из строя ранг модулей DIMM переводится в автономный режим, а запасной ранг подключается к сети и используется в качестве активной памяти вместо вышедшего из строя ранга;
- «Correctable Error Threshold» — исправляемый порог ошибки. Исправляемые ошибки могут быть обнаружены и исправлены, если набор микросхем и модуль DIMM поддерживают эту функциональность. Исправляемые ошибки, как правило, представляют собой однобитовые ошибки;
- «SDDC Plus One». При работе с UDIMMS (встроенными устройствами x8 DRAM) система может пережить полный сбой DRAM (SDDC). В режиме независимого канала этот сбой был бы неисправимой ошибкой;
- «ADDDC Sparing» — адаптивная двойная коррекция данных устройства;
- «Set NGN Die Sparing»;
- «Patrol Scrub». Процессор при возможности исправляет ошибки (режим коррекции оперативной памяти ECC (error-correcting code)) автоматически, после — отправляет обратно. После включения данной функции концентратор ввода-вывода будет считывать и записывать данные каждые 16 Кбайт при отсутствии задержки, вызванной внутренней обработкой;
- «Patrol Scrub Interval» — интервал поиска ошибок;
- «Patrol Scrub Address Mode».

«NGN Configuration» — настройки сети следующего поколения (рисунок 2.17).

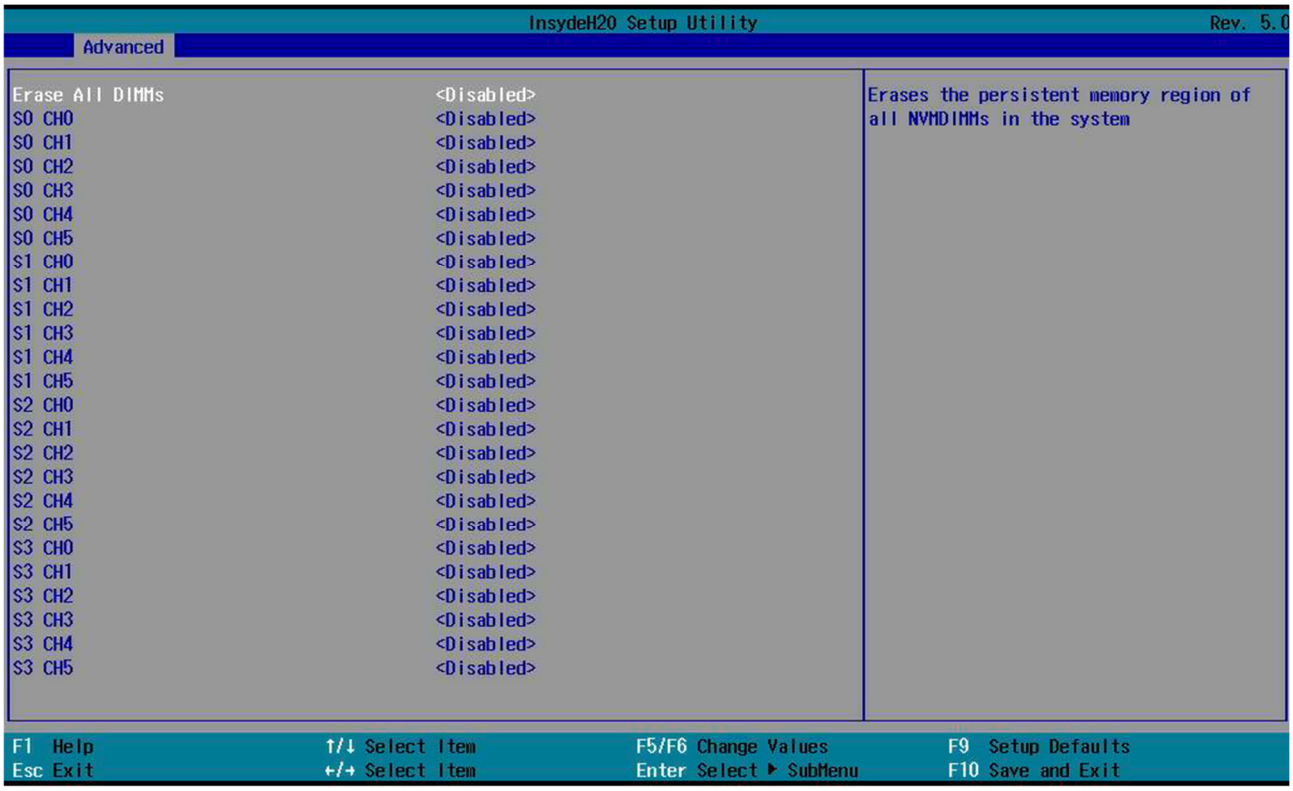
Рисунок 2.17. «NGN Configuration»



В окне «NGN Configuration»:

- «NGNVM DIMM Secure Erase Unit» — включение/отключение (по умолчанию) безопасного стирания области постоянной памяти PMEM в системе (рисунок 2.18);

Рисунок 2.18. «NGNVM DIMM Secure Erase Unit»



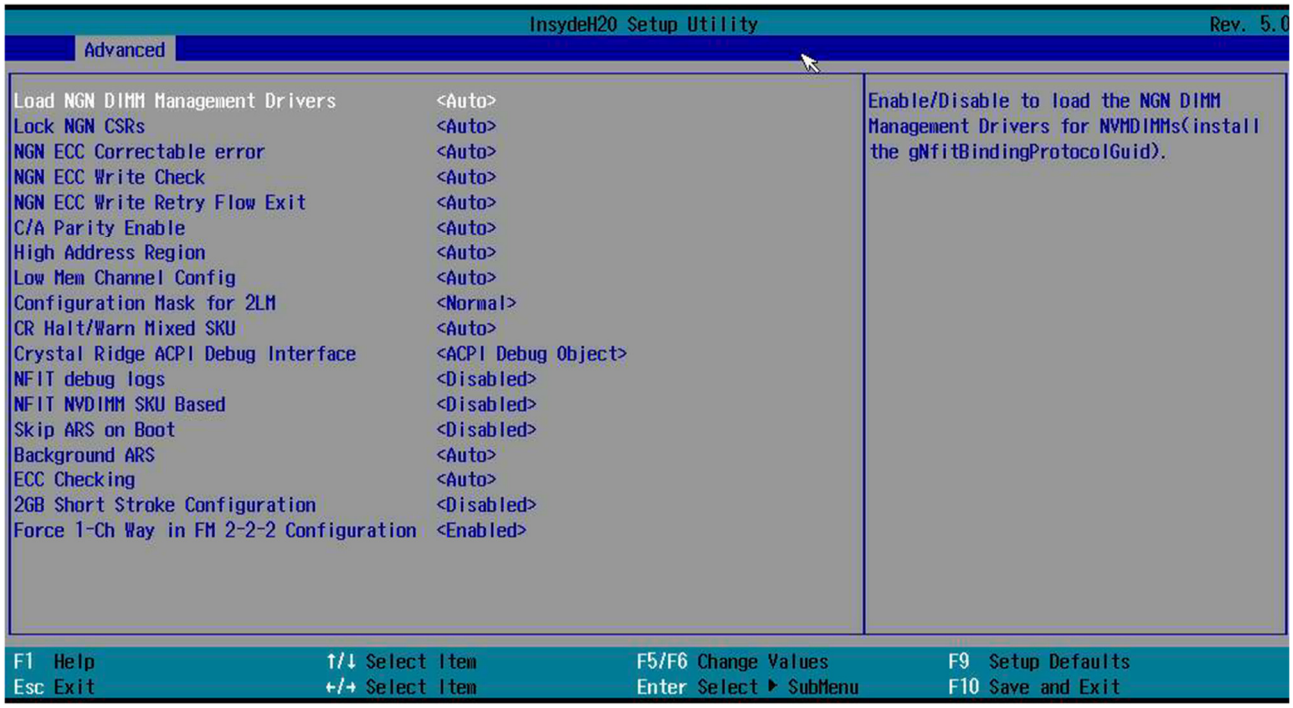
- «NGN Factory Reset/Clear» — сброс до заводских настроек;
- «Average Power Budget (in mW)» — установка политики управления питанием для средней мощности (должно быть увеличено на 250 МВт). Средний диапазон мощности

зависит от размера модуля DIMM. Для 128 ГБ диапазон составляет 10–15 Вт, для 256/512 ГБ диапазон составляет 12–18 Вт. Если установлено значение, выходящее за пределы диапазона, оно автоматически корректируется;

- «Publish ARS capability» — включение/отключение публикации ARS диапазона для ОС;
- «NGN CMD Time» — выбор времени выполнения команды 1N/2N NGN;
- «NGN ECC Read Check» — проверка считывания кода исправления ошибок;
- «Thermal Throttling Thresholds Offset» — установка температуры троттлинга;
- «CR FastGo Configuration» — выбор настроек профиля CR QoS;
- «CR Latch System Shutdown State»;
- «Snoopy mode for 2LM» — включение новой специфичной для 2LM функции, позволяющей избежать обновления каталогов в удаленной памяти при не оптимизированных по количеству рабочих нагрузках;
- «Extended Type 17 Structure» — использование расширенного Type 17 SMBIOS. Структура Type 17 SMBIOS описывает одно запоминающее устройство, которое является частью более крупного массива физической памяти;
- «Enable Power cycle policy» — включение/выключение политики цикла питания, когда NVMDIMM получает неожиданную остановку;
- «Snoopy mode for AD» — включение новой специфичной для AD функции, позволяющей избежать обновления каталогов в памяти DDRT при рабочих нагрузках, не оптимизированных для NUMA;
- «App Direct Memory Hole». Для правильной работы некоторых карт ISA требуется эксклюзивный доступ к блоку памяти объемом 1 МБ, от 15 до 16 МБ. Функция BIOS «Memory Hole 15-16 M» позволяет зарезервировать этот блок памяти объемом 1 МБ для использования такими картами;
- «LSx implementation» — методы меток NVDIMM, которые прикреплены к объекту NVDIMM:
  - _LSI — информация о хранении меток. Возвращает информацию об области хранения меток, связанной с объектом NVDIMM, включая ее размер;
  - _LSR — чтение хранилища меток. Возвращает данные метки из области хранения меток объекта NVDIMM;
  - _LSW — запись в хранилище меток. Записывает данные меток в область хранения меток объекта NVDIMM;
- «SMBus Max Access Time» — максимальное количество времени, в течение которого драйверу UEFI mgmt разрешено использовать SMBus;
- «SMBus Release Delay» — временная задержка после разблокировки доступа к SMBus драйвера UEFI mgmt.

«Memory Dfx Configuration» (рисунок 2.19). Конфигурация динамического обмена функциями (DFX) позволяет независимо перепрограммировать одну или несколько подобластей устройства с новыми конфигурационными данными, в то время как все остальные области (статические или реконфигурируемые) остаются активными и незатронутыми. DFX PDI может быть получен либо из PCIe, DDR-памяти, либо с основного загрузочного устройства. Для загрузки PDF-файлов DFx можно использовать команды XilLoader CDO, используя интерфейс API. XilFPGA предоставляет необходимые API-интерфейсы для загрузки DFx PDI из APU или центрального процессора.

Рисунок 2.19. «Memory Dfx Configuration»

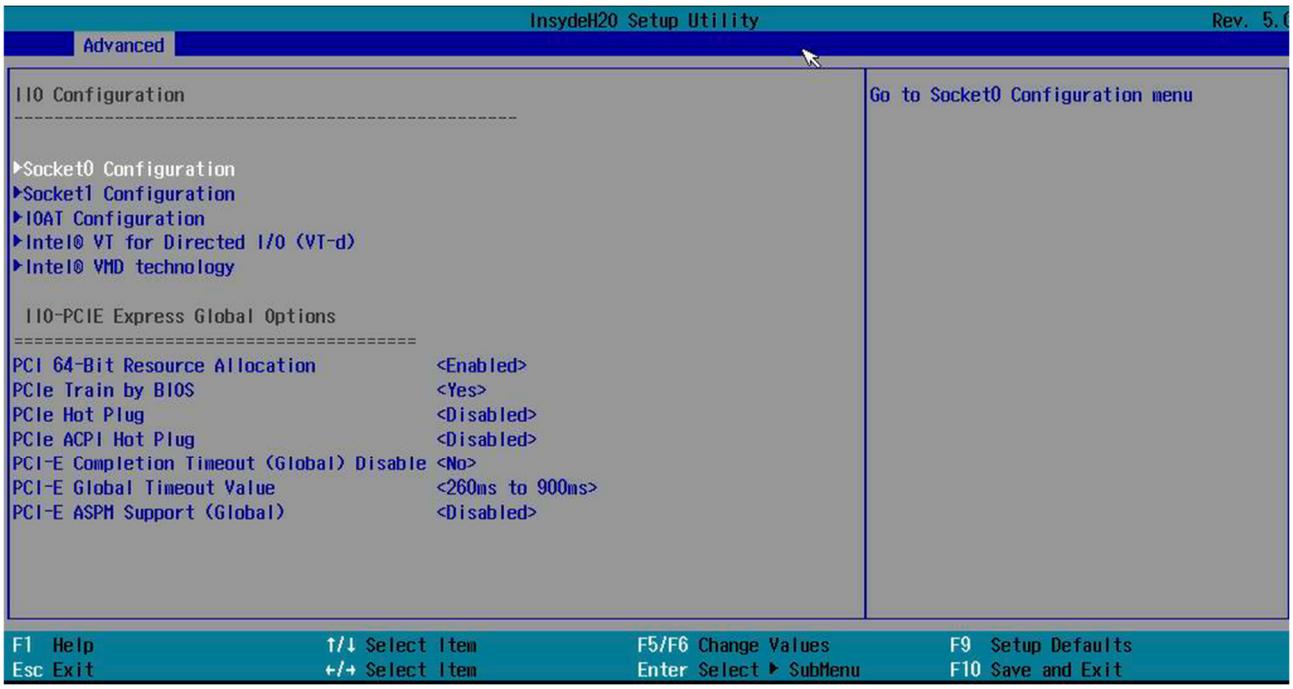


В окне «Memory Dfx Configuration»:

- «Load NGN DIMM Management Drivers» — загрузка управляющих драйверов NGN DIMM;
- «Lock NGN CSRs»;
- «NGN ECC Correctable error»;
- «NGN ECC Write Check»;
- «NGN ECC Write Retry Flow Exit»;
- «C/A Parity Enable»;
- «High Address Region»;
- «Low Mem Channel Config»;
- «Configuration Mask for 2LM»;
- «CR Halt/Warn Mixed SKU»;
- «Crystal Ridge ACP Debug Interface»;
- «NFIT Debug logs»;
- «NFIT NVDIMM SCU Based»;
- «Skip ARS on Boot»;
- «Background ARS»;
- «ECC Checking»;
- «2GB Short Stroke Configuration»;
- «Force 1-Ch Way in FM 2-2-2 Configuration».

2.2.5.5. «IIO Configuration» (рисунок 2.20). Конфигурация ввода-вывода — это набор аппаратных ресурсов, доступных ОС и/или средствам сопряжения, а также соединения между этими ресурсами. Аппаратные ресурсы обычно включают в себя каналы (все типы каналов, включая соединительные линии, которые соединяются между z/OS и средством связи).

Рисунок 2.20. «IIO Configuration»

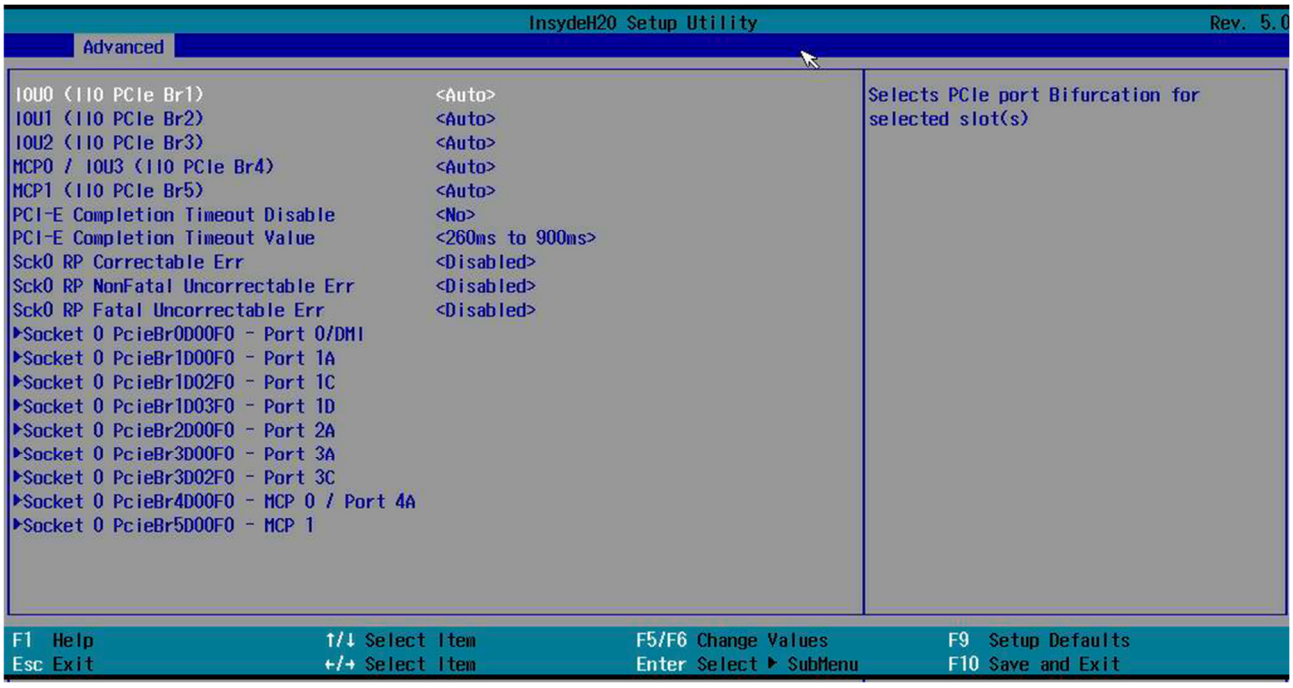


«Socket0 Configuration» — настройки устройств, связанных с нулевым сокетом (рисунок 2.21).

🕮 ПРИМЕЧАНИЕ

Данное описание также является верным для «Socket1 Configuration» и его подпунктов (рисунок 2.24).

Рисунок 2.21. «Socket0 Configuration»



В окне «Socket0 Configuration»:

- «IOU0 (IIO PCIe Br1)» — выбор настройки бифуркации для выбранного слота.

Раздвоение PCIe ничем не отличается от определения, т. е. разделения слота PCIe на более мелкие фрагменты/ответвления. Например, слот для карт PCIe x8 может быть разделен на

два (2) блока x4 или PCIe x16 на четыре (4) блока x4, т. е. x4x4x4x4 ИЛИ два (2) x8, т. е. x8x8 ИЛИ один (1) x8 и два (2) x4, т. е. x8x4x4 / x4x4x8.

Раздвоение PCIe не снижает скорость, а только разделяет полосы движения. Чтобы использовать раздвоение, материнская плата должна поддерживать его и, если это так, BIOS также должен поддерживать его;

🕮 ПРИМЕЧАНИЕ

Данное описание также является верным для «IOU1 (IIO PCIe Br2)», «IOU2 (IIO PCIe Br3)», «MCP0 / IOU3 (IIO PCIe Br4)», «MCP1 / (IIO PCIe Br5)».

- «IOU1 (IIO PCIe Br2)»;
- «IOU2 (IIO PCIe Br3)»;
- «MCP0 / IOU3 (IIO PCIe Br4)»;
- «MCP1 / (IIO PCIe Br5)»;
- «PCI-E Completion Timeout Disable» — отключает механизм тайм-аута завершения. При включении ядро поддерживает механизм отключения тайм-аута завершения через устройство PCI Express;
- «PCI-E Completion Timeout Value» — установка временного значения тайм-аута завершения;
- «Sck0 RP Correctable Err». Применяется только к корневым портам. Позволяет включить или отключить прерывание при исправляемых ошибках;
- «Sck0 RP NonFatal Uncorrectable Err». Применяется только к корневым портам. Позволяет включить или отключить прерывание при нефатальной ошибке;
- «SCK0 RP Fatal Uncorrectable Err». Применяется только к корневым портам. Позволяет включить или отключить прерывание при фатальной ошибке;
- «Socket 0 PcieBr0D00F0 — Port 0/DM1» — настройки указанного порта (рисунок 2.22):

1) «Link Speed» — установка скорости соединения для данного порта;

2) «Override Max Link Width» — настройка ширины канала, заданного бифуркацией;

3) «PCI-E Port DeEmphasis» — определяет настройки смещения акцента порта PCIe. PCIe использует смещение акцента передачи для компенсации потерь в высокочастотном канале. Форма сигнала с пониженным акцентом определяется в терминах уровней напряжения Va (пониженный акцент) и Vb (ровный уровень). Этот параметр доступен только в том случае, если скорость соединения установлена на Gen 2 (5 Гбит/с);

4) «PCI-E Port Link Status» — отображает текущее состояние соединения;

5) «PCI-E Port Link Max» — отображает текущую ширину канала;

6) «PCI-E Port Link Speed» — отображает текущую скорость соединения;

7) «PCI-E Port Clocking» — настройка синхронизации портов с помощью LNKCON. Это относится к данному компоненту и компоненту нисходящего потока;

8) «PCI-E Port Max Payload Size» — указывает максимальный размер полезной нагрузки для порта PCIe;

9) «PCI-E Port D-state» — установка значения D0 для нормальной работы, D3 Hot — для работы в режиме низкого энергопотребления;

10) «PCI-E ASPM Support» — включение/отключение Active-state power management (ASPM) — механизма управления питанием для устройств PCI Express, позволяющего экономить электроэнергию, находясь в полностью активном состоянии;

11) «PCI-E Port L0s Exit Latency» — настройка времени, необходимого этому порту для завершения перехода с L0s на L0;

12) «PCI-E Port L1 Exit Latency» — настройка времени, необходимого этому порту для завершения перехода с L1s на L1;

13) «MSI» — BUS0 DEVx FUN0 OFF 0x5a bit 0, where X is 0-3;

14) «PCI-E Extended Sync» — включает/отключает режим расширенной синхронизации;

15) «Compliance Mode» — позволяет установить версию базовых спецификаций PC Express, которой должна соответствовать материнская плата;

16) «E0I» — Dev 0,2,3 MISCCTRLSTS (Reg 0x188) Bit 26;

17) «Fatal Err Over» — включает/отключает принудительное распространение фатальной ошибки в логике ошибок ядра IIO для этого порта;

18) «Non-Fatal Err Over» — включает/отключает принудительное распространение нефатальной ошибки в логике ошибок ядра IIO для этого порта;

19) «Corr Err Over» — включает/отключает принудительное распространение исправляемой ошибки в логике ошибок ядра IIO для этого порта;

20) «ACPI PME Interrupt» — когда этот параметр включен, прерывания ACPI PME генерируются с этого порта;

21) «L0s Support» — когда отключен, не переводит свой передатчик в состояние L0s;

22) «P2P Memory Write» — управляет декодированием записи в память Peer2Peer;

23) «P2P Memory Read» — управляет считыванием и декодированием данных из памяти Peer2Peer;

24) «PME to ACK» — управляет использованием тайм-аута для IIO, ожидающего PME_T0_ACK после сообщения PME_TURN_OFF;

25) «Unsupported Request» — управляет отчетами о неподдерживаемых запросах, которые сам IIO обнаруживает в запросах, которые он получает от порта PCIe/HDMI;

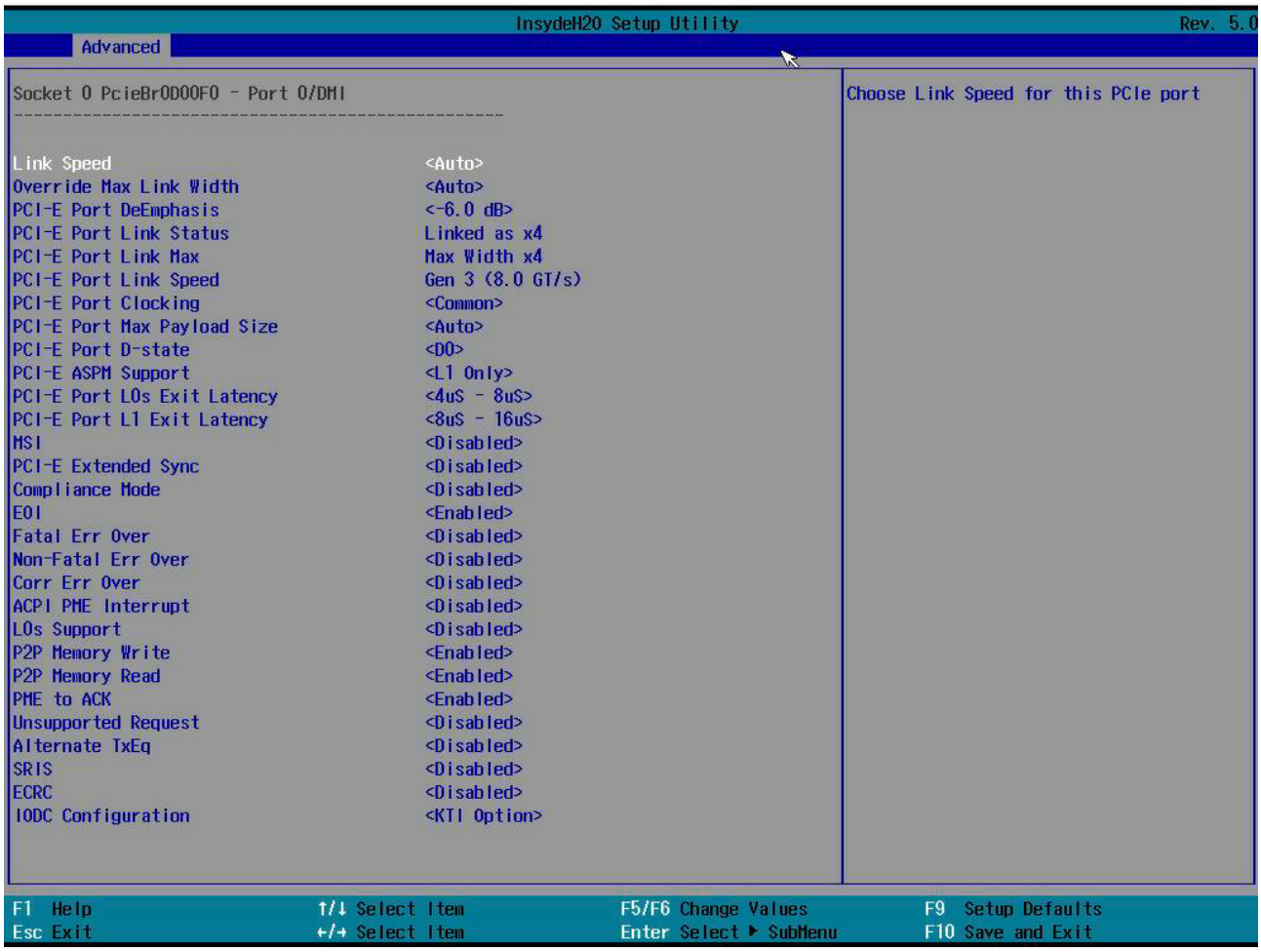
26) «Alternate TxEq»;

