BIOS Manual

SR124-2A/SR224-2A/
SR121-2A/SR221-2A

Revision : 1.4
Release Date : 2025/10/02

Version Control

This is a history of the documents highlighting significant changes per revision number and date.

Revision	Description	Date
0.1	Initial release	2024/05/28
1.0	1. Added Genoa support of platform overview. 2. Modify BIOS ROM size to 32MB. 3. Added product support list of front page.	2024/11/11
1.1	1. Modify POST event of section 2.10 2. Turin support DIMM 6400 MT/s of section 1.3 3. Modify SKU number and Family description on SMBIOS Type 1.	2024/11/25
1.2	Modify lack section in Table of contents list	2024/11/28
1.3	Add description and Rear HDD slot of section 4	2025/01/03
1.4	Update model name	2025/10/02

Overview

This document provides the information for Basic Input-Output System (BIOS) and software features. It describes the architecture and feature set for all function in the system.

Table of contents

1. Architecture

These BIOS is implemented as firmware that resides in Flash Memory – Electrically Erasable Programmable Read Only Memory (EEPROM) – on the Server Board. The BIOS provides hardware-specific initialization algorithms and standard compatible basic input/output service. The Flash Memory also contains firmware for certain embedded devices. These images are supplied by the device manufacturers and are not specified in this document.

This BIOS implementation is based on the Extensible Firmware Interface (EFI), according to the Intel® Platform Innovation Framework for EFI architecture, as embodied in the industry standards for Unified Extensible Firmware Interface (UEFI).

The implementation is compliant with EFI architecture specifications, as further specified in the Unified Extensible Firmware Interface Reference Specification, Version.

In the UEFI BIOS design, there are three primary components: the BIOS itself, the Human Interface Infrastructure (HII) that supports communication between the BIOS and external programs, and the Shell which provides a limited OS-type command-line interface. This BIOS system implementation complies with HII, and includes a Shell.

The UEFI BIOS structure is quite different from the traditional “Legacy BIOS”, primarily to offer more generalization of the interface between system hardware and Operating System while still providing the same level of functionality. This is achieved by compartmentalization and layering of the BIOS components.
It is also important to understand that the UEFI BIOS structure is designed for implementation in a High Level Language, the C language, rather than the low-level Assembly language in which Legacy BIOS was typically implemented. This makes the programming involved in implementation and maintenance far easier to write, read, understands, and debug.

1.1. BIOS POST Flow

These BIOS is implemented according to the Unified Extensible Firmware Interface (UEFI) Specification Version 2.4.
There is a formalized path that is followed through the course of Power On Self-Test (POST). The BIOS is highly modular and “layered”, where each layer represents a different phase of POST during which different conditions are in effect.

- Initially, at reset, the system is in a purely hardware phase. It begins execution through the hardware reset vector, and then performs preliminary tasks such as selecting the primary Bootstrap Processor (BSP).
- When the minimal hardware initialization is complete, the system moves into a phase called “Security”, or SEC.
- Next is the Pre-EFI Initialization (PEI) phase, in which additional processor and chipset initialization are performed.
- As the initialization proceeds, the Driver Execution Environment (DXE) phase begins.
- From the DXE phase, there is a Boot Device Selection (BDS) phase to prepare for booting the system.
- The boot operation itself begins with a Transient System Load (TSL) to bring in the OS loader.
- Finally the OS takes over for runtime.

1.2. Specifications

- UEFI Specification Revision 2.8
- PI 1.7 Support
- ACPI Specification Revision 6.2
- PCI Express Base Specification Revision 5.0.
- SMBIOS Table Specification Version 3.5.0.
- SATA (Serial ATA) Specification Revision 2.0.
- SmBus Specification Version 2.0
- MultiProcessor Specification Version 1.4.
- IPMI Specification Version 2.0, Revision 1.1
- PCI Firmware Specification, Version 3.0.
- NVMe spec. Version V1.1.
- TCG TPM Specification Version 1.2/2.0
- TCG Storage Architecture Core Specification, Version 2.01
- TCG ACPI Specification 1.2