27) «SRIS» — отдельная ссылка с независимым расширением (SRIS): RC и EP могут не использовать модуляцию расширения каждый. Если только один из них использует расширенную модуляцию, это считается SRIS;

28) «ECRC» — включает или отключает ECRC (возможности обнаружения ошибок и регистр управления);

29) «IODC Configuration» — включает/отключает IODC (прямой кэш ввода-вывода): генерирует snoops вместо поиска в памяти для удаленного InvItoM (IIO) и/или WCiLF;

Рисунок 2.22. «Socket 0 PcieBr0D00F0 — Port 0/DM1»



- «Socket 0 PcieBr1D00F0 — Port 1A» (рисунок 2.23):

1) «PCI-E Port»;
2) «Hot Plug Capable»;
3) «Surprise Hot Plug Capable»;
4) «PCI-E Port Link»;
5) «Link Speed» — установка скорости соединения для данного порта;
6) «Override Max Link Width» — настройка ширины канала, заданного бифуркацией;
7) «PCI-E Port DeEmphasis» — определяет настройки смещения акцента порта PCIe. PCIe использует смещение акцента передачи для компенсации потерь в высокочастотном канале. Форма сигнала с пониженным акцентом определяется в терминах уровней напряжения Va (пониженный акцент) и Vb (ровный уровень). Этот параметр доступен только в том случае, если скорость соединения установлена на Gen 2 (5 Гбит/с);
8) «PCI-E Port Link Status» — отображает текущее состояние соединения;
9) «PCI-E Port Link Max» — отображает текущую ширину канала;
10) «PCI-E Port Link Speed» — отображает текущую скорость соединения;
11) «PCI-E Port Clocking» — настройка синхронизации портов с помощью LNKCON. Это относится к данному компоненту и компоненту нисходящего потока;
12) «PCI-E Port Max Payload Size» — настройка синхронизации портов с помощью LNKCON. Это относится к данному компоненту и компоненту нисходящего потока;
13) «PCI-E Port D-state» — установка значения D0 для нормальной работы, D3 Hot — для работы в режиме низкого энергопотребления;

14) «PCI-E ASPM Support» — включение/отключение Active-state power management (ASPM) — механизма управления питанием для устройств PCI Express, позволяющего экономить электроэнергию, находясь в полностью активном состоянии;

15) «PCI-E Port L0s Exit Latency» — настройка времени, необходимого этому порту для завершения перехода с L0s на L0;

16) «PCI-E Port L1 Exit Latency» — настройка времени, необходимого этому порту для завершения перехода с L1s на L1;

17) «MSI» — BUS0 DEVx FUN0 OFF 0x5a bit 0, where X is 0-3;

18) «PCI-E Extended Sync» — включение/отключение режима расширенной синхронизации;

19) «Compliance Mode» — данная функция BIOS позволяет установить версию базовых спецификаций PC Express, которой должна соответствовать материнская плата;

20) «E0I» — Dev 0,2,3 MISCCTRLSTS (Reg 0x188) Bit 26;

21) «Fatal Err Over» — включение/отключение принудительного распространения фатальной ошибки в логике ошибок ядра IIO для этого порта;

22) «Non-Fatal Err Over» — включение/отключение принудительного распространения нефатальной ошибки в логике ошибок ядра IIO для этого порта;

23) «Corr Err Over» — включение/отключение принудительного распространения исправляемой ошибки в логике ошибок ядра IIO для этого порта;

24) «ACPI PME Interrupt» — когда этот параметр включен, прерывания ACPI PME генерируются с этого порта;

25) «L0s Support» — когда отключен, не переводит свой передатчик в состояние L0s;

26) «P2P Memory Write» — управляет декодированием записи в память Peer2Peer;

27) «P2P Memory Read» — управление считыванием и декодированием данных из памяти Peer2Peer;

28) «PME to ACK» — управление использованием тайм-аута для IIO, ожидающего PME_T0_ACK после сообщения PME_TURN_OFF;

29) «PM ACPI Mode» — когда отключен, MSI генерируется по событию PM; при включении генерируется сообщение HPQPSE;

30) «Unsupported Request» — управление отчетами о неподдерживаемых запросах, которые сам IIO обнаруживает в запросах, которые он получает от порта;

31) «Alternate TxEq»;

32) «SRIS» — отдельная ссылка с независимым расширением (SRIS): RC и EP могут не использовать модуляцию расширения каждый. Если только один из них использует расширенную модуляцию, это считается SRIS;

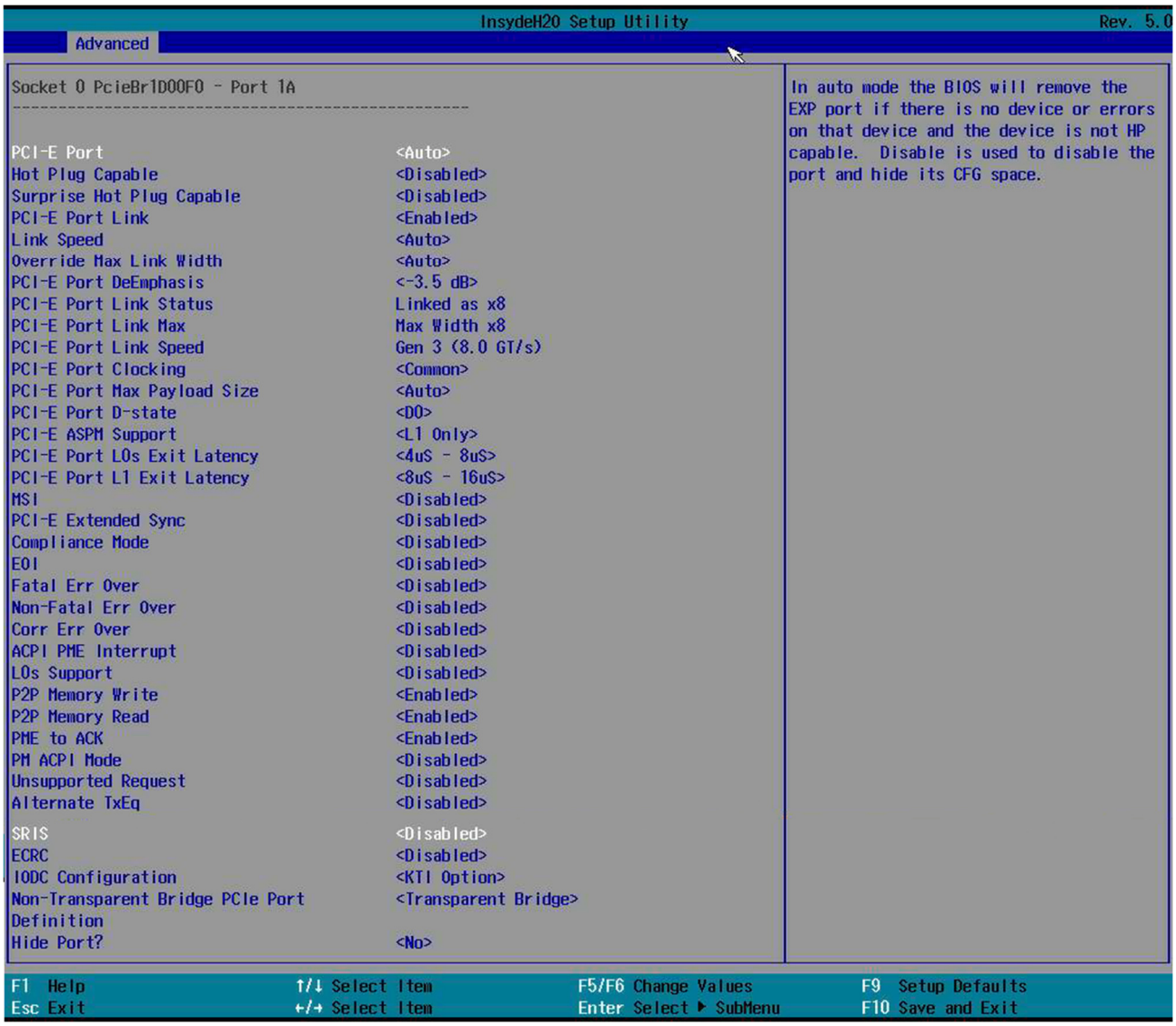
33) «ECRC» — включает или отключает ECRC (возможности обнаружения ошибок и регистр управления);

34) «IODC Configuration» — включение/отключение IODC (прямой кэш ввода-вывода: генерирует snoops вместо поиска в памяти для удаленного InvItoM (IIO) и/или WCiLF);

35) «Non-Transparent Bridge PCIe Port Definition»;

36) «Hide Port?» — скрыть порт.

Рисунок 2.23. «Socket 0 PcieBr1D00F0 — Port 1A»



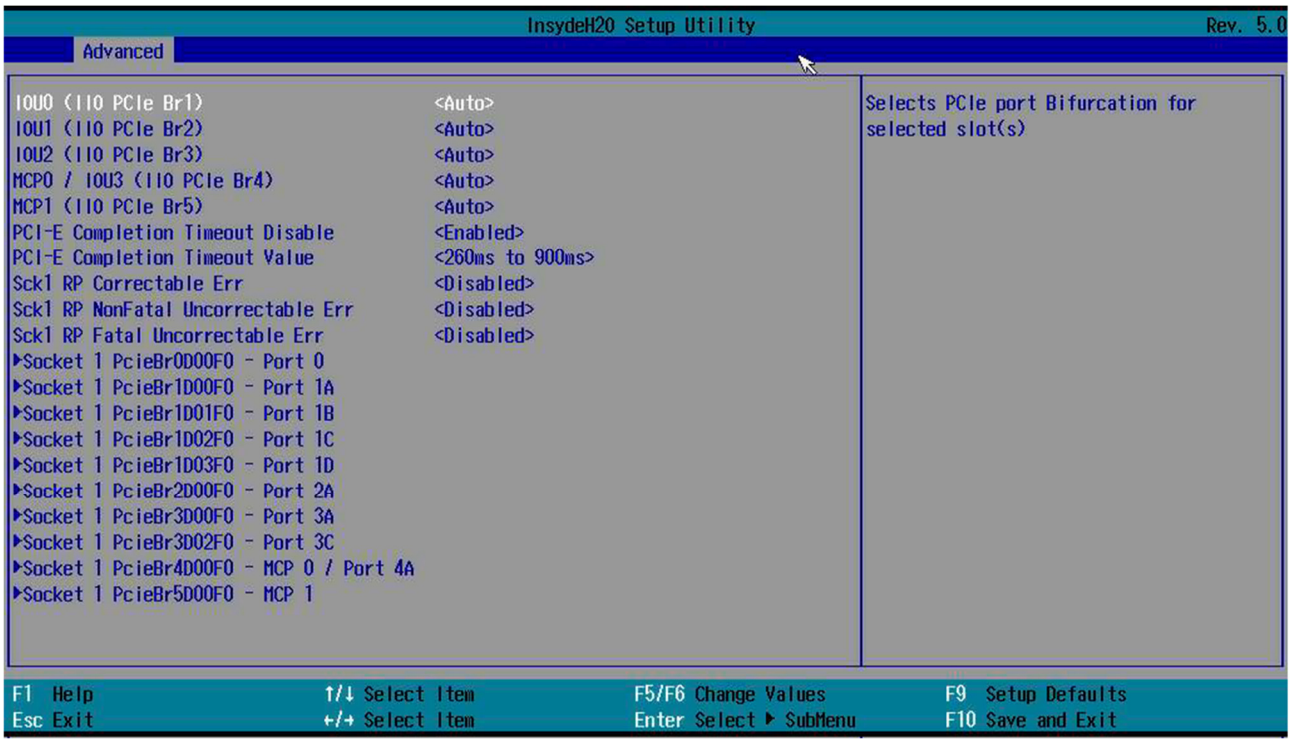
🕮 ПРИМЕЧАНИЕ

Данное описание также является верным для:

- «Socket 0 PcieBr1D02F0 — Port 1C»;
- «Socket 0 PcieBr1D03F0 — Port 1D»;
- «Socket 0 PcieBr2D00F0 — Port 2A»;
- «Socket 0 PcieBr3D00F0 — Port 3A»;
- «Socket 0 PcieBr3D02F0 — Port 3C»;
- «Socket 0 PcieBr4D00F0 — MCP 0 / Port 4A»;
- «Socket 0 PcieBr5D00F0 — MCP 1».

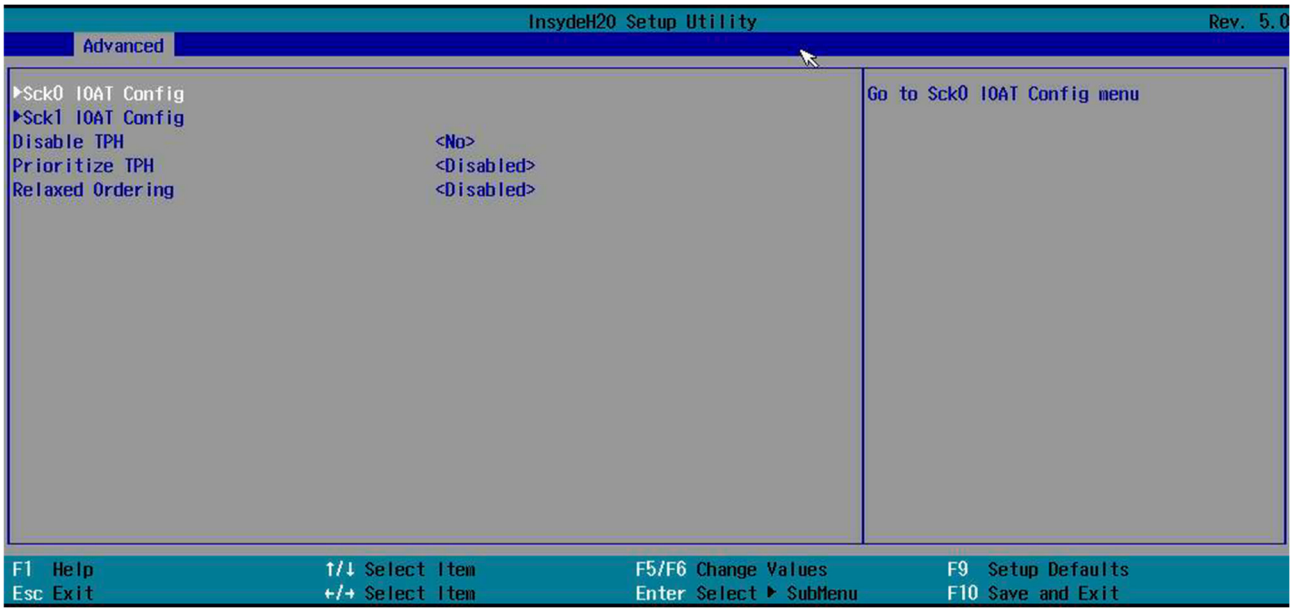
«Socket1 Configuration» (рисунок 2.24). Описание соответствует «Socket0 Configuration» и его подпунктам.

Рисунок 2.24. «Socket1 Configuration»



«IOAT Configuration» (рисунок 2.25) — технология ускорения (Intel ® I/OAT). Компонент технологии виртуализации Intel ® для подключения, улучшает поток данных по платформе для повышения производительности системы.

Рисунок 2.25. «IOAT Configuration»



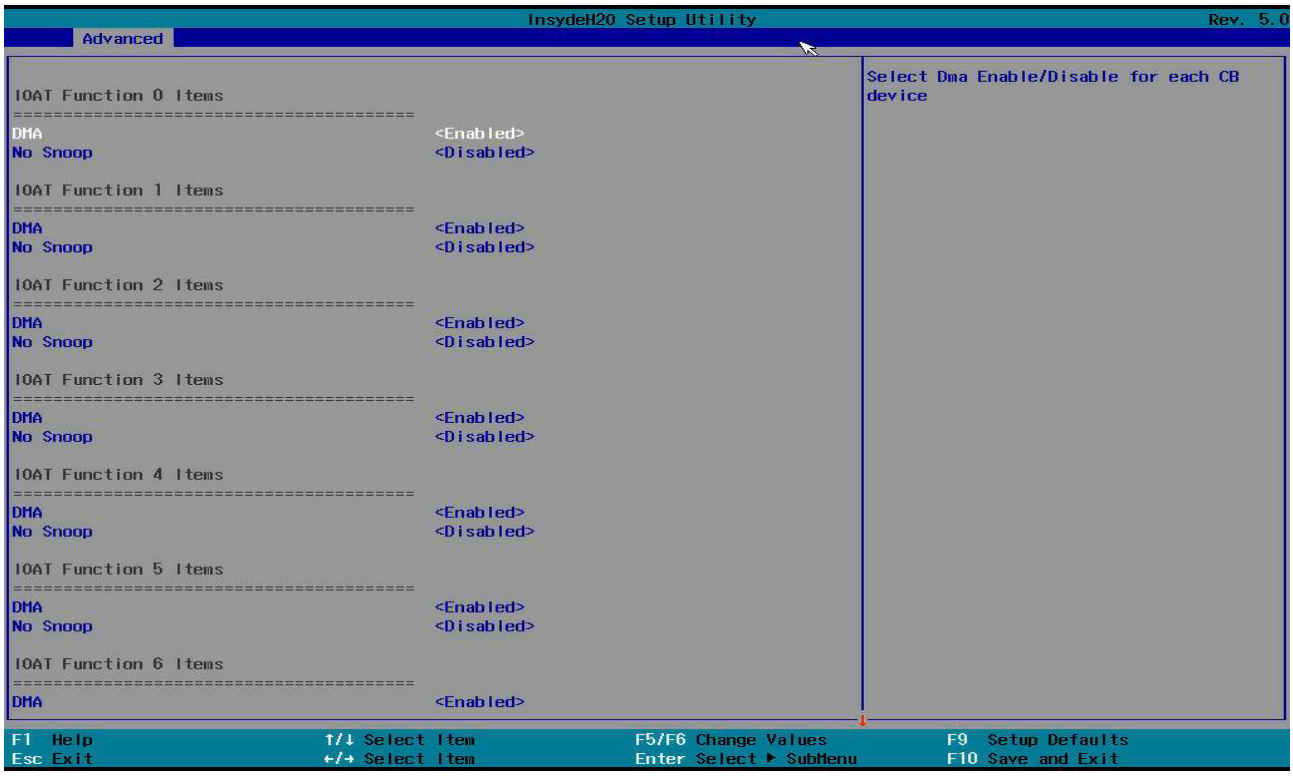
В окне на рисунке 2.25:

- «Sck0 IOAT Config»:

  1) «IOAT Function 0–7 items» (рисунок 2.26):

  - «DMA» (Direct Memory Access, прямой доступ к памяти) — это режим работы, при котором устройство обменивается данными с оперативной памятью без участия центрального процессора;
  - «No Snoop»;

Рисунок 2.26. «IOAT Function 0–7 items»

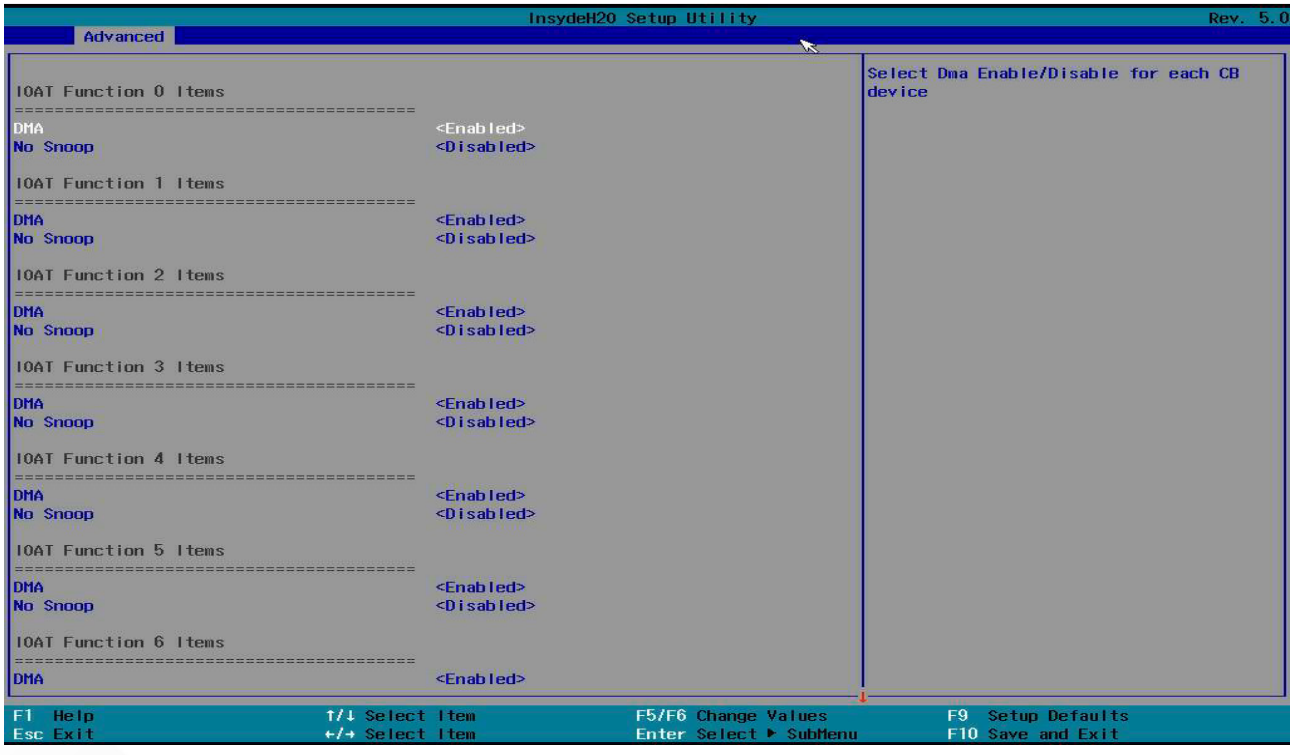


- «Sck1 IOAT Config»:

  1) «IOAT Function 0–7 items» (рисунок 2.27):

  - «DMA»;
  - «No Snoop»;

Рисунок 2.27. «IOAT Function 0–7 items»

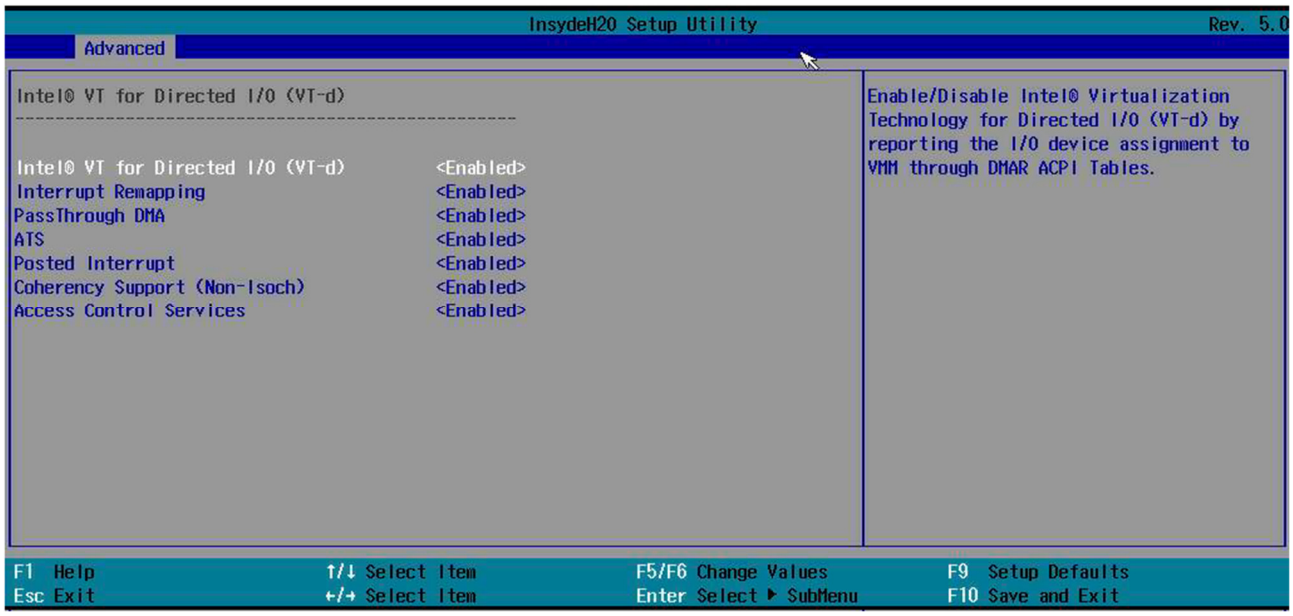


- «Disable TPH». Transparent Huge Pages (TPH) — это система управления памятью Linux, которая обеспечивает обмен данными в больших блоках (страницах). Включение этой функции повысит производительность;
- «Prioritize TPH» — использовать эту функцию, чтобы включить приоритетную поддержку TPH. Доступны следующие опции: включить и отключить;
- «Relaxed Ordering» — выбрать «Включить», чтобы включить поддержку упрощенного упорядочения, что позволит определенным транзакциям нарушать строгие правила упорядочения шины PCI, чтобы транзакция выполнялась раньше других транзакций, которые уже поставлены в очередь.