1.3. Platform overview

Component		Description
Turin	Processor	Base on Zen5/Zen5c CPU core with AMD EPYC™ Turin processor family, SP5 Socket Compatible. 192 Zen5c cores per socket. 128 Zen5 cores per socket.
	Memory	DIMM Type: DDR5 RDIMM/3DSDIMM, Memory speed up to *6400 MT/s (1DPC) DIMM Channel: 12 channels per socket DIMM Count: 12 DIMMs per socket
Genoa	Processor	Base on Zen4/Zen4c CPU core with AMD EPYC™ Genoa and Bergamo processor family, SP5 Socket Compatible. 128 Zen4c cores per socket. 96 Zen4 cores per socket.
	Memory	DIMM Type: DDR5 RDIMM/3DSDIMM, Memory speed up to 4800 MT/s (1DPC) DIMM Channel: 12 channels per socket DIMM Count: 12 DIMMs per socket
PCIe		Up to Gen5
BMC		AST2600
BIOS Flash		32-MB SPI flash chip
TPM		TPM2.0

*AGESA PI 1.0.0.3 starts to support DIMM-6400 MT/s.

1.4. Memory Population

Each SP5 socket has 12 memory channels labeled A–L. Depending on platform design, each memory channel supports up to 2 DIMMs per channel (2DPC). In this project design is support 1 DIMM per channel (1DPC.)

Memory channel interleaving mode depends on memory channels populated, symmetry of channel capacity, and NUMA1 nodes per socket (NPS) selected by firmware boot options.

Figure 1 shows the best-performing configuration, which is populating 12 channels per socket with symmetric memory capacity. And memory channels are recommended to be populated in the order shown in Figure 2.

Figure 1. Socket SP5 Full Memory Population

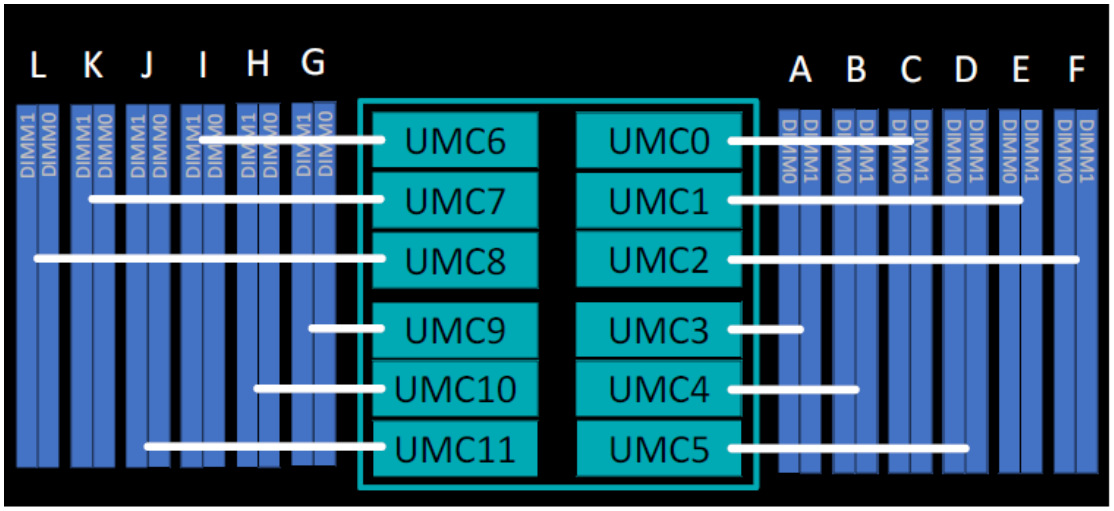


Figure 2. Memory Channel Population Order

Number of Memory Channels Populated	Recommended Memory Channels (UMC to Memory Channel Mapping)													Nodes per Socket (NPS) Supported[2]
12	Memory Channel	A	C	B	E	D	F	G	I	H	K	J	L	NPS4, NPS2, NPS1
	UMC Instance	3	0	4	1	5	2	9	6	10	7	11	8	
10	Memory Channel	A	C	B	E	D		G	I	H	K	J		NPS2, NPS1
	UMC Instance	3	0	4	1	5		9	6	10	7	11		
8	Memory Channel	A	C	B	E			G	I	H	K			NPS4, NPS2, NPS1
	UMC Instance	3	0	4	1			9	6	10	7			
6	Memory Channel	A	C	B				G	I	H				NPS2, NPS1
	UMC Instance	3	0	4				9	6	10				
4	Memory Channel	A	C					G	I					NPS4, NPS2, NPS1
	UMC Instance	3	0					9	6					
2	Memory Channel	A						G						NPS2, NPS1
	UMC Instance	3						9						
1	Memory Channel	A												NPS1
	UMC Instance	3												

2.Server feature

2.1. Updateable Firmware

Updateable Firmware

• System Firmware ROM, updateable through the BMC.

• Method is same as 2.3 step.