«Intel® VT for Directed I/O (VT-d)» (рисунок 2.28):

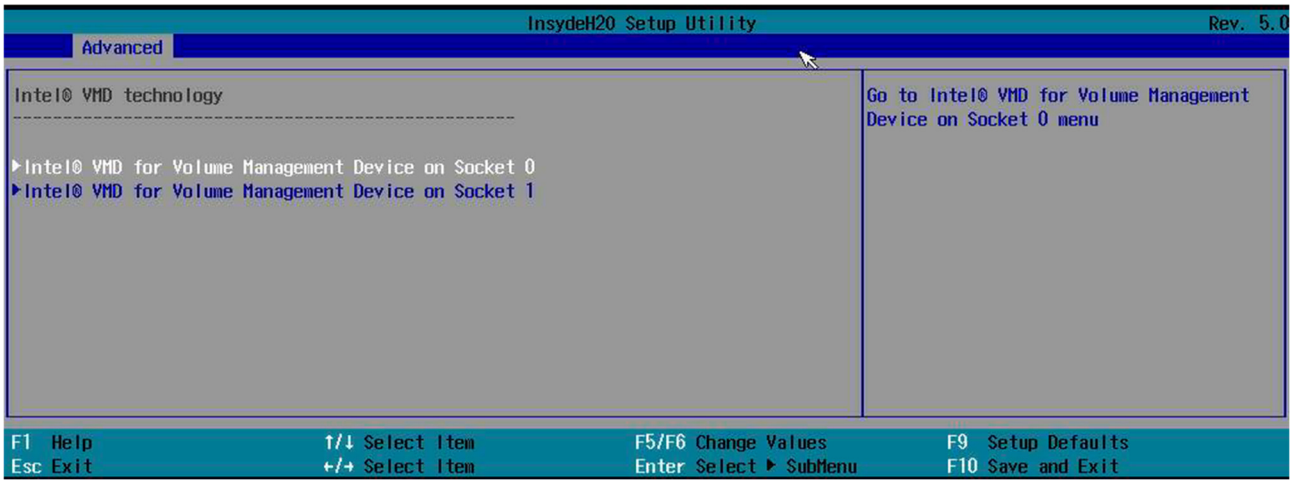
- «Intel® VT for Directed I/O (VT-d)» — выбрать «Включить», чтобы использовать технологию виртуализации Intel для поддержки Direct I/O VT-d, сообщая назначения устройств ввода-вывода в VMM (Virtual Machine Monitor) через таблицы DMAR ACPI. Эта функция предлагает полностью защищенное совместное использование ресурсов ввода-вывода на платформах Intel, обеспечивая более высокую надежность, безопасность и доступность в сети и при совместном использовании данных;
- «Interrupt Remapping» — использовать эту функцию, чтобы включить поддержку переназначения прерываний, которая обнаруживает и контролирует внешние запросы на прерывание;
- «PassThrough DMA» — использовать эту функцию, чтобы разрешить таким устройствам, как сетевые карты, доступ к системной памяти без использования процессора. Выбрать «Включить», чтобы использовать поддержку Non-Isoch VT_D Engine Pass Through Direct Memory Access (DMA);
- «ATS» — использовать эту функцию, чтобы включить поддержку служб преобразования адресов (ATS) ядра VT-d, отличных от Isoch. ATS преобразует виртуальные адреса в физические адреса;
- «Posted Interrupt» — использовать эту функцию, чтобы включить VT_D Posted Interrupt;
- «Coherency Support (Non-Isoch)» — использовать эту функцию для обеспечения согласованности настроек между процессорами или другими устройствами. Выбрать «Включить», чтобы механизм Non-Isoch VT-d проходил через прямой доступ к памяти для повышения производительности системы;
- «Access Control Services» — выбрать «Включить», чтобы включить поддержку расширенных возможностей служб контроля доступа (ACS) для повышения производительности системы.

Рисунок 2.28. «Intel® VT for Directed I/O (VT-d)»



«Intel® VMD technology» (рисунок 2.29).

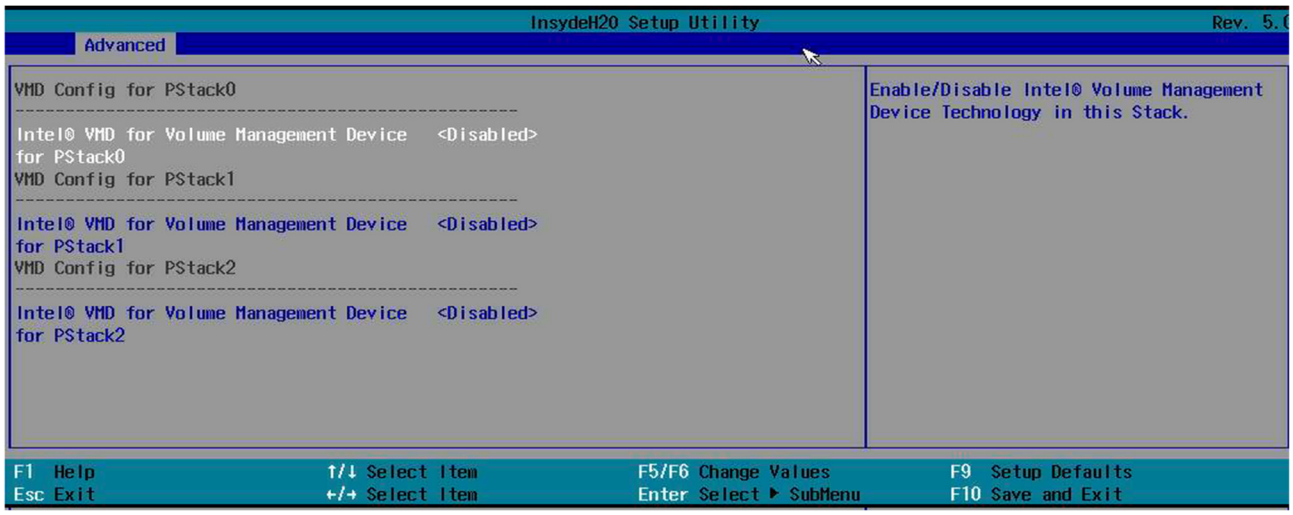
Рисунок 2.29. «Intel® VMD technology»



В окне на рисунке 2.29:

- «Intel® VMD for Volume Management Device on Socket 0» (рисунок 2.30) — после того как был включен VMD в выбранном слоте PCI-E, этот слот PCI-E будет предназначен только для устройств хранения данных NVMe и больше не будет поддерживать устройства PCI-E с другими функциональными возможностями. Чтобы повторно активировать этот слот для использования с PCI-E, необходимо отключить VMD:

Рисунок 2.30. «Intel® VMD for Volume Management Device on Socket 0»



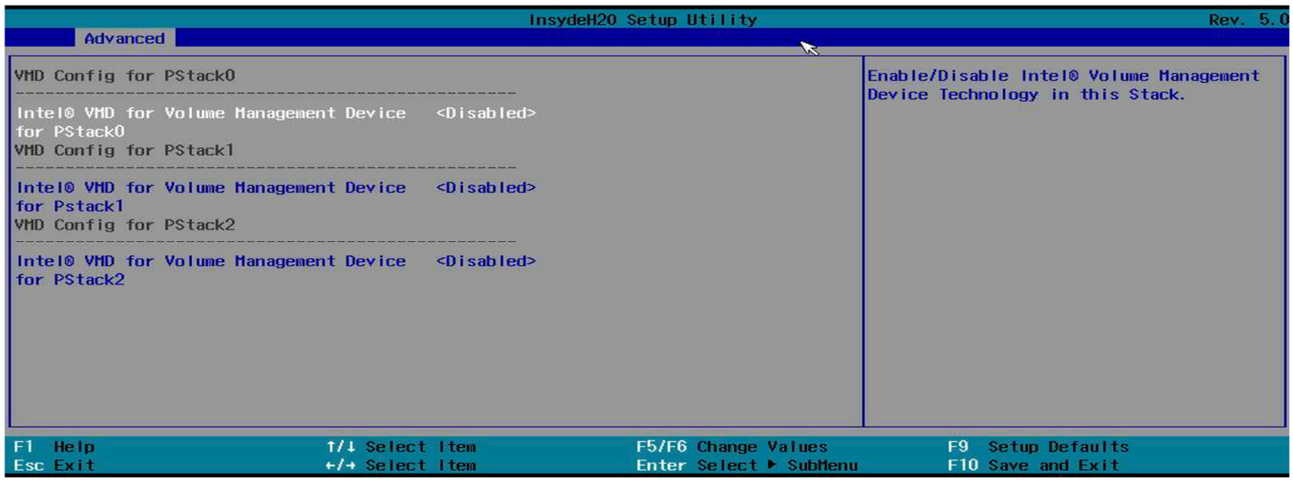
1) «Intel® VMD for Volume Management Device for PStack0» — выбрать «Включить», чтобы использовать технологию Intel Volume Management Device для этого стека. Доступны следующие опции: отключить и включить. Если для параметра установлено значение Enable, для настройки будут доступны следующие элементы: поддержка горячего подключения (доступно, когда устройство обнаружено системой). Использовать эту функцию, чтобы включить поддержку горячего подключения для корневых портов PCIe 1A~1D;

2) «Intel® VMD for Volume Management Device for PStack1»;

3) «Intel® VMD for Volume Management Device for PStack2»;

- «Intel® VMD for Volume Management Device on Socket 1» (рисунок 2.31):

Рисунок 2.31. «Intel® VMD for Volume Management Device on Socket 1»



1) «Intel® VMD for Volume Management Device for PStack0»;

2) «Intel® VMD for Volume Management Device for PStack1»;

3) «Intel® VMD for Volume Management Device for PStack2».

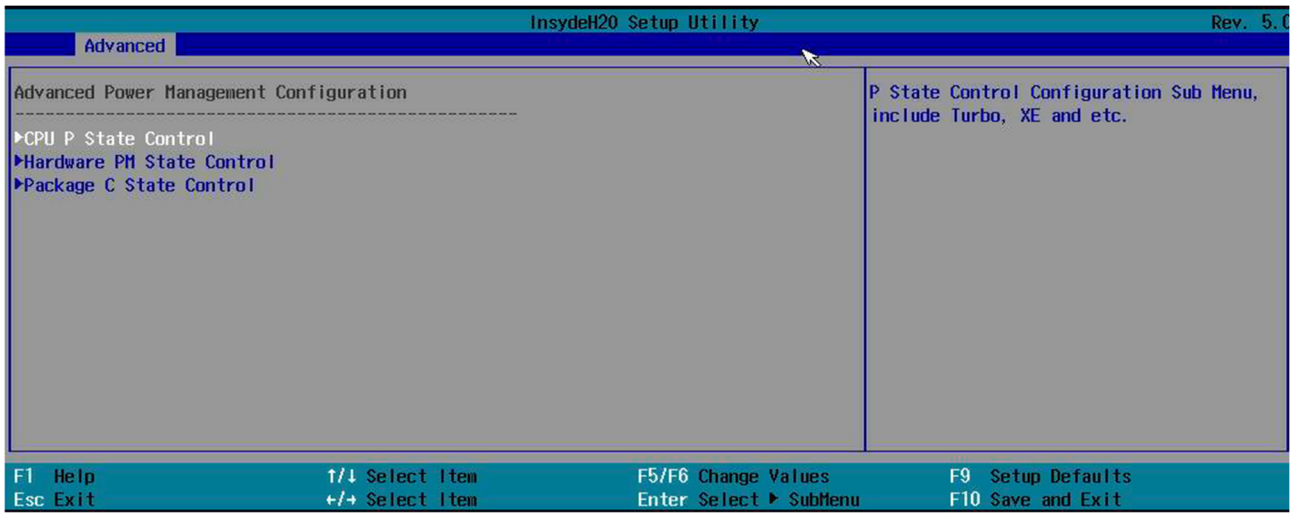
«IIO-PCIE Express Global Options» — этот раздел позволяет пользователю настроить следующие глобальные параметры PCI-E:

- «PCI 64-Bit Resource Allocation»;
- «PCIe Train by BIOS»;
- «PCIe Hot Plug» — выбрать «Включить», чтобы поддерживать горячее подключение для выбранных слотов PCI-E, что позволит пользователю заменять устройства, установленные в слотах, без выключения системы;

- «PCIe ACPI Hot Plug» — виртуальная платформа использует hotplug на основе ACPI, чтобы избавить пользователя от необходимости создавать иерархии PCIe только для поддержки hotplug. Это также избавляет от необходимости моделировать контроллеры PCIe, поддерживающие hotplug. Платформа virt использует горячий разъем на базе PCI для центрального процессора и памяти;
- «PCI-E Completion Timeout (Global) Disable» — использовать эту функцию, чтобы выбрать параметры тайм-аута завершения работы PCI-E;
- «PCI-E Global Timeout Value» — значение тайм-аута;
- «PCI-E ASPM Support (Global)». ASPM (Active-State Power Management) — технология активного энергосбережения для шины PCI Express, позволяющая отдельным линиям шины уменьшать мощность в зависимости от нагрузки за счет прекращения подачи пустых, не содержащих данных, сигналов. Базовая спецификация PCI Express определяет два уровня ASPM, которые предназначены для обеспечения возможности компенсировать повышенное энергосбережение с быстрым восстановлением до состояния L0.

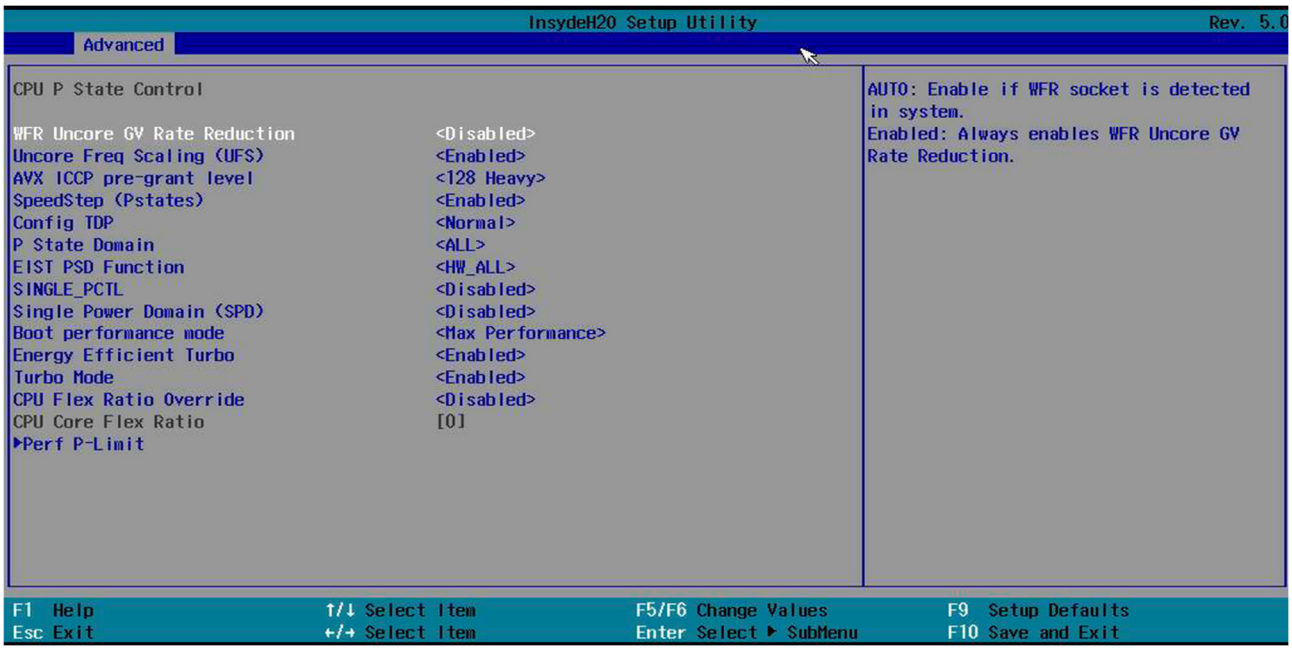
2.2.5.6. «Advanced Power Management Configuration» (рисунок 2.32). Продвинутые настройки питания.

Рисунок 2.32. «Advanced Power Management Configuration»



«CPU P State Control» (рисунок 2.33). Состояния P-state позволяют масштабировать частоту и напряжение, на которых работает процессор, чтобы снизить энергопотребление процессора. Количество доступных P-состояний может быть разным для каждой модели центрального процессора (ЦП), даже из одного семейства. C-state — это состояния, когда ЦП уменьшил или отключил выбранные функции.

Рисунок 2.33. «CPU P State Control»

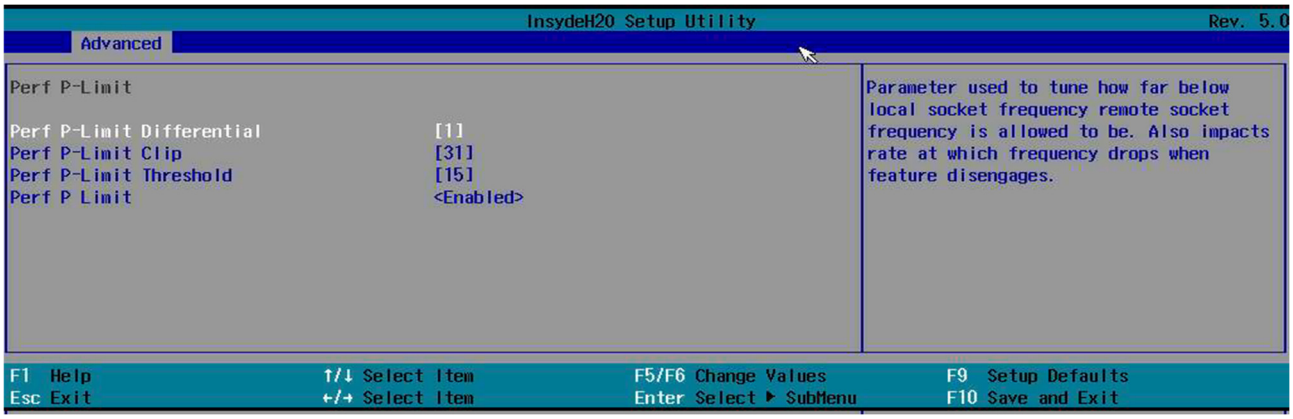


В окне на рисунке 2.33:

- «WFR Uncore GV Rate Reduction» — снижение скорости GV без учета WFR;
- «Uncore Freq Scaling (UFS)»— масштабирование частоты без ядра;
- «AVX ICCP pre-grant level» — позволяет системе выбирать между различными уровнями перехода AVX ICCP, предлагаемыми Intel;
- «SpeedStep (Pstates)» — серия технологий динамического масштабирования частоты (под кодовым названием Geyserville и включающая SpeedStep, SpeedStep II и SpeedStep III), встроенных в некоторые микропроцессоры Intel, которые позволяют программно динамически изменять тактовую частоту процессора (до различных P-состояний). Это позволяет процессору мгновенно удовлетворять потребности в производительности выполняемой операции, сводя к минимуму потребление энергии и выделение тепла;
- «Config TDP» — настраиваемые параметры TDP означают, что производитель компьютера может изменять базовую частоту и TDP;
- «P State Domain»;
- «EIST PSD Function» — EIST уменьшает задержку, связанную с изменением пары напряжение-частота (P-state), тем самым позволяя этим переходам происходить чаще. Это обеспечивает более точную коммутацию по требованию и может оптимизировать баланс мощности и производительности в зависимости от требований приложений;
- «SINGLE_PCTL» — единая модель PCTL заставляет все ядра в процессоре использовать самый последний запрос соотношения;
- «Single Power Domain (SPD)» — единый домен мощности объединяет запросы от всех ядер, и максимальное соотношение запросов применяется ко всем ядрам процессора;
- «Boot performance mode» — это параметр, определяющий производительность процессора, которая будет установлена сразу после запуска компьютера и не будет меняться в течение всей его работы ни при каких условиях;
- «Energy Efficient Turbo» — Energy Efficient Turbo сбрасывает множители турбо, когда ЦП обнаруживает, что ядро тратит слишком много времени на остановку;
- «Turbo Mode»;
- «CPU Flex Ratio Override» — переопределение коэффициента гибкости ЦП;
- «CPU Flex Ratio» — коэффициент гибкости ЦП;

- «Perf P-Limit» (рисунок 2.34) — позволяет осуществлять координацию частоты двух процессоров без использования ядра:

Рисунок 2.34. «Perf P-Limit»



1) «Perf P-Limit Differential» — параметр, используемый для настройки того, насколько ниже частоты локального сокета может быть частота удаленного сокета. Также влияет на скорость, с которой частота падает при отключении функции;

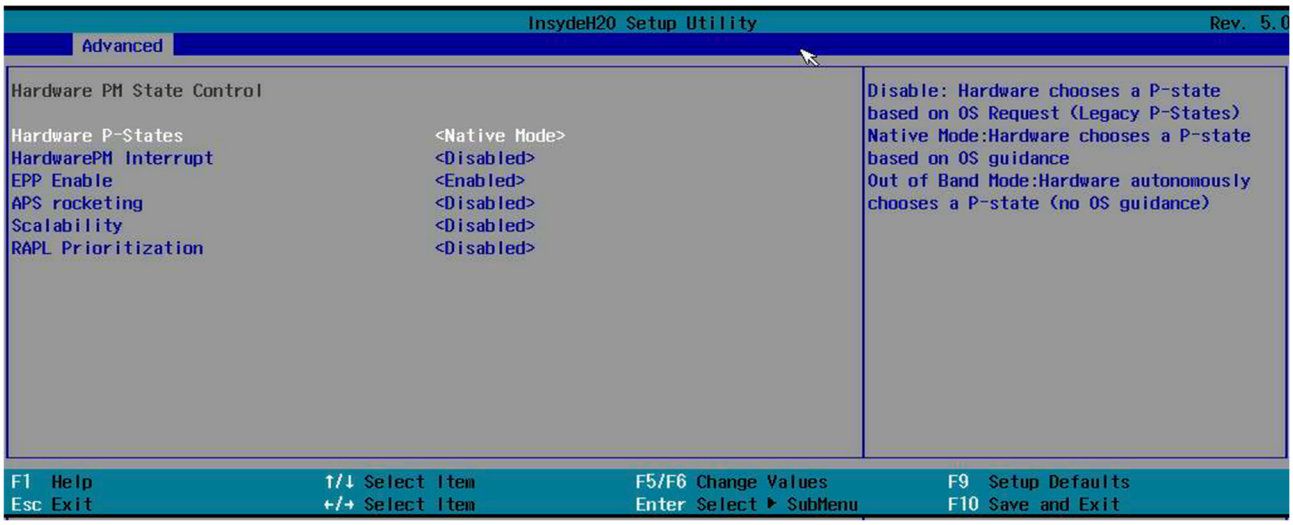
2) «Perf P-Limit Clip» — максимальное значение, которое может быть задано для нижнего предела производительности P-limit;

3) «Perf P-Limit Threshold» — порог частоты, выше которого этот сокет активирует функцию и начнет пытаться поднять частоту других сокетов;

4) «Perf P-Limit» — включение функции.

«Hardware PM State Control» (рисунок 2.35). Параметр Hardware P-State позволяет пользователю выбирать между P-состояниями, управляемыми ОС, и аппаратными средствами. Выбор собственного режима позволяет ОС выбирать P-состояние. Выбор внеполосного режима позволяет аппаратному обеспечению автономно выбирать P-state без указания ОС.

Рисунок 2.35. «Hardware PM State Control»



В окне «Hardware PM State Control»:

- «Hardware P-States»:

1) отключить: аппаратное обеспечение выбирает P-состояние на основе запроса ОС (устаревшие P-состояния);

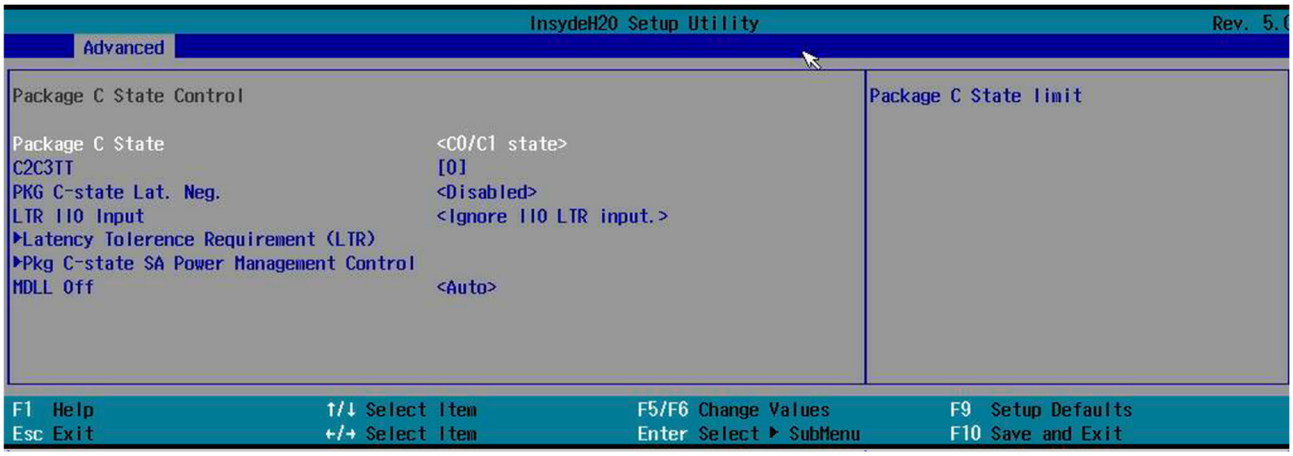
2) собственный режим: аппаратное обеспечение выбирает P-состояние на основе указаний ОС;

3) внеполосный режим: аппаратное обеспечение самостоятельно выбирает P-состояние (без указания ОС);

- «HardwarePM Interrupt» — включение прерывания;
- «EPP Enable» — данная опция позволяет включить «Enhanced Parallel Port» — это режим двунаправленной работы параллельного порта, при котором данные могут передаваться в оба направления со скоростью до 2 Мбайт/с;
- «APS rocketing» — включить/отключить ракетный механизм в алгоритме выбора P-состояния HP. Rocketing позволяет мгновенно увеличить соотношение ядер до максимального турбо, а не плавно;
- «Scalability» — включить/выключить использование масштабируемости в алгоритмы энергоэффективности HWP pcode. Масштабируемость — это мера предполагаемого улучшения производительности при заданном увеличении частоты ядра;
- «RAPL Prioritization» — позволяет создавать основные группы с разным приоритетом.

«Package C State Control» (рисунок 2.36).

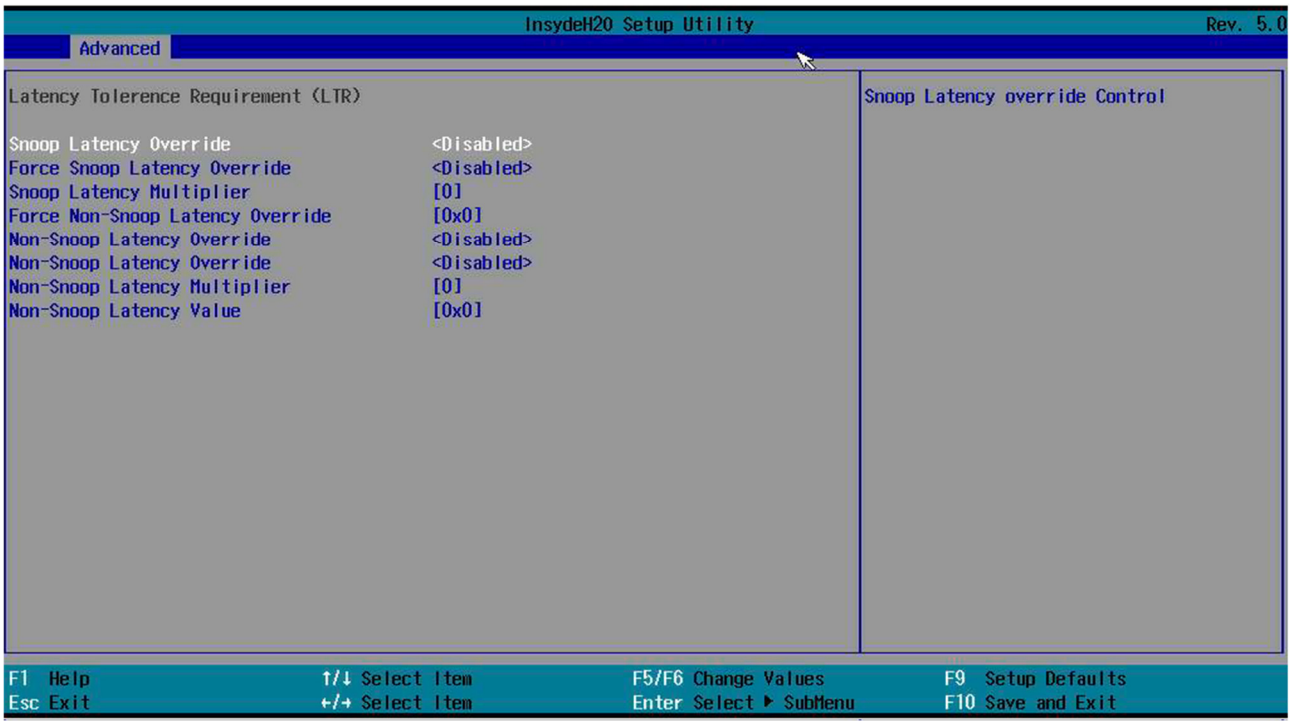
Рисунок 2.36. «Package C State Control»



В окне «Package C State Control»:

- «Package C State» — ограничение C State;
- «C2C3TT» — по умолчанию = 0, означает [AUTO].
  C2 to C3
  Таймер перехода, PPDN_INIT = 1:10:1:74
  Бит [11:01];
- «PKG C-State Lat. Neg» — включение функции, MSR 1FCh Bit [30] = PCH_NEG_DISABLE;
- «LTR IIO Input». LTR — это механизм, который позволяет конечным точкам отправлять информацию о своих требованиях к задержке для операций чтения/записи памяти и прерываний;
- «Latency Tolerance Requirement (LTR)» (рисунок 2.37):

Рисунок 2.37. «Latency Tolerance Requirement (LTR)»



1) «Snoop Latency Override» — управление отслеживанием. Отслеживание является частью реализации протокола когерентности кэша. Если когерентность кэша не требуется для корректного функционирования приложения/драйвера, можно выдавать неотслеживаемые транзакции, которые не отслеживают (потенциально более поздние) копии данных в кэшах, а напрямую считывают/записывают память;

2) «Force Snoop Latency Override» — управление усиленным отслеживанием;

3) «Snoop Latency Multiplier» — значение переопределения умножается на это поле, чтобы получить временное значение;

4) «Force Non-Snoop Latency Override» — управление отслеживанием;

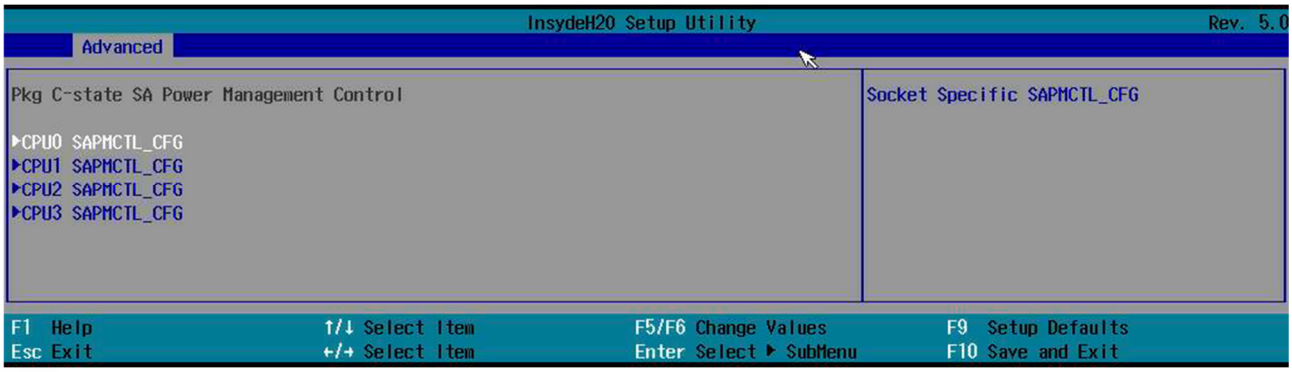
5) «Non-Snoop Latency Override» — управление отслеживанием;

6) «Non-Snoop Latency Multiplier»;

7) «Non-Snoop Latency Value»;

- «Pkg C-state SA Power Management Control» (рисунок 2.38) — настройки управления питания каждого ядра:

Рисунок 2.38. «Pkg C-state SA Power Management Control»



🕮 ПРИМЕЧАНИЕ

Пункты 1–4 имеют одинаковое наполнение.

1) «CPU0 SAPMCTL_CFG» (рисунок 2.39). SAPMCTL — System Agent Power Management Control. Усовершенствованная технология системного агента Intel SpeedStep® представляет собой динамическое масштабирование частоты напряжения системного агента на основе использования памяти. В отличие от ядра процессора и пакета Enhanced Intel SpeedStep® Technology System Agent Enhanced Intel SpeedStep® Technology имеет три действительные рабочие точки. При работе с небольшой рабочей нагрузкой и включенной технологии SA Enhanced Intel SpeedStep® скорость передачи данных DDR может измениться следующим образом: перед изменением скорости передачи данных DDR процессор устанавливает DDR на самообновление и изменяет необходимые параметры. Напряжение DDR остается стабильным и неизменным. Обучение BIOS/MRC DDR на максимальной, средней и минимальной частотах устанавливает параметры ввода-вывода и временные параметры.

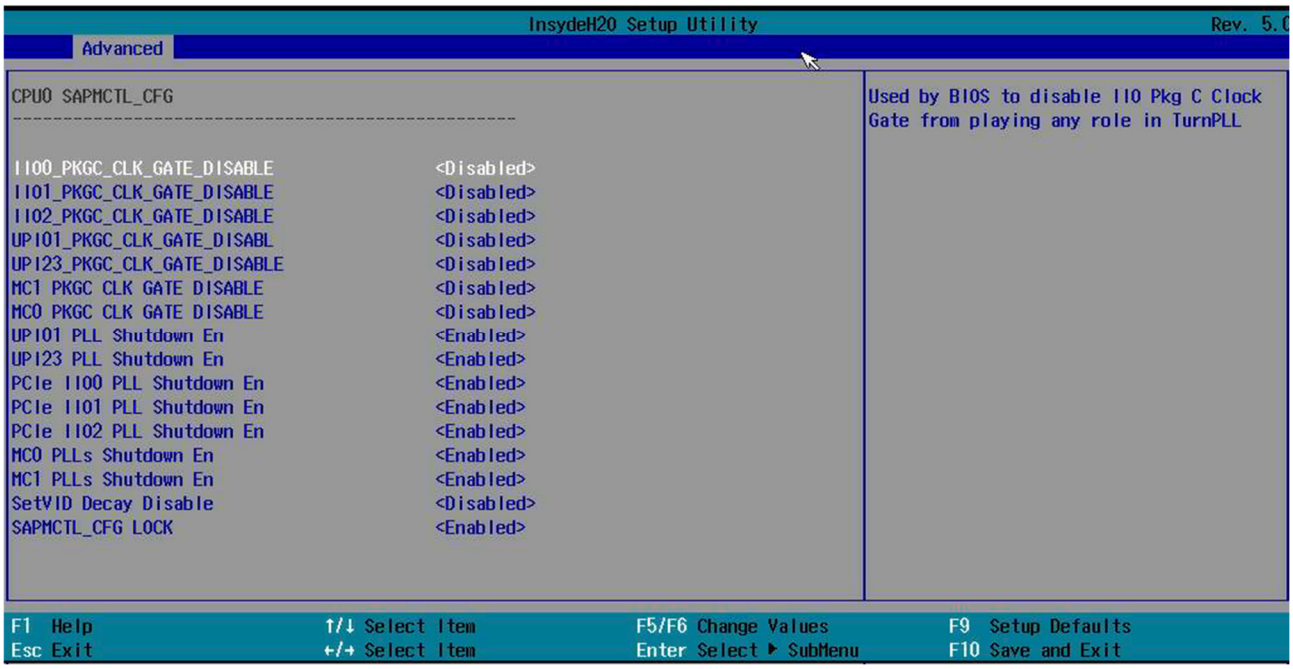
Специфическая конфигурация сокета — IO Package Clock Gate имеет возможность динамически стробировать каждый выходной счетчик PLL Intel® Stratix® 10 I/O. Это обеспечивает полезную альтернативу корневому шлюзу синхронизации, поскольку корневой шлюз синхронизации может стробировать только 1 из 9 выходных счетчиков. Однако тактовый шлюз PLL ввода-вывода не зависит от цикла. Когда используется тактовый шлюз ввода-вывода PLL, ожидается задержка в несколько тактовых циклов между установлением или снятием тактового шлюза и соответствующим изменением тактового сигнала. Количество циклов задержки не является детерминированным, поскольку сигнал разрешения должен быть синхронизирован с тактовой областью выходных тактовых импульсов, что гарантирует отсутствие сбоев в работе логического элемента.

QPI (QuickPath Interconnect) — это процессорное межсоединение «точка-точка», разработанное Intel, которое заменило внешнюю шину (FSB) в Xeon, Itanium и некоторых настольных платформах начиная с 2008 года. Это увеличило масштабируемость и доступную пропускную способность.

Контроллер PLL предлагает гибкость и удобство благодаря программно-конфигурируемым делителям (от PLLDIV1 до PLLDIV16) для внутренней модификации входного тактового сигнала. Контроллер PLL также содержит регистры (PLLM и SECCTL), которые используются для управления логикой PLLM, OUTPUT DIVIDE и YPASS PLL. Результирующие выходные сигналы от контроллера PLL передаются в ядро DSP, периферийные устройства и другие модули внутри устройства:

- «IIO0_PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «IIO1_PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «IIO2_PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «UPI01_ PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «UPI23_ PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «MC1_ PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «MC2_ PKGC_CLK_GATE_DISABLE» — отвечает за включение и отключение опции;
- «UPI01 PLL Shutdown En» — отвечает за включение и отключение опции;
- «UPI23 PLL Shutdown En» — отвечает за включение и отключение опции;
- «PCIe IIO0 PLL Shutdown En» — отвечает за включение и отключение опции;
- «PCIe IIO1 PLL Shutdown En» — отвечает за включение и отключение опции;
- «PCIe IIO2 PLL Shutdown En» — отвечает за включение и отключение опции;
- «MC0 PLLs Shutdown En» — отвечает за включение и отключение опции;
- «MC1 PLLs Shutdown En» — отвечает за включение и отключение опции;
- «Set VID Decay Disable» — отвечает за включение и отключение опции;
- «SAPMCTL_CFG LOCK»;

Рисунок 2.39. «CPU0 SAPMCTL_CFG»

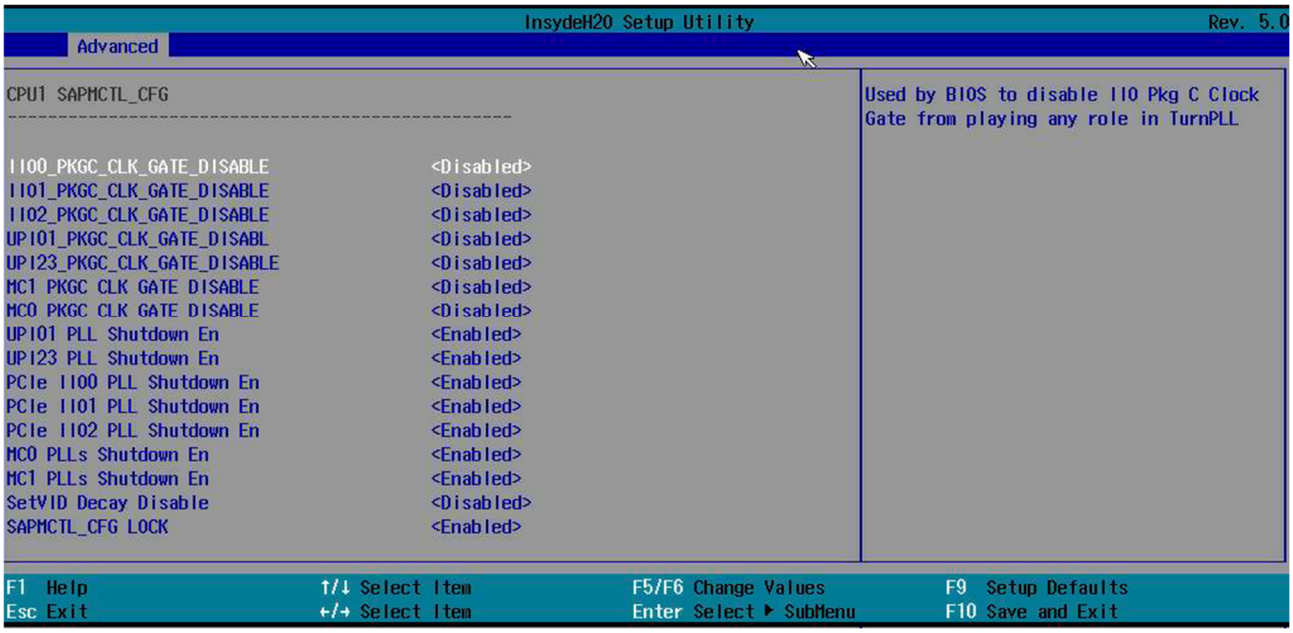


🕮 ПРИМЕЧАНИЕ

Данное описание является также верным для «CPU1 SAPMCTL_CFG», «CPU2 SAPMCTL_CFG», «CPU3 SAPMCTL_CFG» и их подпунктов.

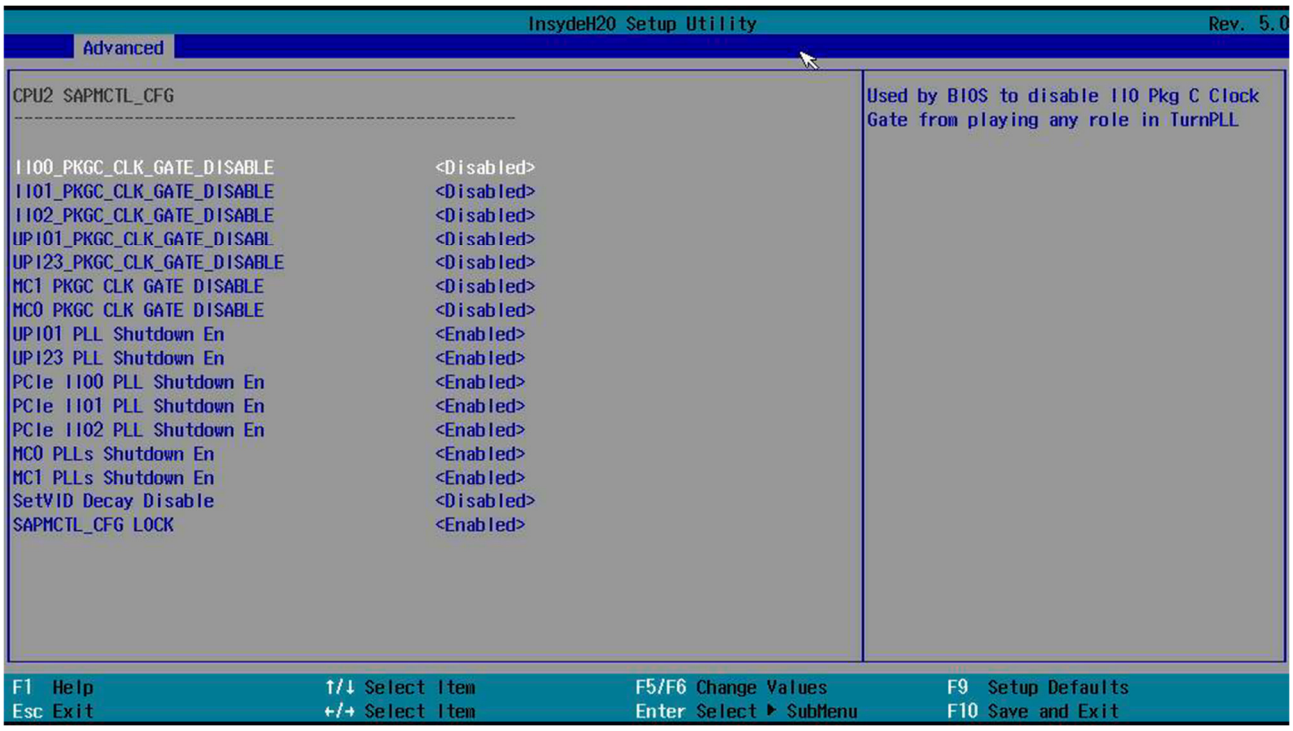
2) «CPU1 SAPMCTL_CFG» (рисунок 2.40);

Рисунок 2.40. «CPU1 SAPMCTL_CFG»



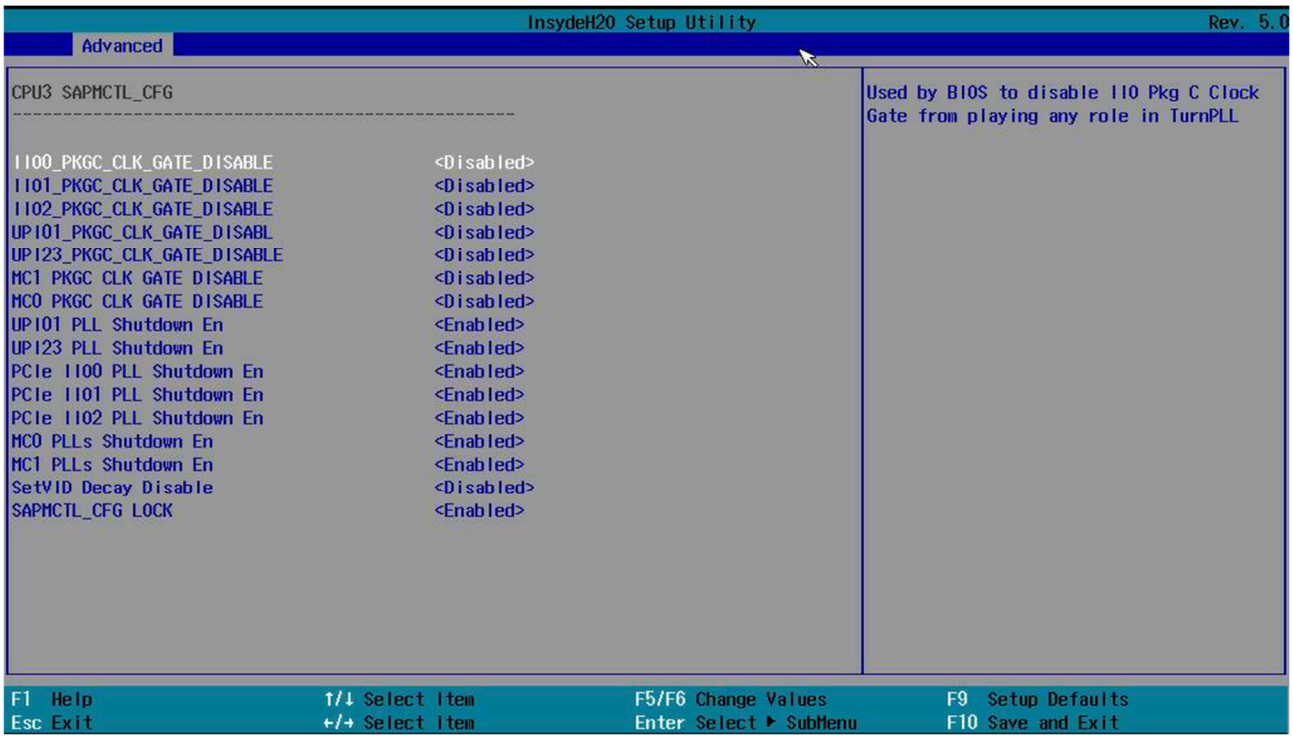
3) «CPU2 SAPMCTL_CFG» (рисунок 2.41);

Рисунок 2.41. «CPU2 SAPMCTL_CFG»



4) «CPU3 SAPMCTL_CFG» (рисунок 2.42);

Рисунок 2.42. «CPU3 SAPMCTL_CFG»



- «MDLL Off».

2.2.6. «ME Configuration»

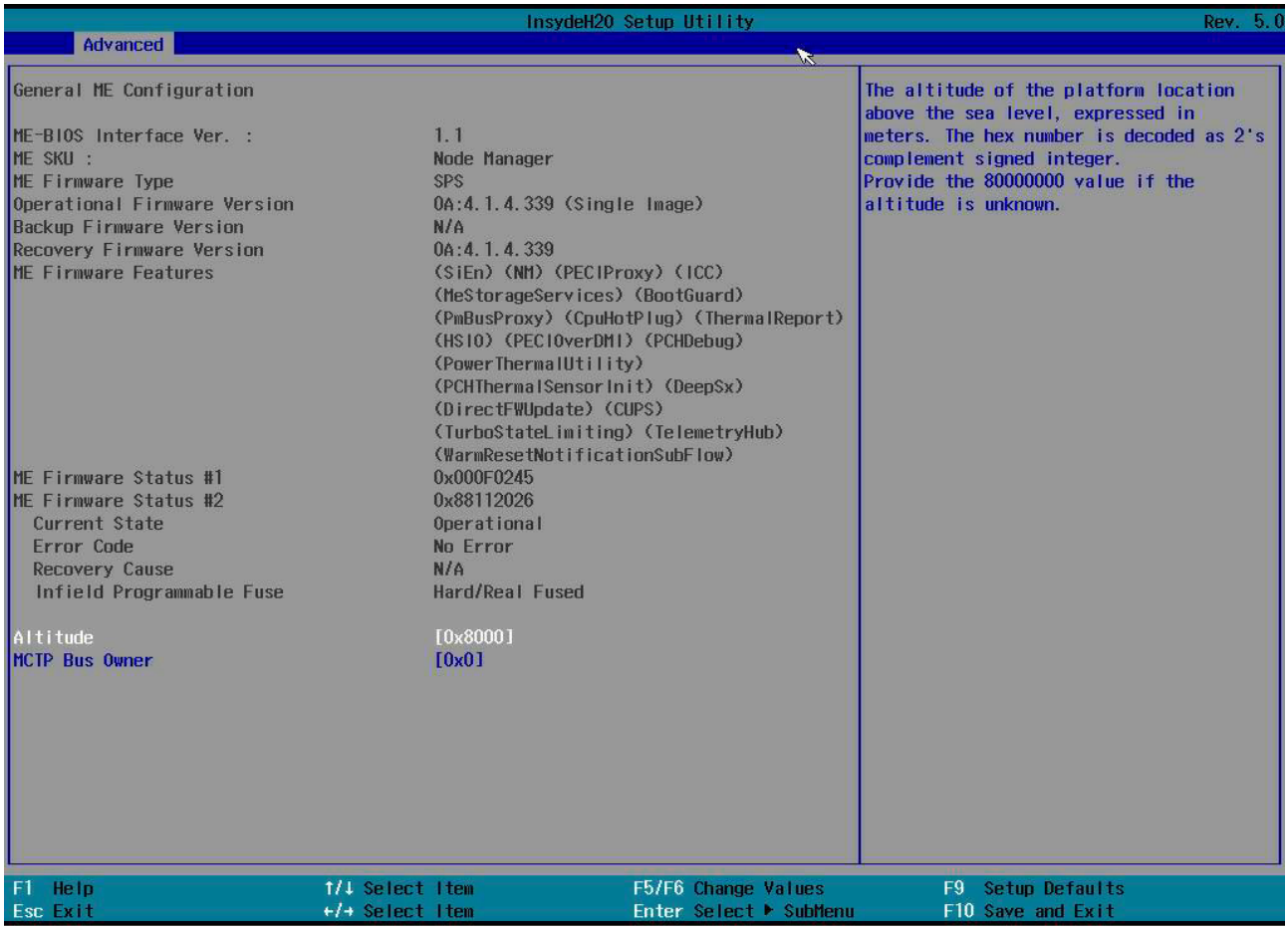
«ME Configuration» представлена на рисунке 2.43.