2.2. UEFI System Firmware

• Compliant with ACPI specifications version 6.2

• Compliant with System Management BIOS (SMBIOS) specification, version 3.5.0.

• Compliant with Prestart Execution Environment (PXE), version 2.0.

• ACPI Power states S0, S5, C0, C1, CC1, CC6.

2.3. Recovery BIOS function

Recovery BIOS Step:

Step1. Login system BMC web

Step2. Press BIOS Firmware update

Step3. Select .CPM fil in BIOS release package

Step4. Press Start Firmware update

Step5. Press Proceed and Wait progress bar complete

Step6. After progress bar done, system will auto restart.

Note : Sign key encrypted is different by project, so different project .cpm file can't update successful in same test machine, so please use correct .cpm file.

2.4. Clear Password Function

The BIOS support the clear password function when forgot password and cannot boot to setup menu or operating system.

Method is below:

Step1. Send IPMI command to set flag of clear password:
Ex: ipmitool.exe raw 0x3C 0x76 0x01

Step2. Reboot server and boot to POST complete.

Step3. Password will be cleared.

2.5. POST Hot Keys

- POST shall provide support for 'hot keys' that allow the user to enter Setup, bypass Enhanced POST switch to Quick POST, perform a boot from the network, shown POST diagnostic information and so on. In addition to these key strokes, a method must be surfaced that allows the keys to be pressed, It needs to keep about 2s to make sure the user can have response and it also needs a related indicate string for the hot key pressed. Such as when pressing F1, the indicate string is 'Entering setup …'

Function	Function 1
Enter setup	F1
Boot menu	F12

- **In BIOS Setup Hot KEY define:**

Hotkey	Function
←→↑↓	Move
Enter	Select and enter subsystem
+/-	Add and reduce value
ESC	Exit
F1	General Help
F2	Previous Value
F3	Optimized Defaults
F4	Save & Exit Setup
<K>	Scroll help area upwards
<M>	Scroll help area downwards

- **Note:** BIOS setup time setting only can be changed by +/- and number key.

2.6. System Management BIOS (SMBIOS)

The BIOS provides support for the System Management BIOS. This specification is also intended to provide enough information for developers of management instrumentation to develop generic routines for translating from SMBIOS. The BIOS provides this interface via data structures through which the system attributes are reported. Using SMBIOS, a system administrator can obtain the types, capabilities, operational status, installation date and other information about the server components.

As defined in the SMBIOS specification, the approved method of accessing the SMBIOS information is through the table method. The table convention allows the SMBIOS structures to be accessed under 32-bit protected-mode operating systems.

Relationship with FRU

SMBIOS below fields should synch with FRU. The contents mainly relate are as below:

Type1“Product Name”

Type1“Version”

Type1“SerialNumber”

Type1“UUID”

Type2“Version”

Type2“SerialNumber”

Type2“Asset Tag”

Type3“Version”

Type3“SerialNumber”

Type3“Asset Tag”

SMBIOS support TYPE

- BIOS Information(Type0)
- System Information(Type1)
- Baseboard(orModule)Information(Type2)
- System EnclosureorChassis (Type3)
- Processor Information(Type4)
- CacheInformation(Type7)
- PortConnectorInformation(Type8)
- SystemSlots(Type9)
- Physical MemoryArray(Type16)
- MemoryDevice(Type17)
- MemoryArrayMappedAddress (Type19)
- OnboardDevicesExtendedInformation(Type41)
- End–Of-Table(Type127)

2.6.1 Type 0 Structure – BIOS information

Offset	Name	Length	Value	Description
00h	Type	Byte	0	BIOS information (type 0) indicator.
01h	Length	Byte	1Ah	Both extension bytes are supported.
02h	Handle	Word	Varies	The number of this structure in the table.
04h	Vendor	Byte	String	Number of Null terminated string. "American Megatrends International, LLC. ".
05h	BIOS Version	Byte	String	Number of Null terminated string. Contains full BIOS ID string. For system, this format should be “xx.xx.xx”.
06h	BIOS Starting Address Segment	Word	Varies	Segment location of BIOS starting address.
08h	BIOS Release Date	Byte	String	Number of Null terminated string. Date is in mm/dd/yyyy format.
09h	BIOS ROM Size	Byte	Varies (n)	Size (n) where 64K*(n+1) is the size of the BIOS flash part. 16 MB (FFh) is the maximum reported value in this field. If physical BIOS ROM size is greater than 16MB, any reported value is no meaningfulness in this field. That is a SMBIOS spec limitation.
0Ah	BIOS Characteristics	QWord	Bit Field	See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.1.1 for enumeration of values.
12h	BIOS Characteristics Extension Bytes	Word	Bit Field	See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.1.2 for enumeration of values. Byte 1 and Byte 2 are supported.
14h	System BIOS	Byte	Varies	Identifies the