Рисунок 2.43. «ME Configuration»

2.2.6.1. «Server ME Configuration» (рисунок 2.44).

Конфигурация Intel ME включена в BIOS с помощью расширения BIOS Intel® Management Engine (Intel® MEBX). Intel MEBX предоставляет возможность изменять и/или собирать конфигурацию аппаратного обеспечения системы, передает ее микропрограмме управления и предоставляет пользовательский интерфейс конфигурации Intel ME.

Рисунок 2.44. «Server ME Configuration»



«Altitude» — высота расположения платформы над уровнем моря, выраженная в метрах. Шестнадцатеричный номер декодируется как целое число со знаком в дополнении 2'3. Указать значение 80000000, если высота неизвестна.

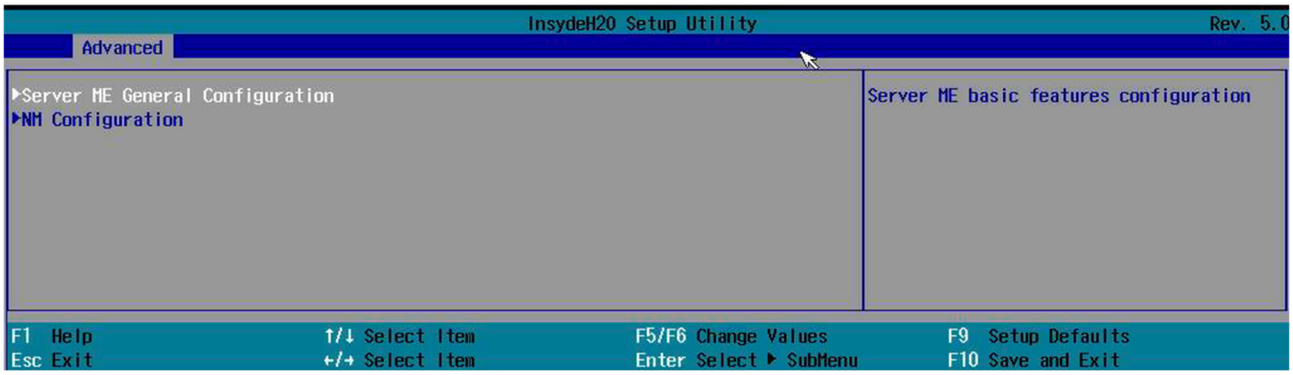
«MCTP Bus Owner» — расположение владельца шины MCTP на PCIe:

- [15:81] шина;
- [7:31] устройство;
- [2:01] функция.

Если все нули, то отправка шины владельцем отключена.

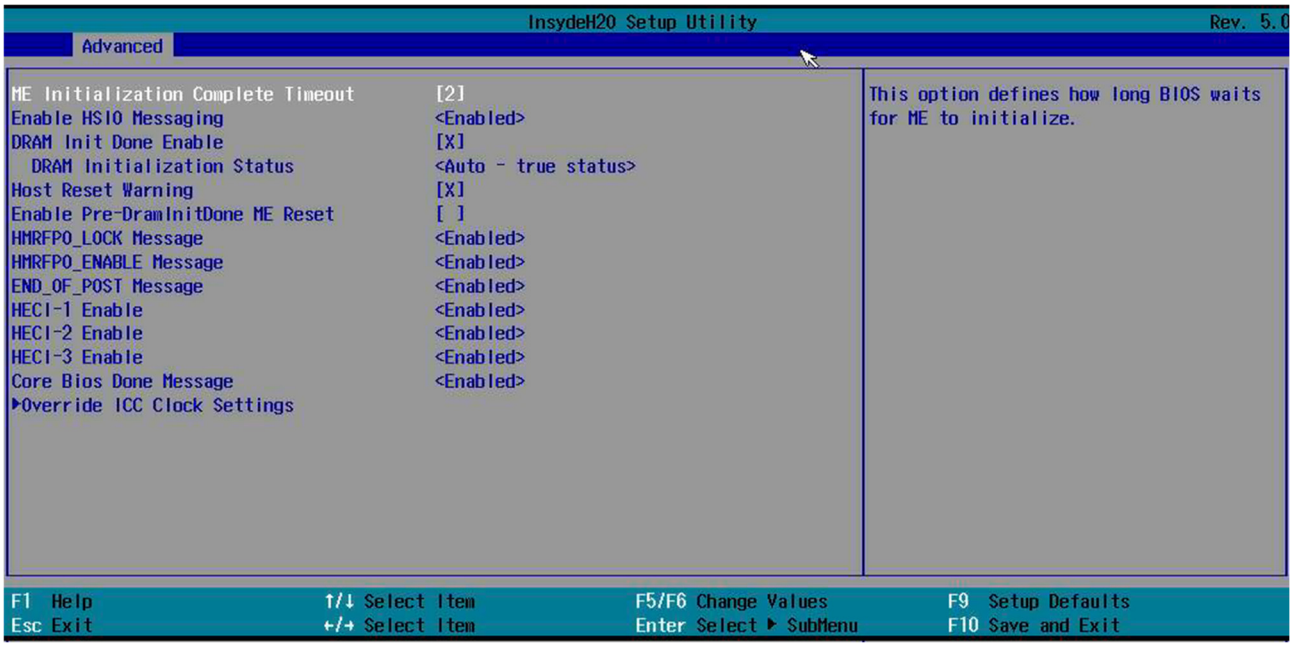
2.2.6.2. «Server ME Debug Configuration» (рисунок 2.45) — конфигурация параметров отладки прошивки Server ME.

Рисунок 2.45. «Server ME Debug Configuration»



«Server ME General Configuration» (рисунок 2.46):

Рисунок 2.46. «Server ME General Configuration»



В окне на рисунке 2.46:

- «ME Initialization Complete Timeout» — опция указывает, как долго BIOS ожидает инициализации ME;
- «Enable HSIO Messaging» — разрешить сообщения высокоскоростных линий ввода-вывода;
- «DRAM Init Done Enable» — сообщать или не сообщать ME об инициализации DRAM;
- «DRAM Initialization Status» — переопределение значение состояния инициализации DRAM;
- «Host Reset Warning» — сообщать ли ME о перезагрузке;
- «Enable Pre-DramInitDone ME Reset» — когда SPS находится в процессе восстановления, сбросить ME до сообщения DramInitDone;
- «HMRFPO_LOCK Message» — показывать сообщение;
- «HMRFPO_ENABLE Message» — показывать сообщение;
- «END_OF_POST Message» — показывать сообщение;
- «HECI-1 Enable» — переопределить статус (Host Embedded Controller Interface) HECI-1 на PCI или разрешить прошивке решать в зависимости от типа ME (авто);
- «HECI-2 Enable» — переопределить статус (Host Embedded Controller Interface) HECI-2 на PCI или разрешить прошивке решать в зависимости от типа ME (авто);
- «HECI-3 Enable» — переопределить статус (Host Embedded Controller Interface) HECI-3 на PCI или разрешить прошивке решать в зависимости от типа ME (авто);
- «Core Bios Done Message» — разрешать отправку сообщения о завершении загрузки в ME;
- «Override ICC Clock Settings» (рисунок 2.47):

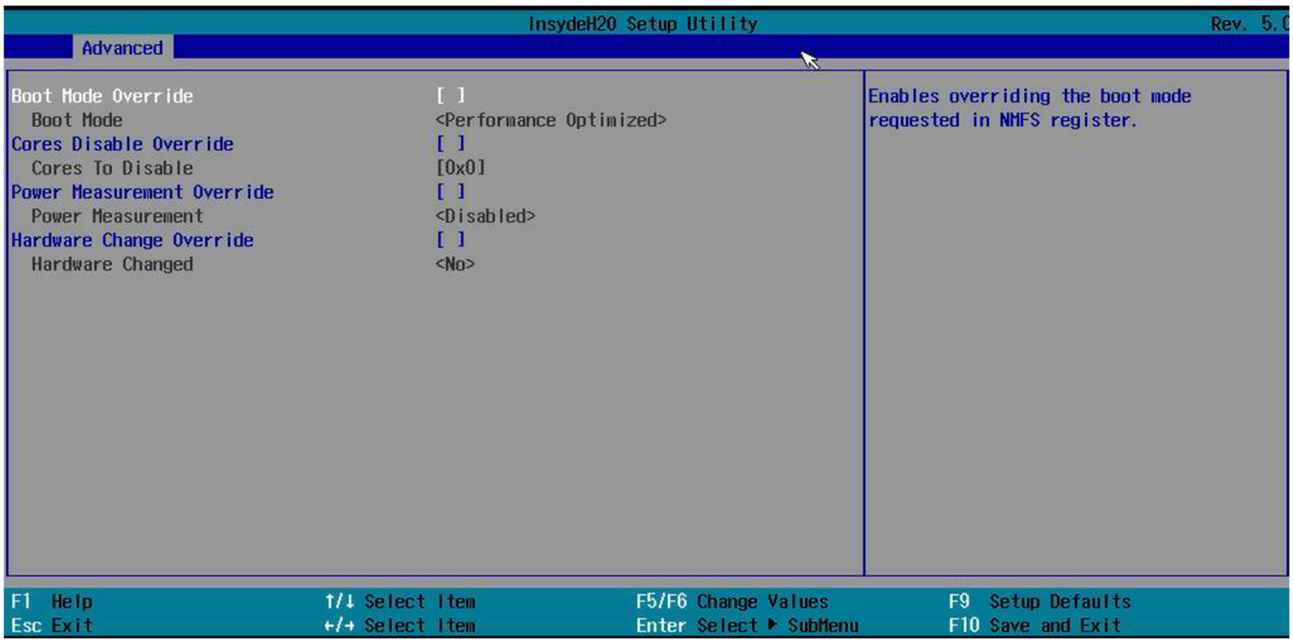
Рисунок 2.47. «Override ICC Clock Settings»

1) «Override ICC Clock Settings»;
2) «ICC Clock Spread Spectrum».

«NM Configuration» (рисунок 2.48):

- «Boot Mode Override» — настройка режима загрузки;
- «Boot Mode» — настройка приоритета производительности или оптимизации питания;
- «Cores Disable Override» — настройка ядер;
- «Cores To Disable» — выбор ядер для отключения;
- «Power Measurement Override» — включение измерения питания;
- «Power Measurement» — включение измерения питания;
- «Hardware Change Override» — отмена аппаратного изменения;
- «Hardware Changed».

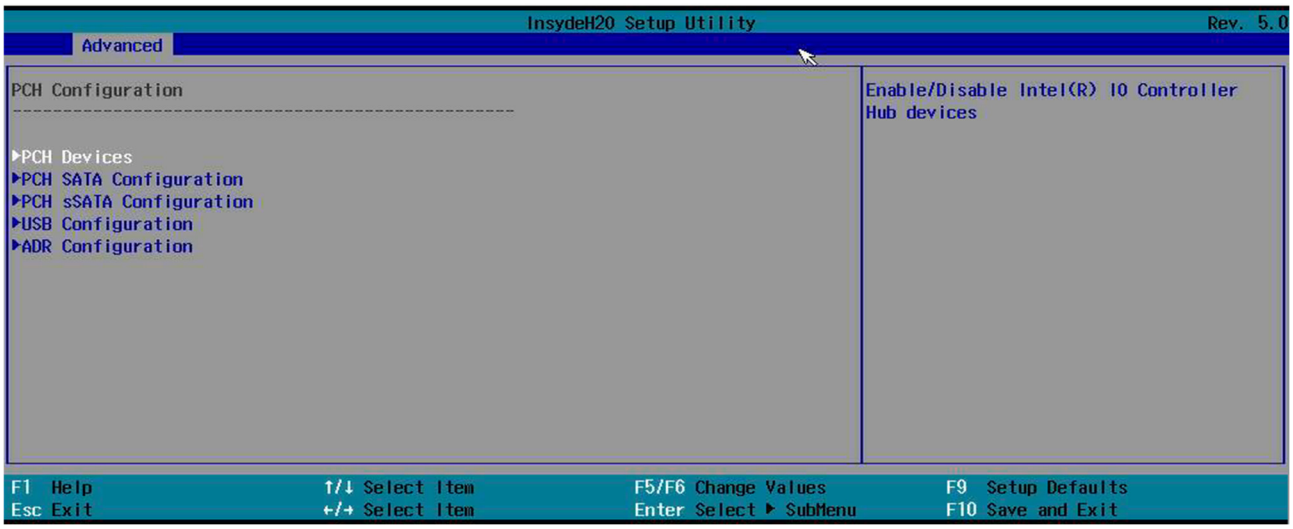
Рисунок 2.48. «NM Configuration»



2.2.7. «Pch Configuration»

PCH (рисунок 2.49) управляет определенными путями данных и функциями поддержки, используемыми в сочетании с процессорами Intel. К ним относятся синхронизация (системные часы), гибкий интерфейс дисплея (FDI) и прямой интерфейс мультимедиа (DMI), хотя FDI используется только тогда, когда набор микросхем требуется для поддержки процессора со встроенной графикой.

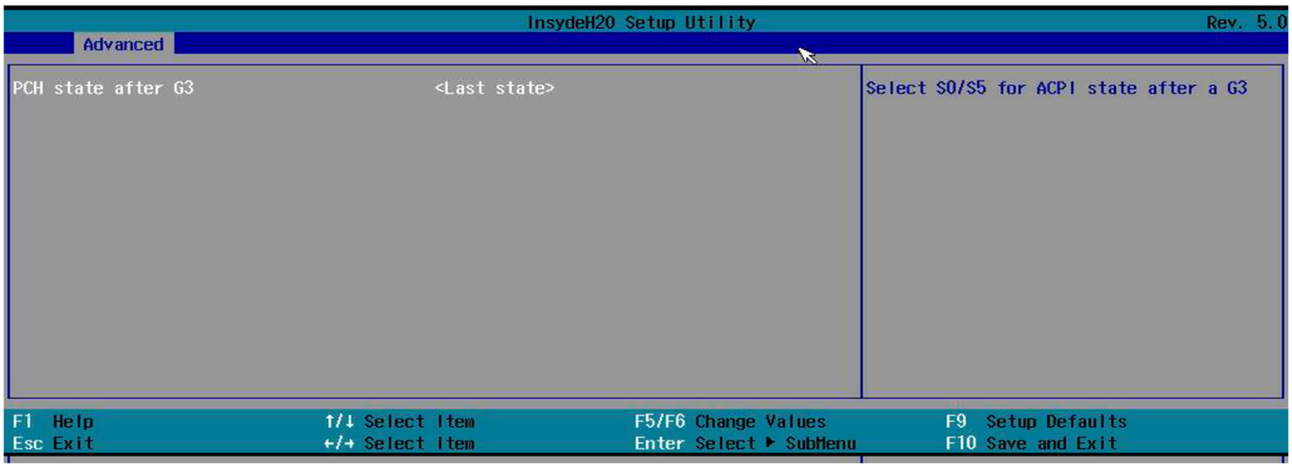
Рисунок 2.49. «Pch Configuration»



2.2.7.1. «PCH Devices» (рисунок 2.50) — настройка для устройств.

«PCH state after G3».

Рисунок 2.50. «PCH Devices»



2.2.7.2. «PCH SATA Configuration» (рисунок 2.51) — устройства и настройки SATA.

Опции для каждого порта одинаковы:

- «SATA Controller» — включить поддержку контроллера;
- «Configure SATA as» — указать, как подключена шина;
- «Support Aggressive Link Power Management». При включении через контроллер AHCI позволяет адаптеру главной шины SATA переходить в состояние пониженного энергопотребления в периоды бездействия, тем самым экономя энергию. Недостатком этого является повышенная периодическая задержка, поскольку накопитель необходимо повторно активировать и снова подключить к сети, прежде чем его можно будет использовать, и это часто воспринимается конечным пользователем как задержка;
- «SATA Port 0» — состояние порта;
- «Software Preserve»;
- «Port 0» — включение порта;
- «SATA Port 0 DevSlp» — DevSlp или DevSleep (иногда называемая спящим режимом устройства или SATA DEVSLP) — это функция некоторых устройств SATA, которая позволяет им переходить в «спящий режим» с низким энергопотреблением при отправке соответствующего сигнала, который потребляет на один или два порядка меньше энергии, чем традиционный режим ожидания (около 5 мВт, но некоторые диски могут потреблять всего 2,5 мВт). Эта функция была представлена SanDisk в партнерстве с Intel. Некоторые считают, что благодаря этой инициативе ноутбуки будут включаться почти мгновенно, в то время как другие заявляют, что это означает, что ноутбуки могут оставаться включенными все время и всегда быть доступными без негативного влияния на срок службы батареи. В традиционных режимах с низким энергопотреблением канал SATA по-прежнему должен оставаться включенным, чтобы устройство могло получить команду пробуждения. С DevSlp редко используемые контакты 3,3 В разъема питания SATA будут использоваться для сигнала DevSlp вместо обеспечения питания 3,3 В. Этот сигнал может разбудить диск и позволит отключить канал SATA, что еще больше снизит энергопотребление. Из-за того, как они работают, диски с поддержкой DevSleep могут не подходить для большинства настольных ПК и некоторых ноутбуков с напряжением 3,3 В, присутствующим в их разъемах питания SATA. Наличие 3,3 В приводит к тому, что диски с поддержкой DevSleep остаются в состоянии DevSlp. Несовместимость между материнской платой для настольных ПК и твердотельным накопителем SATA может быть

решена путем отключения функции DevSleep с помощью адаптера разъема питания, не пропускающего линию 3,3 В;
- «Hot Plug» — разрешить горячую замену;
- «Configure as eSATA» — настроить как eSATA;
- «Mechanical Presence Switch» — управляет отчетами о наличии на этом порте механического переключателя присутствия;

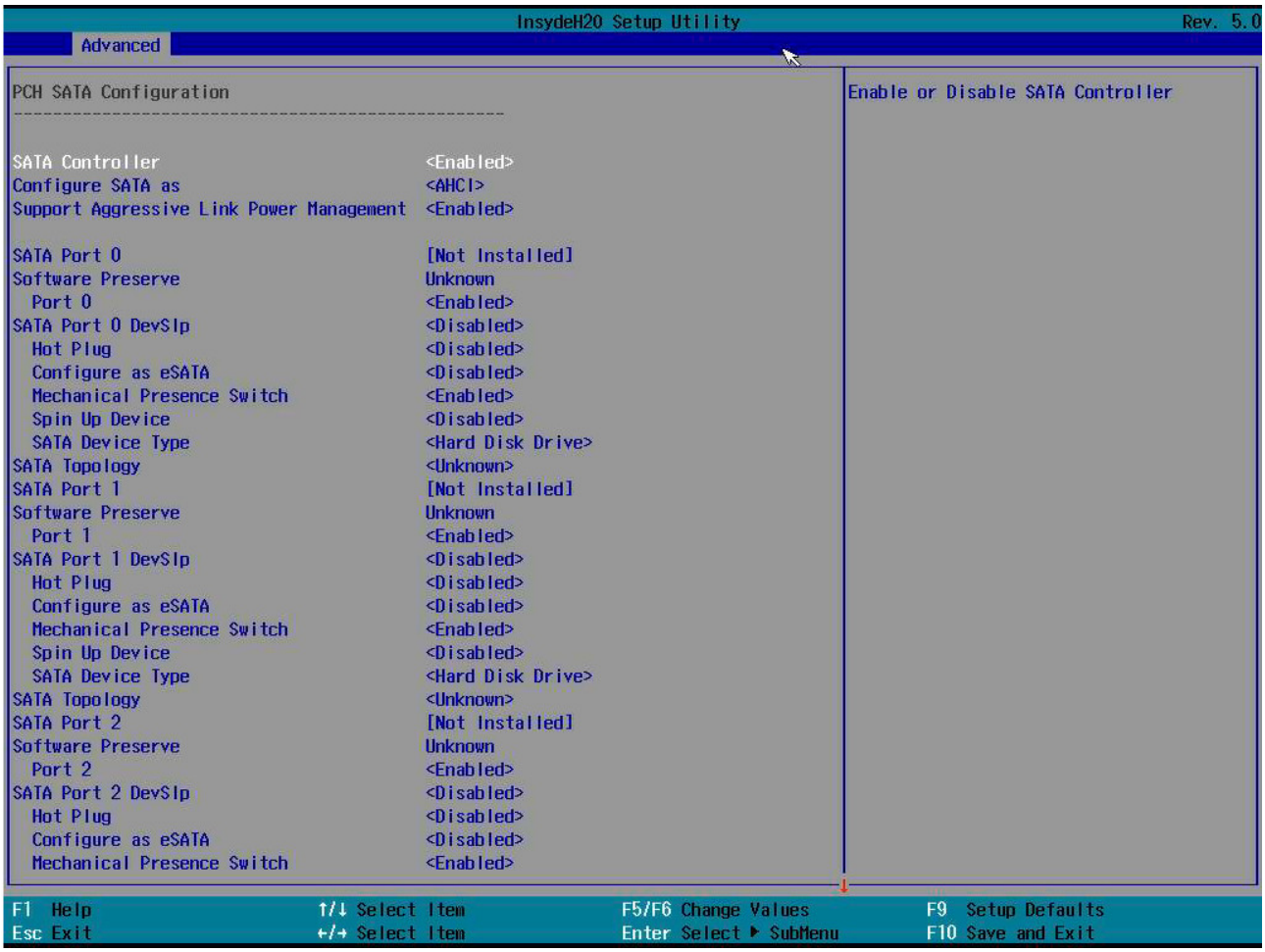
🕮 ПРИМЕЧАНИЕ

Требуется аппаратная поддержка.

- «Spin Up Device» — если включено для любого из портов, будет выполняться поэтапное раскручивание, и только диски, для которых включена эта опция, будут раскручиваться при загрузке. В противном случае все диски раскручиваются при загрузке;
- «SATA Device Type» — указать тип устройства;
- «SATA Topology» — определить топологию SALA, если это топология по умолчанию, ISATA, Flex, DirectConnect или M2;
- «SATA Port 1»;
- «Software Preserve»;
- «Port 1»;
- «SATA Port 1 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «SATA Port 2»;
- «Software Preserve»;
- «Port 2»;
- «SATA Port 2 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «SATA Port 3»;
- «Software Preserve»;
- «Port 3»;
- «SATA Port 0 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «Serial ATA Port 4»;
- «Software Preserve»;
- «Port 4»;
- «SATA Port 4 DevSlp»;

- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «Serial ATA Port 5»;
- «Software Preserve»;
- «Port 5»;
- «SATA Port 5 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «SATA Port 6»;
- «Software Preserve»;
- «Port 6»;
- «SATA Port 6 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «SATA Port 7 Software Preserve»;
- «Port 7»;
- «SATA Port 7 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology».

Рисунок 2.51. «PCH SATA Configuration»



2.2.7.3. «PCH sSATA Configuration» (рисунок 2.52) — устройства и настройки SATA.

Опции для каждого порта одинаковы:

- «sSATA Controller» — включить поддержку контроллера;
- «Support Aggressive Link Power Management». При включении через контроллер AHCI позволяет адаптеру главной шины SATA переходить в состояние пониженного энергопотребления в периоды бездействия, тем самым экономя энергию. Недостатком этого является повышенная периодическая задержка, поскольку накопитель необходимо повторно активировать и снова подключить к сети, прежде чем его можно будет использовать, и это часто воспринимается конечным пользователем как задержка;
- «sSATA Port 0» — состояние порта;
- «Software Preserve»;
- «Port 0» — включение порта;
- «sSATA Port 0 DevSlp». DevSlp или DevSleep (иногда называемая спящим режимом устройства или SATA DEVSLP) — это функция некоторых устройств SATA, которая позволяет им переходить в «спящий режим» с низким энергопотреблением при отправке соответствующего сигнала, который потребляет на один или два порядка меньше энергии, чем традиционный режим ожидания (около 5 мВт, но некоторые диски могут потреблять всего 2,5 мВт). Эта функция была представлена SanDisk в партнерстве с Intel. Некоторые считают, что благодаря этой инициативе ноутбуки будут включаться почти мгновенно, в то время как другие заявляют, что это означает, что ноутбуки могут оставаться включенными все время и всегда быть доступными без негативного влияния на срок службы батареи. В традиционных режимах с низким энергопотреблением канал

SATA по-прежнему должен оставаться включенным, чтобы устройство могло получить команду пробуждения. С DevSlp редко используемые контакты 3,3 В разъема питания SATA будут использоваться для сигнала DevSlp вместо обеспечения питания 3,3 В. Этот сигнал может разбудить диск и позволит отключить канал SATA, что еще больше снизит энергопотребление. Из-за того, как они работают, диски с поддержкой DevSleep могут не подходить для большинства настольных ПК и некоторых ноутбуков с напряжением 3,3 В, присутствующим в их разъемах питания SATA. Наличие 3,3 В приводит к тому, что диски с поддержкой DevSleep остаются в состоянии DevSlp. Несовместимость между материнской платой для настольных ПК и твердотельным накопителем SATA может быть решена путем отключения функции DevSleep с помощью адаптера разъема питания, не пропускающего линию 3,3 В;

- «Hot Plug» — разрешать горячую замену;
- «Configure as eSATA» — настроить как eSATA;
- «Mechanical Presence Switch» — управляет отчетами о наличии на этом порту механического переключателя присутствия;

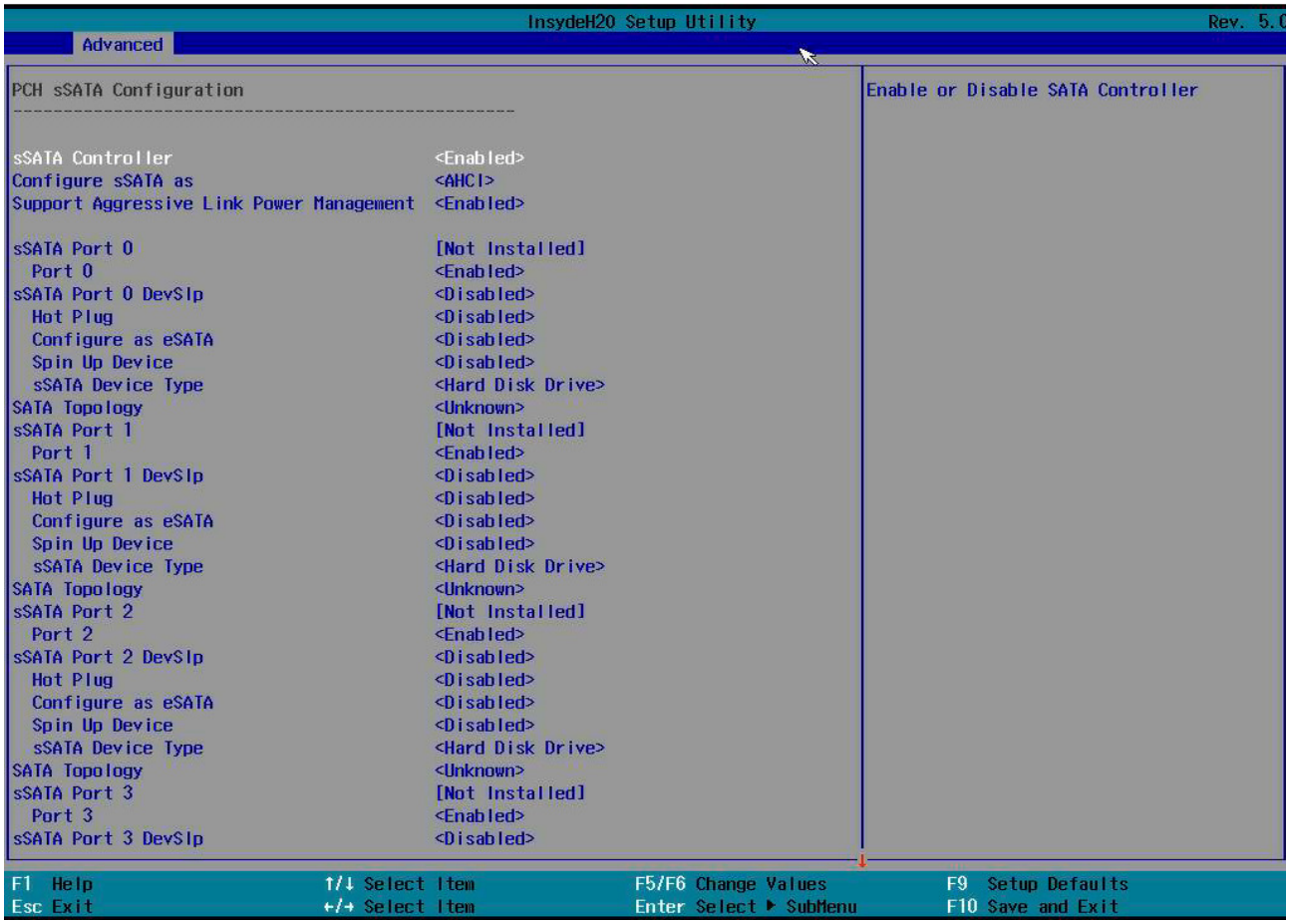
🕮 ПРИМЕЧАНИЕ

Требуется аппаратная поддержка.

- «Spin Up Device». Если включено для любого из портов, будет выполняться поэтапное раскручивание, и только диски, для которых включена эта опция, будут раскручиваться при загрузке. В противном случае все диски раскручиваются при загрузке;
- «sSATA Device Type» — указать тип устройства;
- «SATA Topology» — определить топологию SATA, если это топология по умолчанию, ISATA, Flex, DirectConnect или M2;
- «sSATA Port 1»;
- «Software Preserve»;
- «Port 1»;
- «sSATA Port 1 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «sSATA Device Type»;
- «SATA Topology»;
- «sSATA Port 2»;
- «Software Preserve»;
- «Port 2»;
- «sSATA Port 2 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «sSATA Device Type»;
- «SATA Topology»;
- «sSATA Port 3»;
- «Software Preserve»;
- «Port 3»;
- «sSATA Port 0 DevSlp»;
- «Hot Plug»;

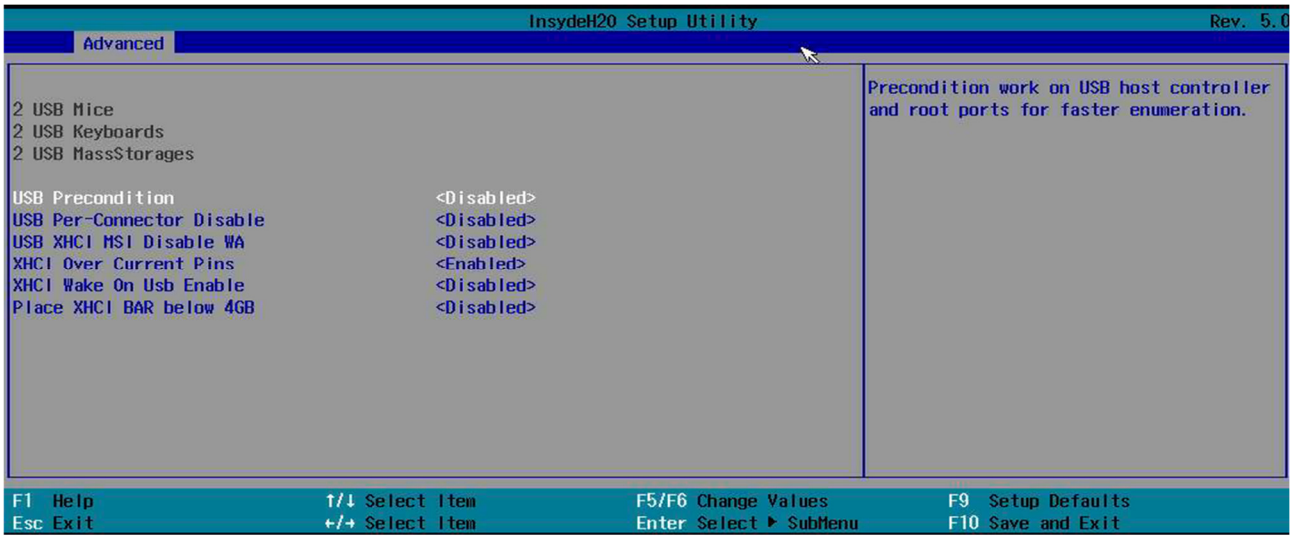
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «sSATA Device Type»;
- «SATA Topology»;
- «sSATA Port 4»;
- «Software Preserve»;
- «Port 4»;
- «SATA Port 4 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «SATA Device Type»;
- «SATA Topology»;
- «Serial ATA Port 5»;
- «Software Preserve»;
- «Port 5»;
- «sSATA Port 5 DevSlp»;
- «Hot Plug»;
- «Configure as eSATA»;
- «Mechanical Presence Switch»;
- «Spin Up Device»;
- «sSATA Device Type»;
- «SATA Topology».

Рисунок 2.52. «PCH sSATA Configuration»



2.2.7.4. «USB Configuration» (рисунок 2.53) — конфигурация и настройка USB:

Рисунок 2.53. «USB Configuration»



- «USB Precondition» — условие работы на хост-контроллере USB и корневых портах для более быстрого перечисления;
- «USB Per-Connector Disable» — выборочное включение/выключение каждого физического разъема USB (физического порта). После отключения разъема любые USB-устройства, подключенные к разъему, не будут обнаружены ни BIOS, ни ОС;
- «USB XHCI MSI Disable WA» — расширяемый интерфейс хост-контроллера (xHCI) — спецификация компьютерного интерфейса, которая определяет описание на уровне

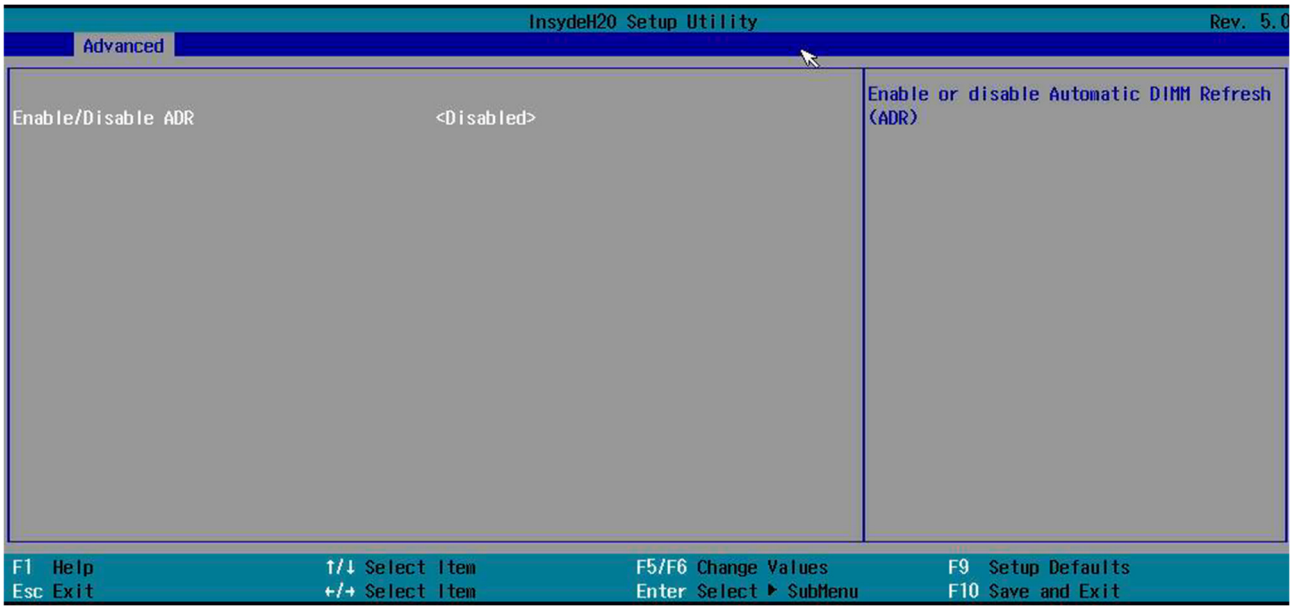
регистров хост-контроллера для универсальной последовательной шины (USB), который может взаимодействовать с устройствами, совместимыми с USB 1.x, 2.0 и 3.x. Спецификация также называется спецификацией хост-контроллера USB 3.0;

- «XHCI Over Current Pins»;
- «XHCI Wake On Usb Enable»;
- «Place XHCI BAR below 4GB».

2.2.7.5. «ADR Configuration» (рисунок 2.54) — конфигурация автоматического обновления DIMM:

- «Enable/Disable ADR».

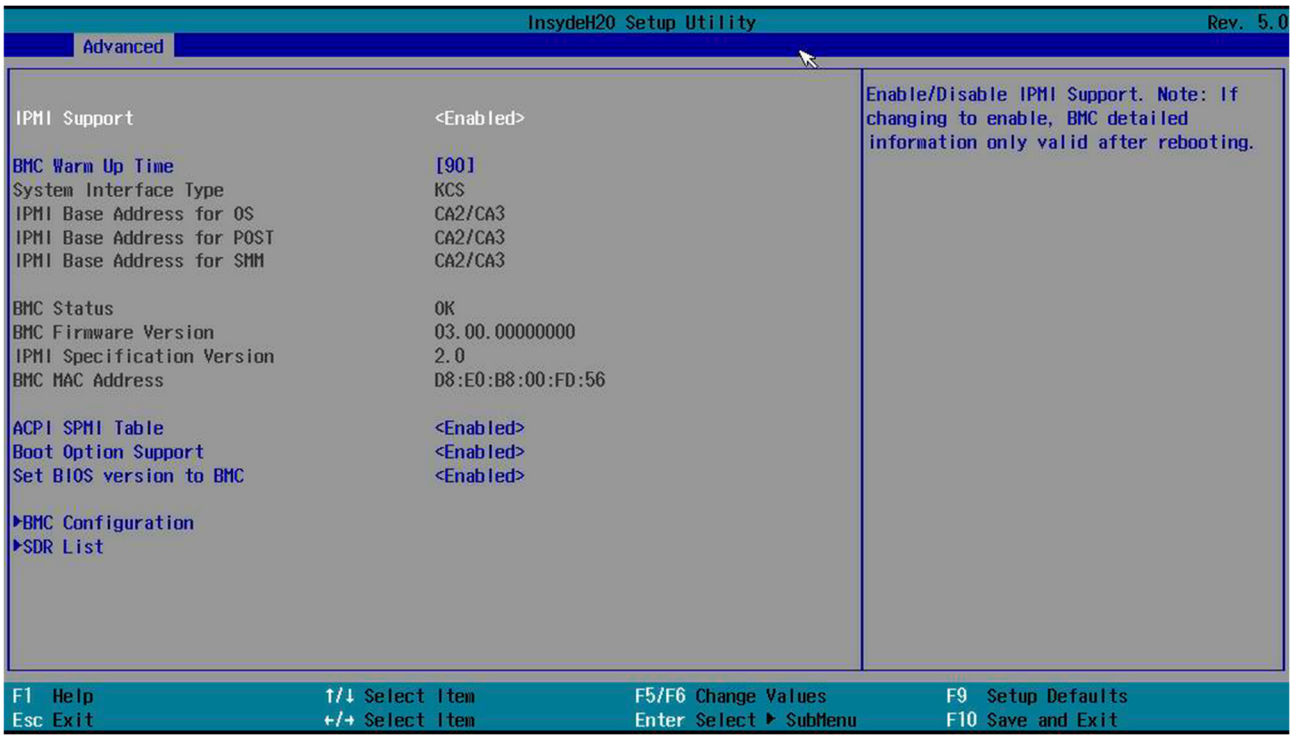
Рисунок 2.54. «ADR Configuration»



2.2.8. «H2O IPMI Configuration»

Настройка и конфигурация BMC/IPMI (рисунок 2.55).

Рисунок 2.55. «H2O IPMI Configuration»



2.2.8.1. «IPMI Support» — поддержка IPMI.

2.2.8.2. «BMC Warm up Time» — время ожидания от POST до запуска BMC.

2.2.8.3. «ACPI SPMI Table» — включение таблицы устройств ACPI SPMI.

ACPI — открытый промышленный стандарт, впервые выпущенный в декабре 1996 года и разработанный совместно компаниями HP, Intel, Microsoft, Phoenix и Toshiba, который определяет общий интерфейс для обнаружения аппаратного обеспечения, управления питанием и конфигурации материнской платы и устройств.

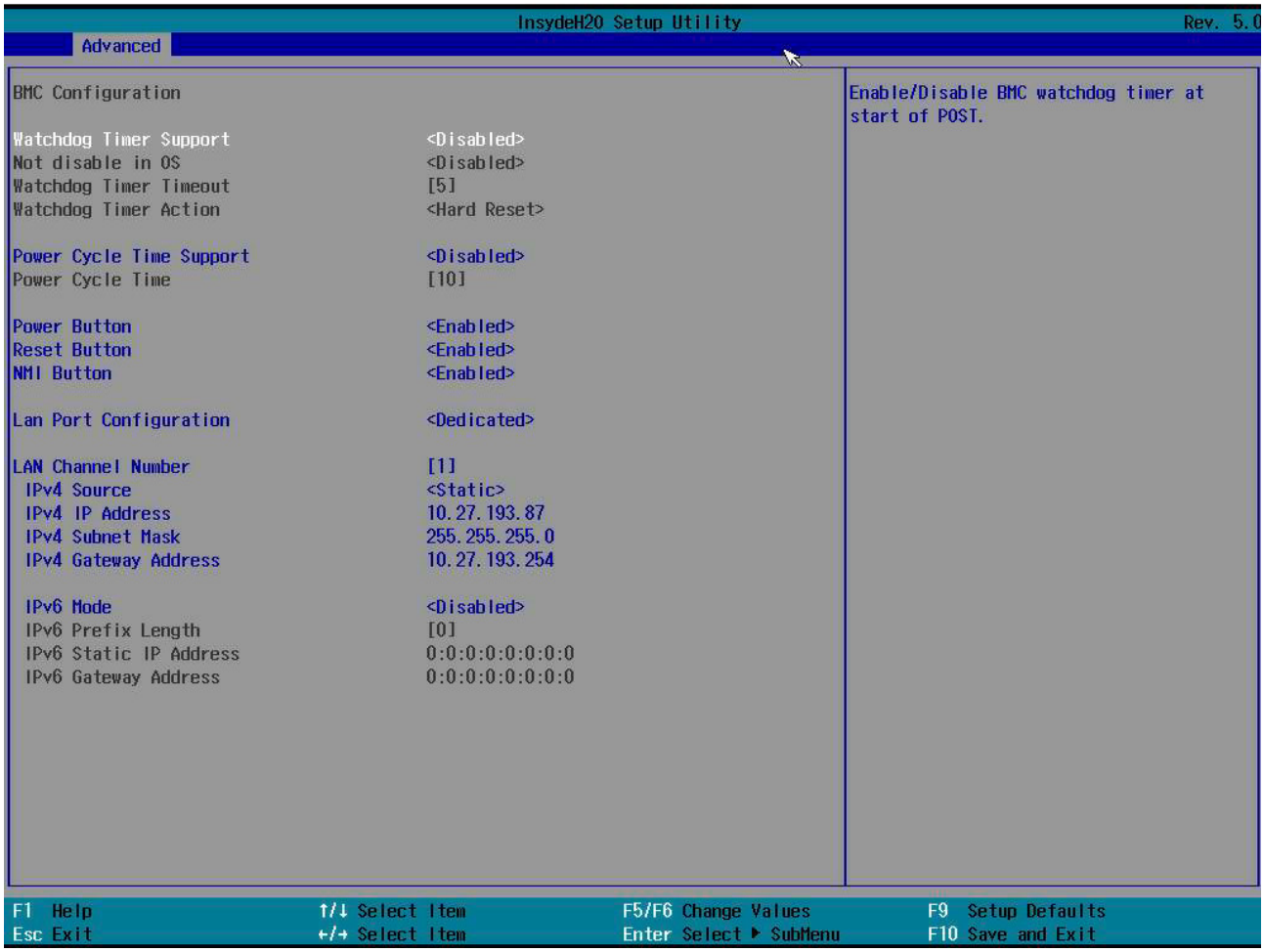
Интерфейс управления питанием системы (SPMI) — это высокоскоростная двунаправленная двухпроводная последовательная шина с малой задержкой, подходящая для управления в режиме реального времени многоядерными процессорами приложений с масштабированием напряжения и частоты, а также для управления питанием вспомогательных компонентов.

2.2.8.4. «Boot Option Support» — включает функцию загрузки IPMI.

2.2.8.5. «Set Bios Version to BMC» — если этот параметр включен, BIOS отправит строку версии BIOS в BMC во время POST.

2.2.8.6. «BMC Configuration» (рисунок 2.56) — настройка BMC.

Рисунок 2.56. «BMC Configuration»



«Watchdog Timer Support» — включить таймер, отслеживающий старт во время POST.

«Not Disable in OS» — не разрешать отслеживать во время загрузки ОС.

«Watchdog Timer Timeout» — введите количество минут, в течение которых системная прошивка должна загрузить ОС, прежде чем она выполнит действие тайм-аута. Допустимые значения: от 2 до 8 минут.

«Watchdog Time Action» — выбор действия по достижении тайм-аута:

- никаких действий;
- жесткая перезагрузка;
- выключение питания;
- перезагрузка питания.

«Power Cycle Time Support» — разрешать отправлять BMC команду на перезагрузку по тайм-ауту.

«Power Cycle Time» — срок тайм-аута.

«Power Button» — разрешить действие кнопки питания.

«Reset Button» — разрешить действие кнопки перезагрузки.

«NMI Button» — Non-Maskable-Interrupt обычно является предпочтительным методом перезагрузки SP, если он переходит в зависшее состояние (не отвечает на команды программного обеспечения).

«Lan Port Configuration» — настройка доступа LAN порта.

«LAN Channel Number».

«IPv4 Source» — ручная настройка или получение настроек по DHCP.

«IPv4 IP Address» — адрес IPv4.

«IPv4 Subnet Mask» — маска сети.

«IPv4 Gateway Address» — шлюз.

«IPv6 Mode» — разрешить IPv6.

«IPv6 Prefix Length» — маска.

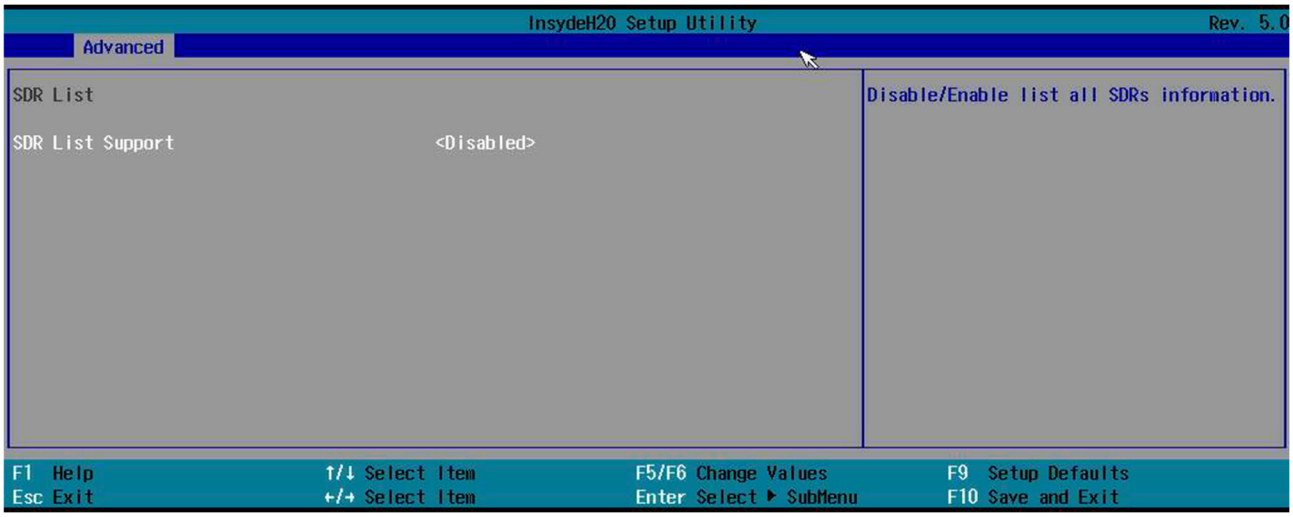
«IPv6 Static IP Address» — адрес IPv6.

«IPv6 Gateway Address» — шлюз.

2.2.8.7. «SDR List» (рисунок 2.57).

«SDR List Support».

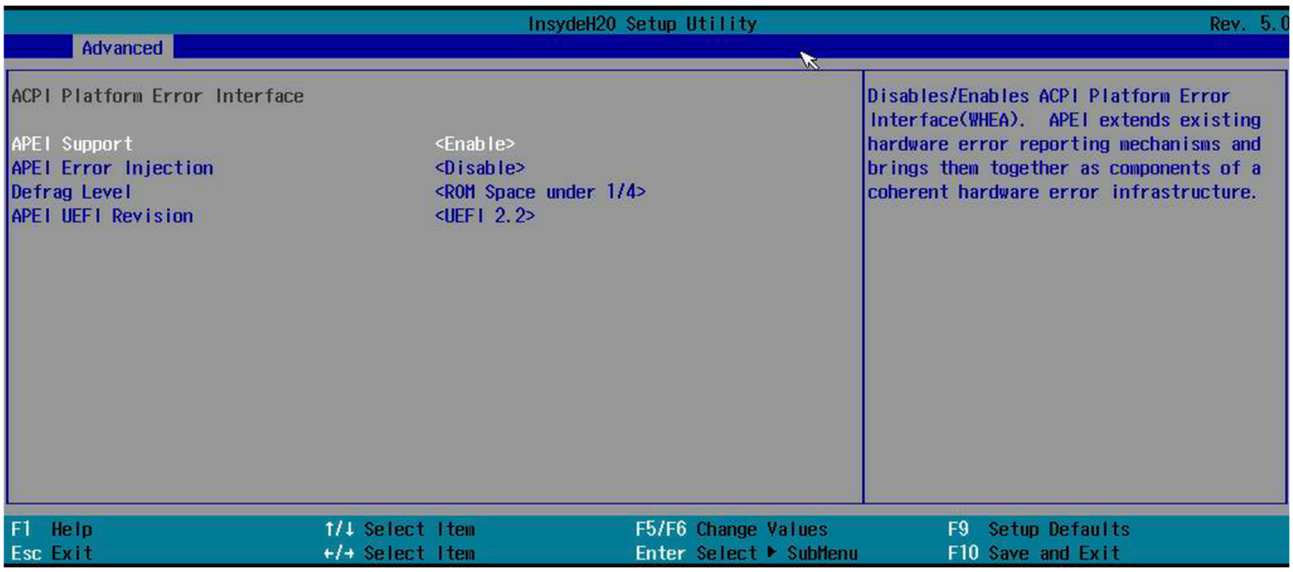
Рисунок 2.57. «SDR List»



2.2.9. «APEI Configuration»

ACPI Platform Error Interfaces (APEI) — рисунок 2.58. В этом разделе описываются интерфейсы ошибок платформы ACPI (APEI), которые позволяют компьютерной платформе передавать информацию об ошибках в OSPM. APEI расширяет существующие механизмы отчетности об аппаратных ошибках и объединяет их как компоненты целостной инфраструктуры аппаратных ошибок. APEI использует дополнительную информацию об аппаратных ошибках, доступную в современных аппаратных устройствах, и гораздо более тесно интегрируется с системной прошивкой. В результате APEI обеспечивает следующие преимущества: позволяет предоставлять более подробные данные об ошибках в стандартном формате записей об ошибках для определения основной причины аппаратных ошибок. Является расширяемым, так что по мере того, как поставщики оборудования добавляют к своим устройствам новые и более совершенные механизмы отчетности об аппаратных ошибках, APEI позволяет платформе и OSPM корректно приспосабливаться к новым механизмам. Это предоставляет информацию, помогающую системным разработчикам понять основные проблемы, связанные с аппаратными ошибками, взаимосвязь между прошивкой и OSPM, а также информацию об обработке ошибок и компонентах архитектуры APEI.