	Major Release			major release of the System BIOS core version; for example, the value will be 0Ah for revision 10.22 and 02h for revision 2.1. This field and/or the System BIOS Minor Release field will be updated each time a System BIOS update for a given system is released. If the system does not support the use of this field, the value will be 0FFh for both this field and the System BIOS Minor Release field.
15h	System BIOS Minor Release	Byte	Varies	Identifies the minor release of the System BIOS core version; for example, the value will be 16h for revision 10.22 and 01h for revision 2.1.
016h	Embedded Controller Firmware Major Release	Byte	Varies	Identifies the major release of the embedded controller firmware; for example, the value will be 0Ah for revision 10.22 and 02h for revision 2.1. This field and/or the Embedded Controller Firmware Minor Release field will be updated each time an embedded controller firmware update for a given system is released. If the system does not have field upgradeable embedded controller firmware, the value will be 0FFh.
17h	Embedded Controller Firmware Minor Release	Byte	Varies	Identifies the minor release of the embedded controller firmware; for example, the value will be 16h for revision 10.22 and 01h for revision

				2.1. If the system does not have field upgradeable embedded controller firmware, the value will be 0FFh.

2.6.2 Type 1 Structure – System Information

Offset	Name	Length	Value	Description
00h	Type	Byte	1	System information indicator.
01h	Length	Byte	1Bh	Number of bytes in this type structure.
02h	Handle	Word	Varies	The number of this structure in the table.
04h	Manufacturer	Byte	String “COMPAL”	Number of Null terminated string. This comes from FRU field “Product Manufacturer”.
05h	Product Name	Byte	String “This Products name”	Number of Null terminated string. This comes from the concatenation of the FRU fields “Product Name”.
06h	Version	Byte	String	Number of Null terminated string. This comes from FRU field “Product Version”.
07h	Serial Number	Byte	String	Number of Null terminated string. This comes from FRU field “Product Serial Number”.
08h	UUID	16 bytes	Varies	This is from the value stored in non-volatile RAM (either BIOS Flash or BMC).
18h	Wakeup Type Info	Byte	Enum	See the System Management BIOS Reference Specification, Version 3.2.0 Section 7.2.2 for meaning.
19h	SKU Number	Byte	String	Number of Null terminated string. This text string comes from FRU field “Product SKU ID”.
1Ah	Family	Byte	String	Number of Null terminated string. This text string default is COMPAL.

2.6.3 Type 2 Structure – Base Board Information

The SMBIOS Type 2 structure is populated by obtaining information from the product area of the BMC FRU. The information obtained from this area can be customized.

2.6.4 Type 3 Structure – System Enclosure or Chassis

The SMBIOS Type 3 structure is populated by obtaining information from the product area of the BMC FRU. The information obtained from this area can be customized.

2.6.5 Type 4 Structure – Processor Information

Offset	Name	Length	Value	Description
00h	Type	Byte	4	Processor information indicator.
01h	Length	Byte	30h	Number of bytes in this type structure.
02h	Handle	Word	Varies	The number of this structure in the table.
04h	Socket Designation	Byte	String	Number of Null terminated string. Contains the reference designator on the silkscreen of the processor socket.
05h	Processor Type	Byte	03h	03h = Central processor.
06h	Processor Family	Byte	6Bh	6Bh = AMD Zen processor Family.
07h	Processor Manufacturer	Byte	String	Number of Null terminated string. String contains "Advanced Micro Devices, Inc.".
08h	Processor ID	QWord	Varies	Contains the results of the CPUID instruction with EAX = 1 as follows: Offset 08h-0Bh: EAX Offset 0Ch-0Fh: EDX
10h	Processor Version	Byte	String	Number of Null terminated string that describes the processor. This string is returned from the processor.
11h	Voltage	Byte	Varies	Bit 7 – 1 Bits [6:0] Current processor voltage * 10 - 1.8V = 92h
12h	External Clock	Byte	Varies	External Clock Frequency, in