Рисунок 2.58. «APEI Configuration»



2.2.9.1. «APEI Support» — отключает/включает интерфейс ошибок платформы ACPI (WHEA).

APEI расширяет существующие механизмы сообщения об аппаратных ошибках и объединяет их как компоненты целостной инфраструктуры аппаратных ошибок.

2.2.9.2. «APEI Error Injection» — ввести ошибку, чтобы протестировать функцию APEI.

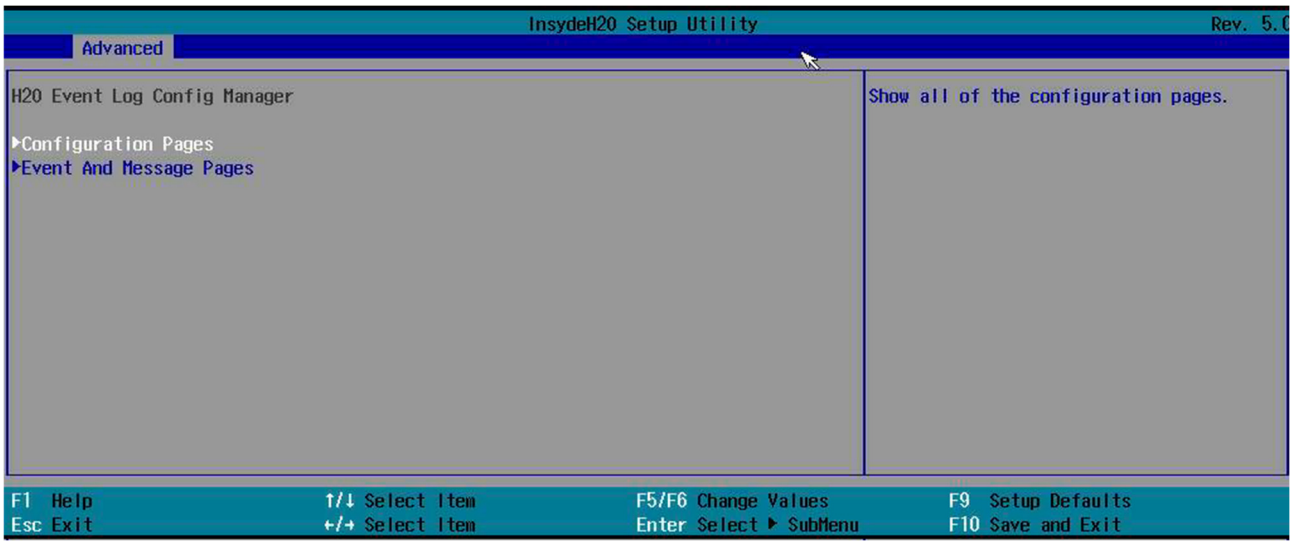
2.2.9.3. «Defrag Level» — уровень реагирования.

2.2.9.4. «APEI UEFI Revision» — версия UEFI.

2.2.10. «H20 Event log Config Manager»

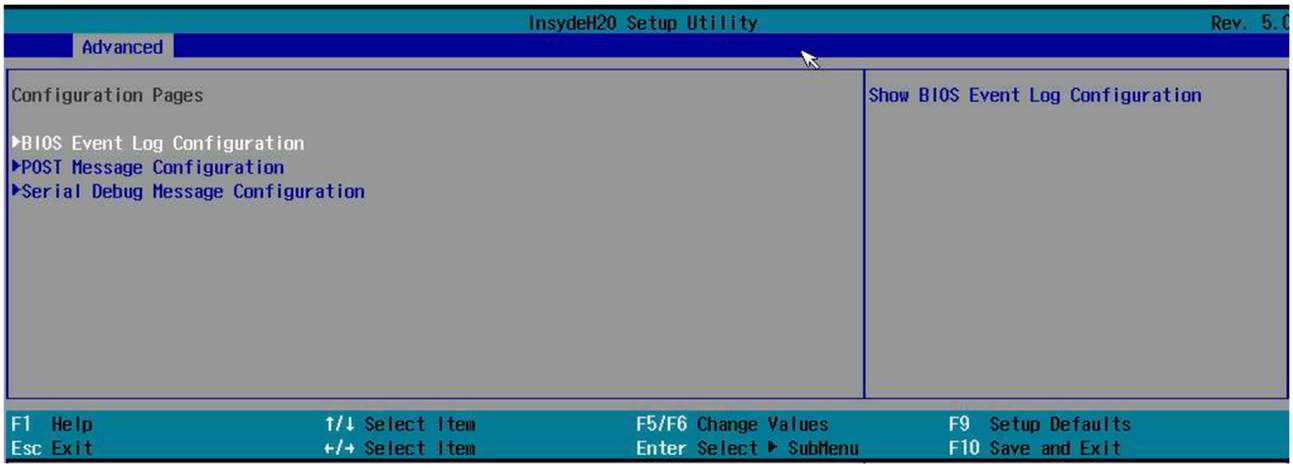
«H20 Event log Config Manager» представлен на рисунке 2.59.

Рисунок 2.59. «H20 Event log Config Manager»



2.2.10.1. «Configuration Pages» (рисунок 2.60).

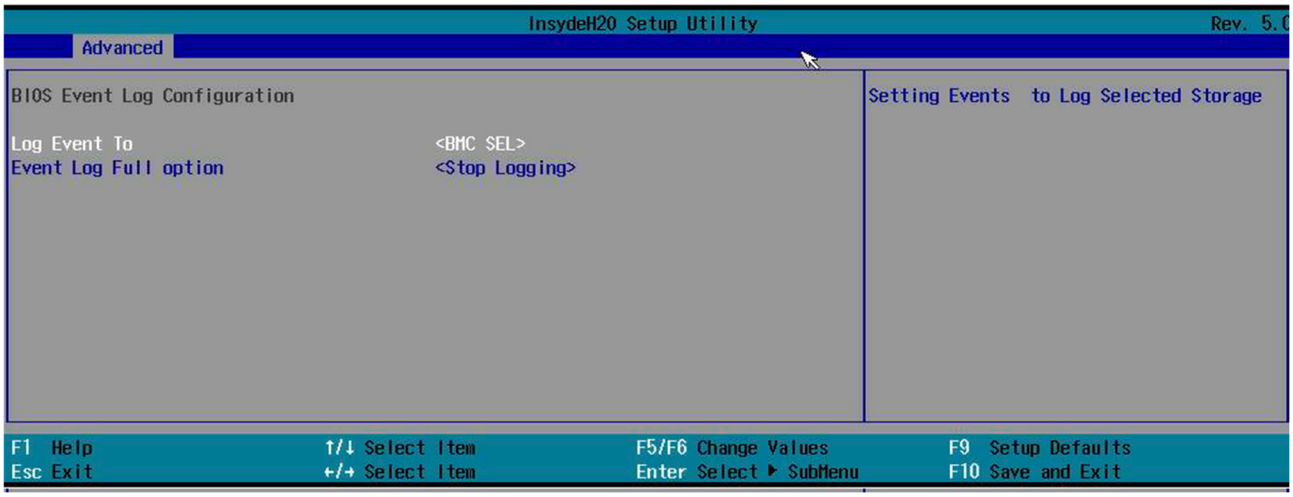
Рисунок 2.60. «Configuration Pages»



«BIOS Event Log Configuration» (рисунок 2.61) — настройка логирования сообщений BIOS:

- «Log Event To» — указание пути логирования;
- «Event Log Full option» — действия при заполнении лога.

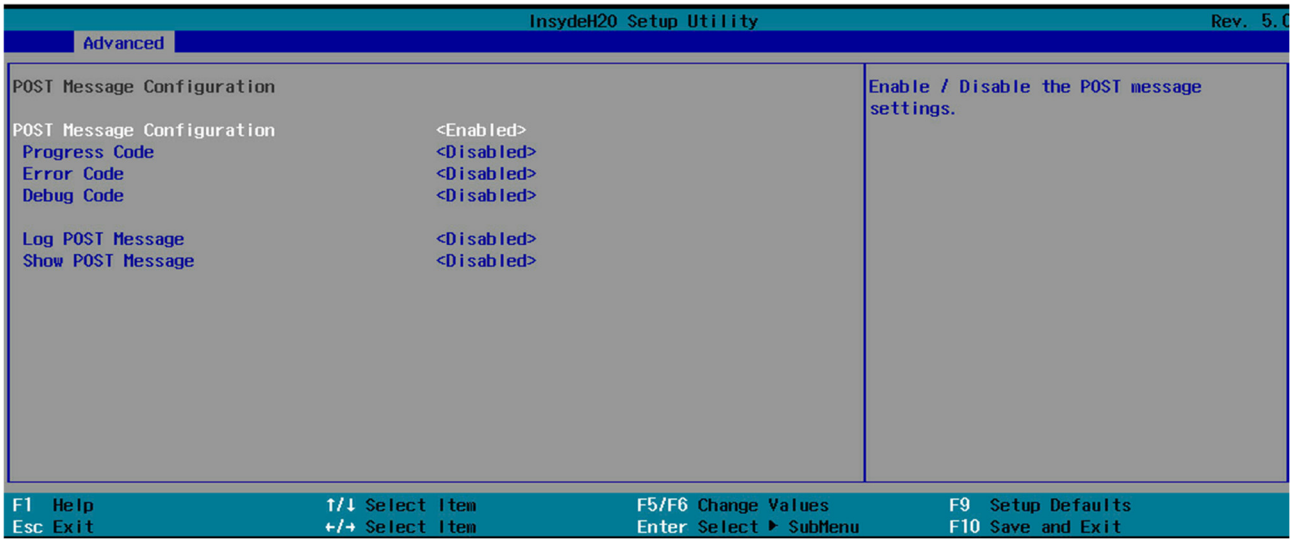
Рисунок 2.61. «BIOS Event Log Configuration»



«POST Message Configuration» (рисунок 2.62) — настройка сообщений POST:

- «POST Message Configuration» — разрешить настройку;
- «Progress Code» — разрешить показывать код процесса загрузки;
- «Error Code» — разрешить показывать код ошибки;
- «Debug Code» — разрешить показывать код отладки;
- «Log POST Message» — разрешить логировать сообщения POST;
- «Show POST Message» — показывать сообщения POST.

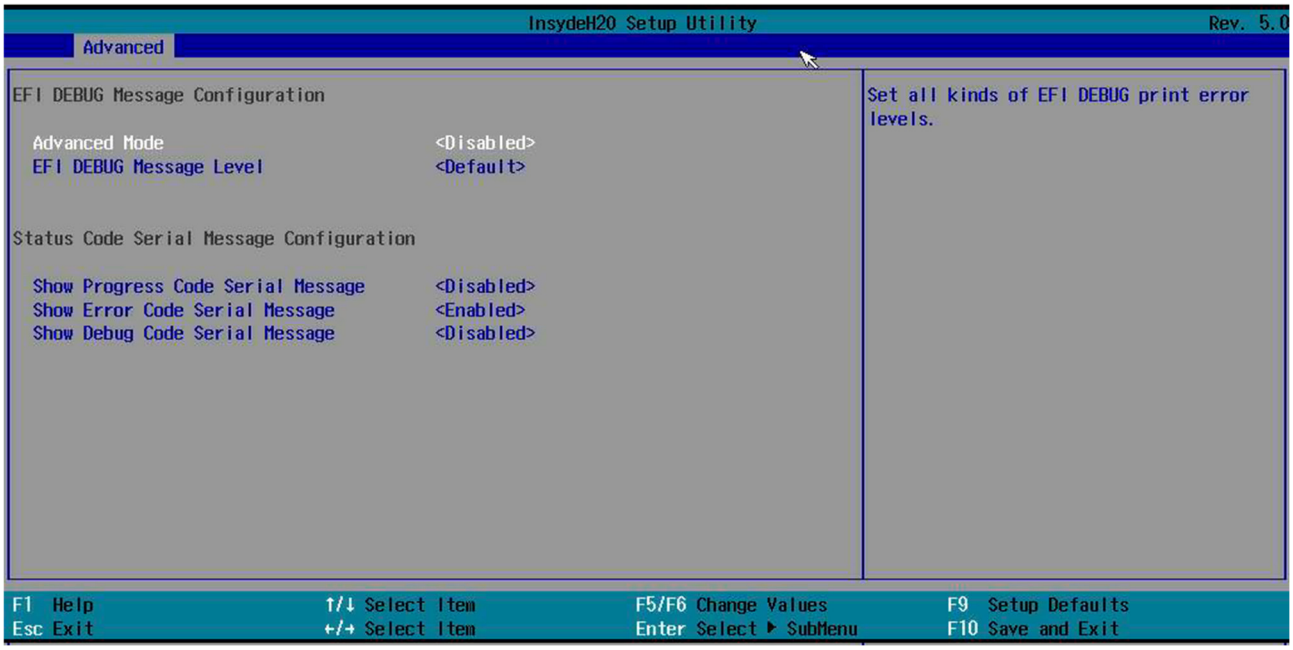
Рисунок 2.62. «POST Message Configuration»



«Serial Debug Message Configuration» (рисунок 2.63) — настройка сообщений отладки:

- «Advanced Mode» — ручная настройка уровня сообщений по каждому уровню;
- «EFI DEBUG Message Level» — доступно при отключенной функции ручной настройки, позволяет выставить вывод сообщений согласно уровню критичности;
- «Status Code Serial Message Configuration»;
- «Show Progress Code Serial Message» — разрешить вывод кода через консоль;
- «Show Error Code Serial Message» — разрешить вывод кода ошибки через консоль;
- «Show Debug Code Serial Message» — разрешить вывод кода отладки через консоль.

Рисунок 2.63. «Serial Debug Message Configuration»

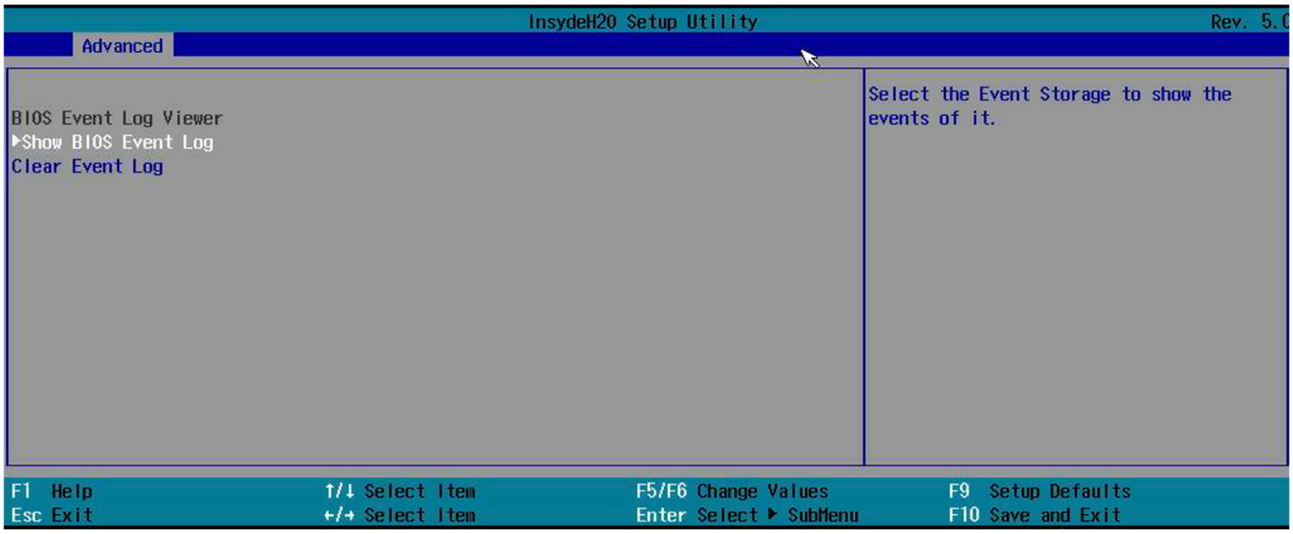


2.2.10.2. «Event and Message Pages» — страницы событий и сообщений.

«BIOS Log Viewer» (рисунок 2.64) — просмотр лога:

- «Show BIOS Event Log» — показать лог:
  - памяти;
  - BMC;
  - BIOS;
- «Clear Event Log» — очистить лог.

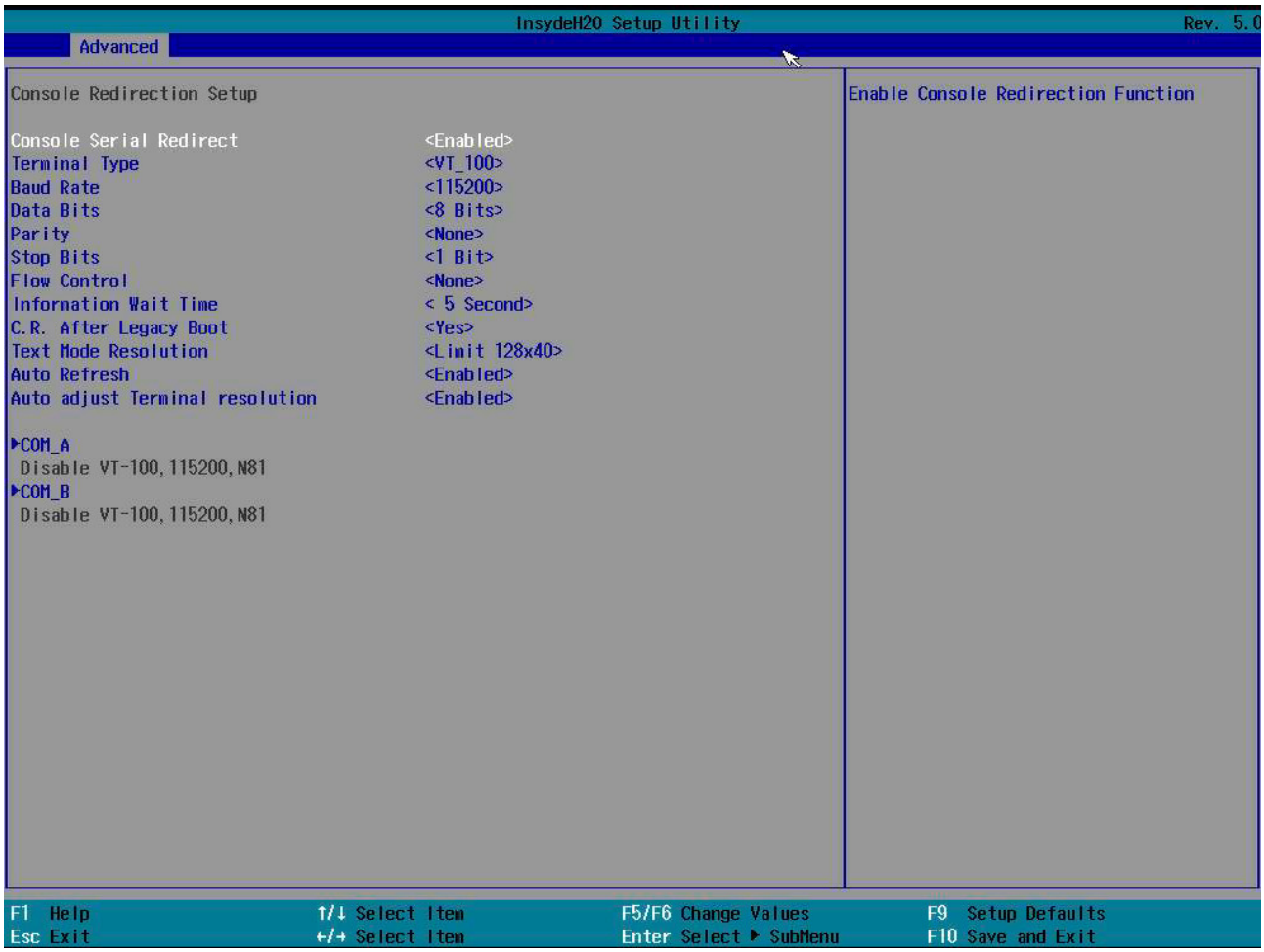
Рисунок 2.64. «BIOS Log Viewer»



2.2.11. «Console Redirection»

Перенаправление вывода консоли — рисунок 2.65.

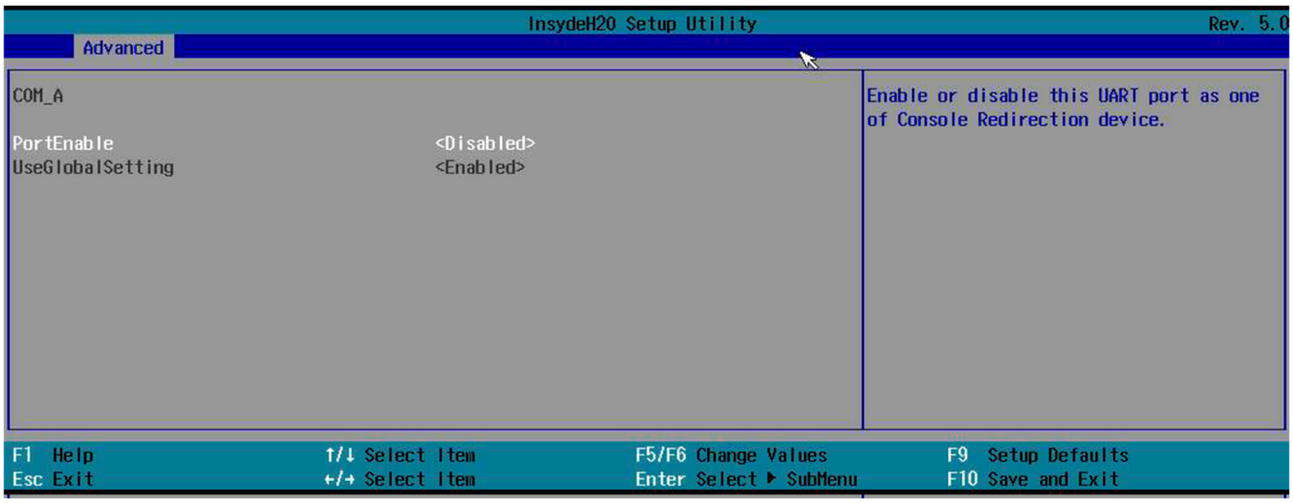
Рисунок 2.65. «Console Redirection»



В окне рисунка 2.65:

- «Console Serial Redirect» — разрешать вывод консоли в последовательный порт;
- «Terminal Type» — тип терминала;
- «Baud Rate» — скорость порта;
- «Data Bits» — количество бит данных;
- «Parity» — соответствие;
- «Stop Bits» — количество бит отказа;
- «Flow Control» — термин используется для описания метода, в котором последовательное устройство управляет объемом данных, передаваемых самому себе;
- «Information Wait Time» — время ожидания информации;
- «C. R. After Legacy Boot» — перенаправление вывода после загрузки в Legacy;
- «Text Mode Resolution» — разрешение вывода;
- «Auto Refresh» — автоматическое обновление вывода;
- «Auto adjust Terminal resolution» — автоматическая настройка яркости вывода;
- «COM_A» (рисунок 2.66) — настройки порта:
  - «PortEnable» — включить порт;
  - «UseGlobalSetting» — выбор между использованием общих настроек или индивидуальной настройкой порта;

Рисунок 2.66. «COM_A»



- «COM_B»:
  - «PortEnable»;
  - «UseGlobalSetting».

2.2.12. «H2oUve Configuration»

2.2.12.1. «H2OUVE Support».

2.3. «Security»

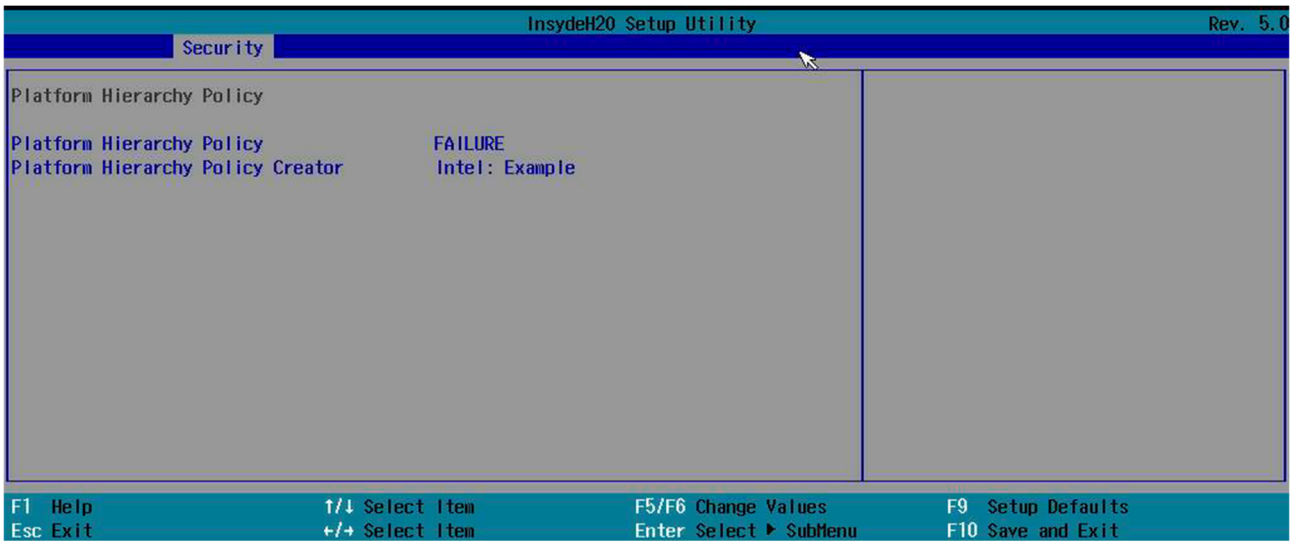
Вкладка «Security» — безопасность (рисунок 2.67).

Рисунок 2.67. Вкладка «Security»

В окне вкладки «Security»:

- «Current TPM Device» — текущее устройство TPM (Trusted Platform Module). Спецификация, описывающая криптопроцессор, в котором хранятся криптографические ключи для защиты информации, а также обобщенное наименование реализаций указанной спецификации, например в виде «чипа TPM» или «устройства безопасности TPM»;
- «TPM State» — состояние службы;
- «TPM Active PCR Hash Algorithm» — информация об алгоритмах;
- «TPM Hardware Supported Hash Algorithm» — информация об алгоритмах;
- «TrEE Protocol Version» — выбор версии протокола;
- «TPM Availability» — доступность TPM;
- «TPM Operation» — выберите нужную функцию;
- «Clear TPM» — очистить все связи;
- «Supervisor Password» — проверка, установлен ли пароль;
- «Set Supervisor Password» — установка пароля;
- «Platform Hierarchy Policy» — рисунок 2.68;
- «Platform Hierarchy Policy» — иерархическая политика;
- «Platform Hierarchy Policy Creator» — создание иерархической политики.

Рисунок 2.68. «Platform Hierarchy Policy»



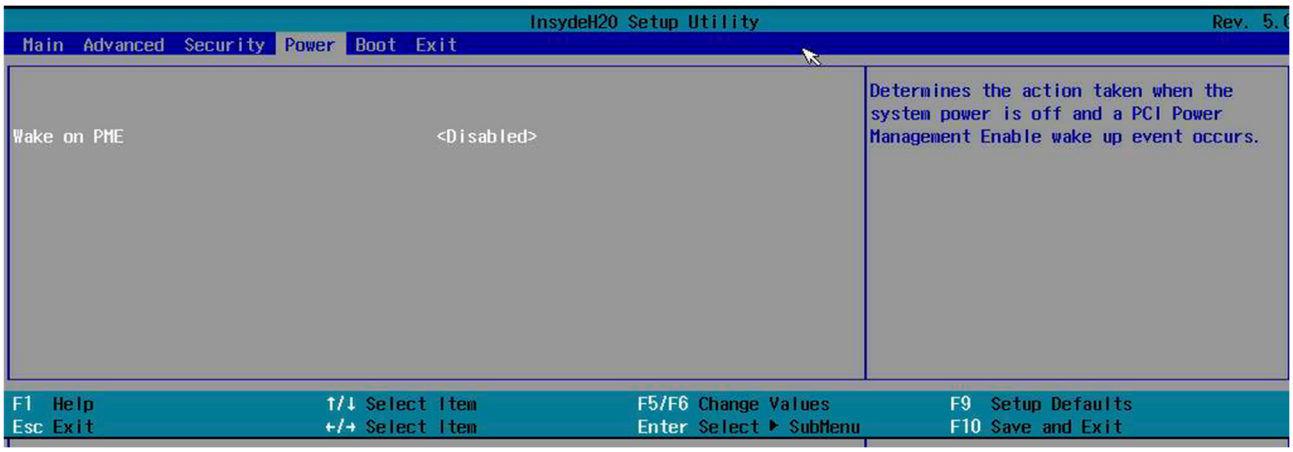
2.4. «Power»

Вкладка «Power» (рисунок 2.69) — настройка питания.

2.4.1. «Wake on PME»

Определяет действие, предпринимаемое при отключении питания системы и отключении питания PCI.

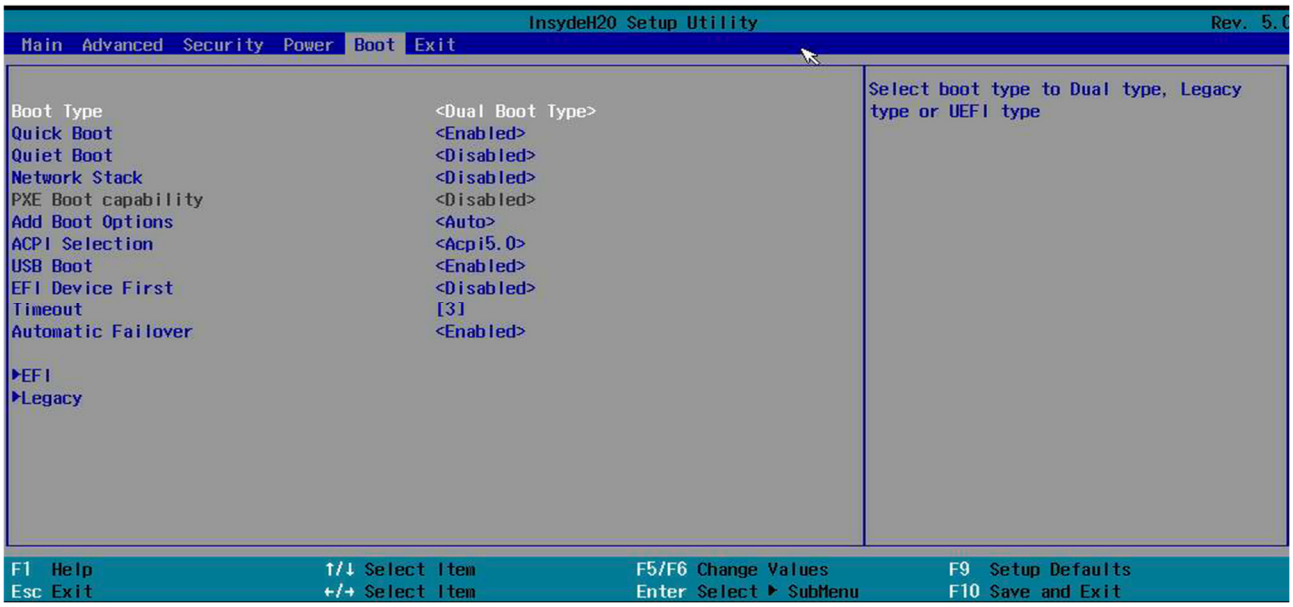
Рисунок 2.69. Вкладка «Power»



2.5. «Boot»

Вкладка «Boot» (рисунок 2.70) — настройка загрузки.

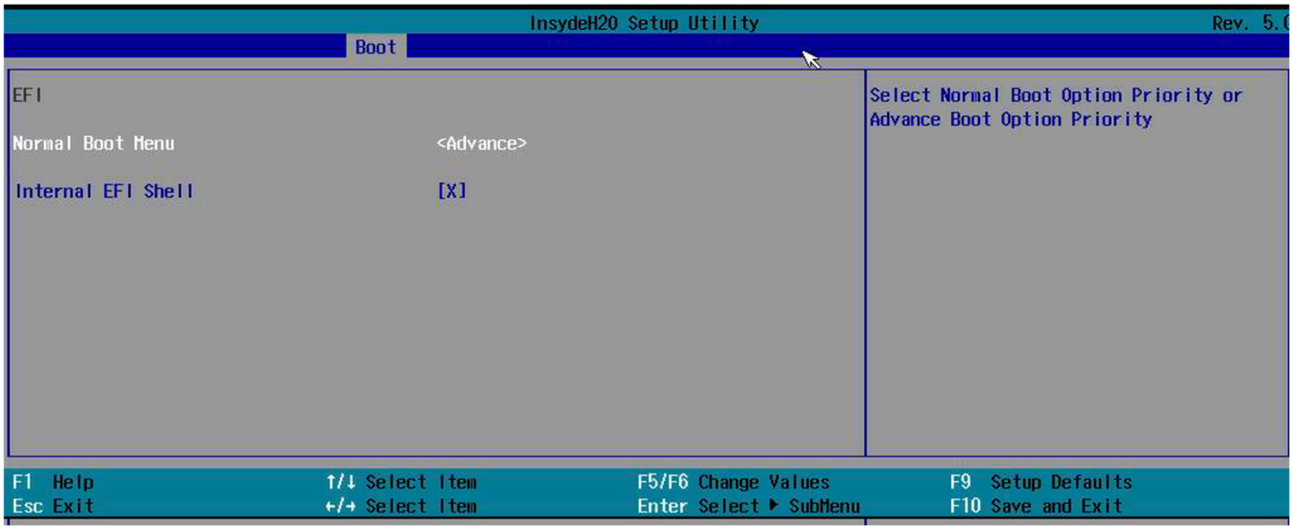
Рисунок 2.70. Вкладка «Boot»



В окне вкладки «Boot»:

- «Boot Type» — тип загрузки;
- «Quick Boot» — быстрая загрузка;
- «Quiet Boot» — настройка загрузки в текстовом режиме;
- «Network Stack» — включение этой опции означает, что пользователи могут загружать ОС через сетевую карту с удаленного компьютера или сервера (загрузка PXE);
- «PXE Boot capability» — включение этой опции означает, что пользователи могут загружать ОС через сетевую карту с удаленного компьютера или сервера (загрузка PXE);
- «Add Boot Options» — добавить опции загрузки;
- «ACPI Selection» — Advanced Configuration and Power Interface (ACPI) — это открытый стандарт, который ОС могут использовать для обнаружения и настройки аппаратных компонентов компьютера, управления питанием (например, перевода неиспользуемых аппаратных компонентов в спящий режим), автоматической настройки (например, Plug and Play и горячей замены) и мониторинга состояния;
- «USB Boot» — разрешает загрузку с USB-носителя;
- «EFI Device First» — настройка приоритетности запуска EFI-устройств;
- «Timeout» — время ожидания перед загрузкой согласно настройке по умолчанию;
- «Automatic Failover»;
- «EFI» (рисунок 2.71) — настройки загрузки EFI:
  - «Normal Boot Menu» — выбор между расширенным и обычным меню загрузки;
  - «Internal EFI Shell» — доступность оболочки;

Рисунок 2.71. «EFI»



- «Legacy» (рисунок 2.72) — настройка загрузки Legacy:
  - «Normal Boot Menu» — выбор между расширенным и обычным меню загрузки;
  - «Boot Type Order» (рисунок 2.73) — выбор устройства, с которого произойдет загрузка:

    1) «Floppy Drive»;
    2) «Hard Disk Drive»;
    3) «CD/DVD-ROM Drive»;
    4) «USB»;
    5) «Others»;

Рисунок 2.72. «Legacy»

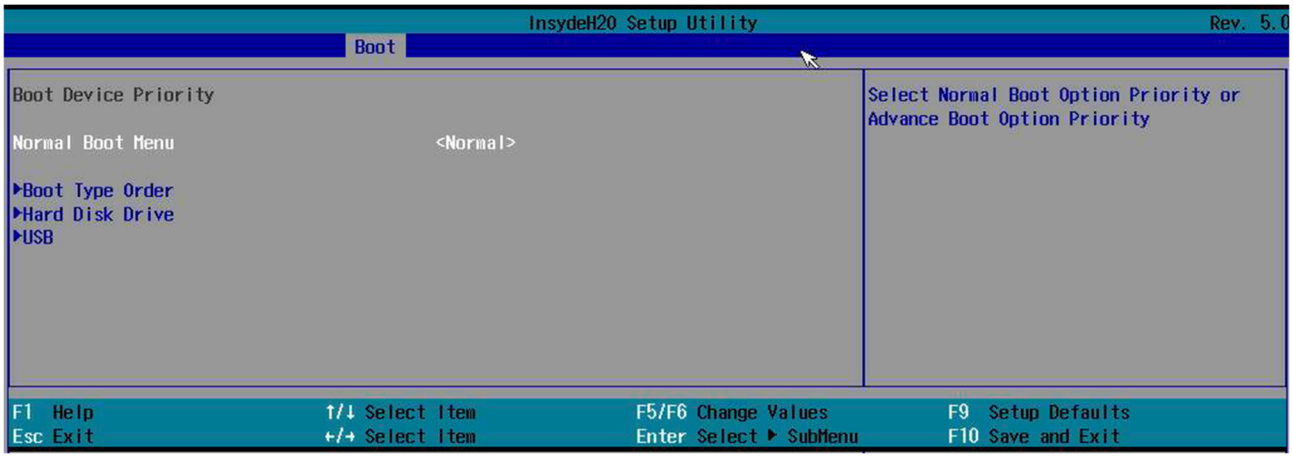
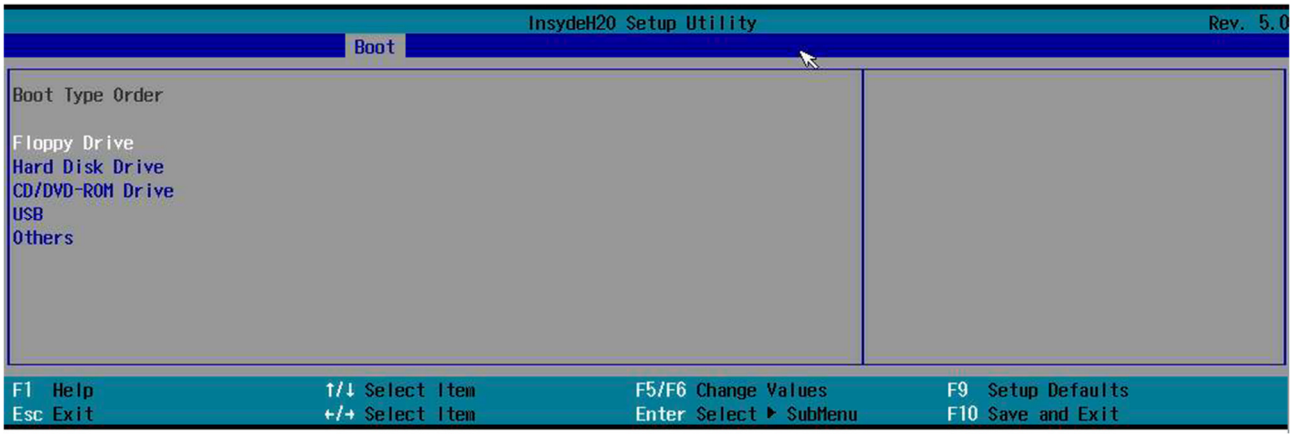
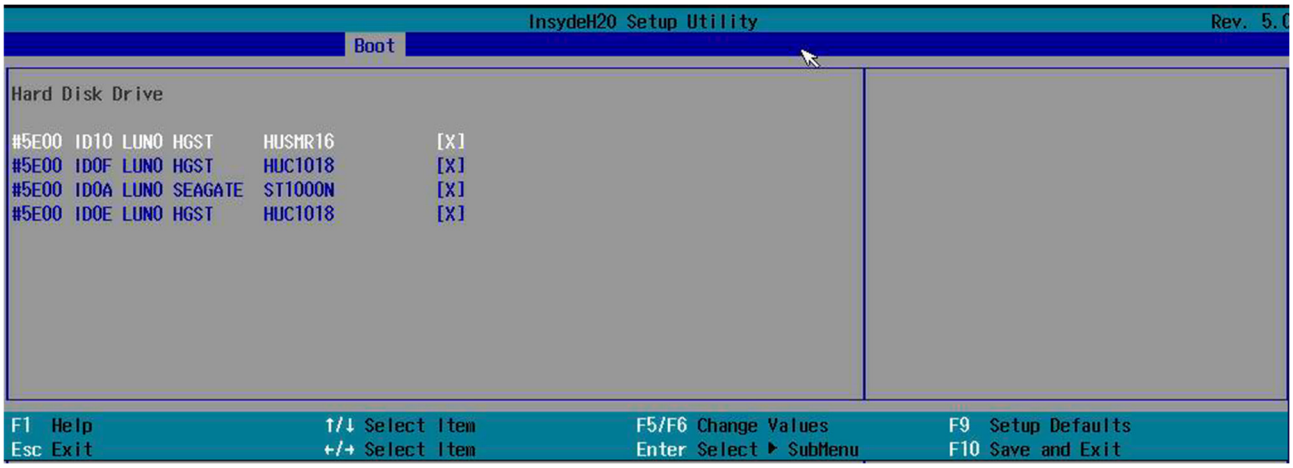


Рисунок 2.73. «Boot Type Order»



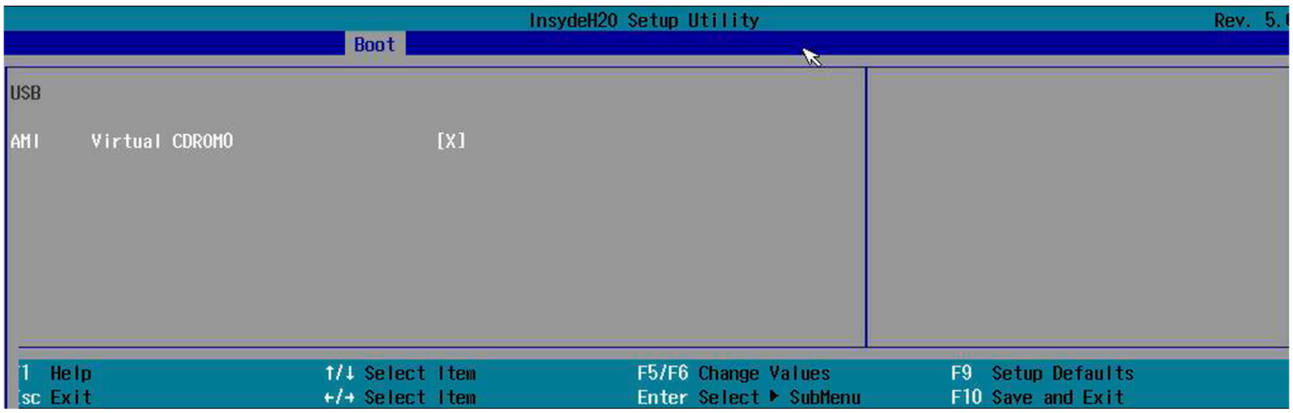
- «Hard Disk Drive» (рисунок 2.74) — вывести список дисковых устройств;

Рисунок 2.74. «Hard Disk Drive»



- «USB» (рисунок 2.75) — вывести список USB-устройств.

Рисунок 2.75. «USB»

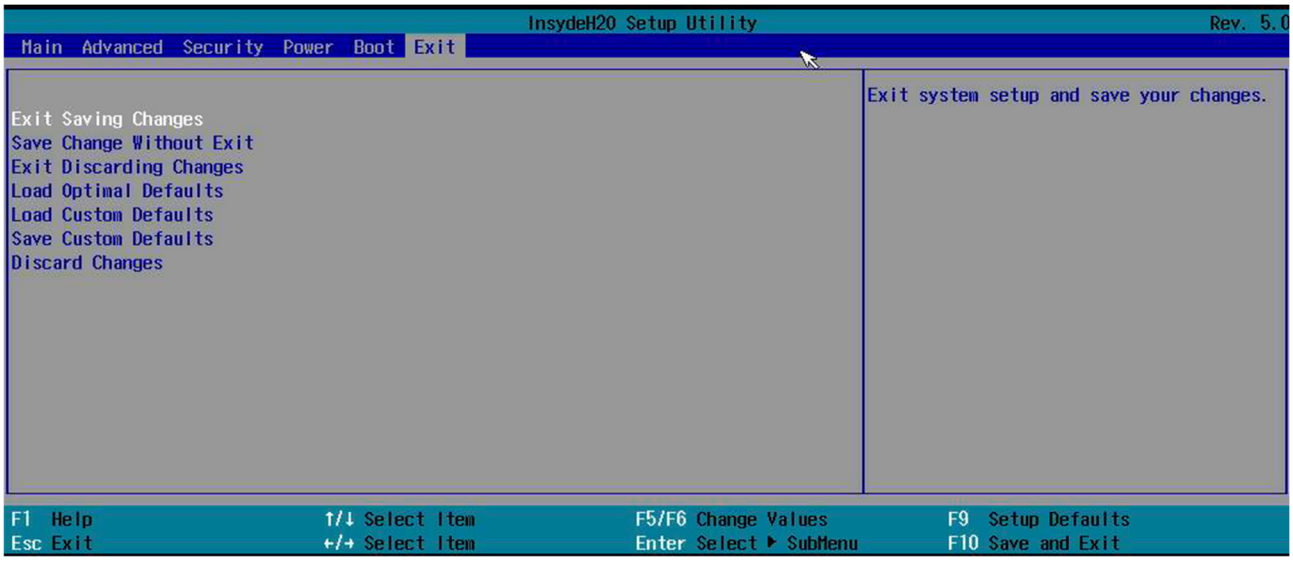


2.6. «Exit»

Вкладка «Exit» (рисунок 2.76) — выход:

- «Exit Saving Changes» — выйти и сохранить;
- «Save Change Without Exit» — сохранить изменения, не выходить;
- «Exit Discarding Changes» — выйти без сохранения;
- «Load Optimal Defaults» — загрузить оптимальные настройки по умолчанию;
- «Load Custom Defaults» — загрузить пользовательские настройки;
- «Save Custom Defaults» — сохранить пользовательские настройки;
- «Discard Changes» — отменить изменения.

Рисунок 2.76. Вкладка «Exit»



Перечень принятых сокращений

Сокращенное наименование	Полное наименование
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
ЦП	Центральный процессор
ACPI	англ. Advanced Configuration and Power Interface — усовершенствованный интерфейс управления конфигурацией и питанием
AHCI	англ. Advanced Host Controller Interface — механизм, используемый для подключения накопителей информации стандарта Serial ATA, позволяющий пользоваться расширенными функциями, такими как встроенная очередность команд и горячая замена
APEI	англ. ACPI Platform Error Interfaces (APEI) — интерфейсы ошибок платформы ACPI
API	англ. Application Programming Interface — специальный протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого
APIC	англ. Advanced Programmable Interrupt Controller — улучшенный программируемый контроллер прерываний
BCLK	англ. Base Clock — тактовая частота работы процессора
BIOS	англ. Basic Input/Output System — базовая система ввода-вывода
BMC	англ. Baseboard Management Controller — контроллер управления материнской платой
CAS	англ. Column Access Strobe — сигнал выборки столбца матрицы данных
CPU	англ. Central Processing Unit — центральный процессор
CSR	англ. Control/Status Register — регистр управления и состояния
DDR	англ. Double Data Rate — синхронная динамическая память с произвольным доступом и удвоенной скоростью передачи данных
DHCP	англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла
DIMM	англ. Dual In-line Memory Module — формфактор модулей памяти DRAM
DMA	англ. Direct Memory Access — прямой доступ к памяти
DMI	англ. Direct Media Interface — прямой интерфейс мультимедиа
DSP	англ. Digital Signal Processor — цифровой процессор обработки сигналов
ECC	англ. Error-correcting Code memory — память с коррекцией ошибок
FDI	англ. Flexible Display Interface — гибкий интерфейс дисплея
HECI	англ. Host Embedded Controller Interface — технология, используемая для технологии активного управления в наборах микросхем Intel, поддерживающих микропроцессоры Core 2 Duo
IBM	англ. International Business Machines — один из крупнейших в мире производителей и поставщиков аппаратного и программного обеспечения, а также ИТ-сервисов и консалтинговых услуг
IMC	англ. Integrated Memory Controller — интегрированный контроллер памяти

Сокращенное наименование	Полное наименование
IP	англ. Internet Protocol — интернет-протокол
IPMI	англ. Intelligent Platform Management Interface — интеллектуальный интерфейс управления платформой
IPv4	англ. Internet Protocol version 4 — четвертая версия интернет-протокола IP
IPv6	англ. Internet Protocol version 6 — новая версия интернет-протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия IPv4
ISA	англ. Industry Standard Architecture — 8- или 16-разрядная шина ввода-вывода IBM PC-совместимых компьютеров
LAN	англ. Local area network — локальная вычислительная сеть
MMIO	англ. Memory-mapped Input/Output — ввод-вывод с отображением памяти
PCH	англ. Platform Controller Hub — элемент системной логики производства Intel, который управляет работой основной массы структур материнской платы
PCIe	англ. Peripheral Component Interconnect Express — компьютерная шина, в которой применяются высокопроизводительный протокол последовательной передачи данных и принцип соединения «точка-точка»
PDF	англ. Portable Document Format — межплатформенный открытый формат электронных документов
PLL	англ. Phase-Locked Loop — специальный генератор со схемой подстройки частоты
PMEM	англ. Persistent Memory — быстрая память, обладающая возможностью хранить данные после отключения питания компьютера
POST	англ. Power-On Self-Test — самотестирование при включении
QoS	англ. Quality of Service — технология предоставления приоритетов в обслуживании
QPI	англ. QuickPath Interconnect — последовательная кэш-когерентная шина типа «точка-точка»
RAM	англ. Random Access Memory — запоминающее устройство с произвольным доступом»
RAS	англ. Row Address Strobe — строб адреса строки
SATA	англ. Serial ATA — последовательный интерфейс обмена данными с носителями информации
SDRAM	англ. Synchronous Dynamic Random Access Memory — синхронная динамическая память с произвольным доступом
SMBus	англ. System Management Bus — последовательный протокол обмена данными для устройств питания
SPD	англ. Serial Presence Detect — чип-микросхема
SPMI	англ. System Power Management Interface — интерфейс управления питанием системы
TDP	англ. Thermal Design Power — расчетная тепловая мощность
TPM	англ. Trusted Platform Module — доверенный платформенный модуль
UEFI	англ. Unified Extensible Firmware Interface — унифицированный расширяемый микропрограммный интерфейс
UPI	англ. Ultra-Path Interconnect — интерфейс двухточечного межчипового соединения
USB	англ. Universal Serial Bus — последовательный интерфейс для подключения периферийных устройств к вычислительной технике

Сокращенное наименование	Полное наименование
VGA	англ. Video Graphics Array — протокол отображения видео
xHCI	англ. Extensible Host Controller Interface — спецификация компьютерного интерфейса, которая определяет описание на уровне регистров хост-контроллера для универсальной последовательной шины