				MHz If the value is unknown, the field is set to 0.
14h	Max Speed	Word	Varies	Maximum internal processor speed in MHz.
16h	Current Speed	Word	Varies	Current internal processor speed in MHz.
18h	Status	Word	Varies	Bit 7 0 = Reserved Bit 6 0 = Socket unpopulated 1 = Socket populated Bits 5:3 0 = Reserved Bits 2:0 0h = Unknown 1h = CPU enabled 2h = CPU disabled by user through BIOS setup 3h = CPU disabled by BIOS (POST Error) 4h = CPU idle, waiting to be enabled 5h, 6h = Reserved 7h = Other
19h	Processor Upgrade	Word	Varies	Describes the byte values for the Processor Information — Processor Upgrade field. See the System Management BIOS Reference Specification, Version 3.7.0, Section 7.5.5 for more information.
1Ah	L1 Cache Handle	Word	Varies	Handle of the cache information structure for L1 cache for this processor. Set to 0FFFFh if the cache information structure is not supported.
1Ch	L2 Cache Handle	Word	Varies	Handle of the cache information structure for L2 cache for this processor. Set to 0FFFFh if the cache information structure is not supported.
1Eh	L3 Cache Handle	Word	Varies	Handle of the cache information structure for L3 cache for this processor. Set to

				0FFFFh if the cache information structure is not supported.
20h	Serial Number	Byte	String	String number for the serial number of this processor. This value is set by the manufacturer and normally not changeable.
21h	Asset Tag	Byte	String	String number for the asset tag of this processor.
22h	Part Number	Byte	String	String number for the part number of this processor. This value is set by the manufacturer and normally not changeable.
23h	Core Count	Byte	Varies	Number of cores per processor socket. If the value is unknown, the field is set to 0. See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.5.6 for more information.
24h	Core Enabled	Byte	Varies	Number of enabled cores per processor socket. If the value is unknown, the field is set 0. See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.5.7 for more information.
25h	Thread Count	Byte	Varies	Number of threads per processor socket. If the value is unknown, the field is set to 0. See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.5.8 for more information.
26h	Processor Characteristics	Word	Bit Field	Defines which functions the processor supports. See the System Management BIOS Reference

				Specification, Version 3.5.0, Section 7.5.9 for more information.
28h	Processor Family 2	Word	Enum	Processor Family 2 is identical to Processor Family field.

2.6.6 Type 7 Structure – Cache Information

Offset	Name	Length	Value	Description
00h	Type	Byte	7	Cache information indicator.
01h	Length	Byte	1Bh	Number of bytes in this type structure.
02h	Handle	Word	Varies	The number of this structure in the table.
04h	Socket Designation	Byte	String	Number of Null terminated string. Same as associated processor.
05h	Cache Configuration	Byte	Varies	Bits 15:10 0 = Reserved Bits 9:8 00b = Write through 01b = Write back 10b = Varies with memory address 11b = Unknown Bit 7 0b = Disabled at boot time 1b = Enabled at boot time Bits 6:5 00b = Internal Bit 4 0 = Reserved Bit 3 1 = Socketed Bits 2:0 Cache level, zero-based
07h	Maximum Cache Size	Word	Varies	Bit 15 0 = 1K granularity 1 = 64K granularity Bits 14:0 Max size in granularity
09h	Installed Size	Word	Varies	Bit 15 0 = 1k granularity 1 = 64k granularity Bits 14:0 Installed size in granularity Set to 0 if no cache or processor installed.
0Bh	Supported SRAM Type	Word	Bit Field	See the System Management BIOS

				Reference Specification, Version 3.5.0, Section 7.8.2 for values.
0Dh	Current SRAM Type	Word	Bit Field	See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.8.2 for values.
0Fh	Cache Speed	Word	Varies	In nanoseconds. Set to 0 if unknown.
10h	Error Correction Type	Byte	Enum	The error-correction scheme supported by this cache component. See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.8.3 for values.
11h	System Cache Type	Byte	05h	05h = Unified cache
12h	Associativity	Byte	Enum	Shows the values for the Cache Information. See the System Management BIOS Reference Specification, Version 3.7.0, Section 7.8.5 for values.

2.6.7 Type 8 Structure – Port Connector Information

The SMBIOS Type 8 structure provides the attributes for all internal and external ports or connectors in the server. There is one type 8 structure for each port/connector.

2.6.8 Type 9 Structure – System Slots

The SMBIOS Type 9 structure describes the attributes of the expansion slots in the server. One Type 9 structure is present for each slot in the server.

2.6.9 Type 16 Structure – Physical Memory Array

Offset	Name	Length	Value	Description
00h	Type	Byte	10h	Physical memory array type.
01h	Length	Byte	17h	Number of bytes in this type structure.
02h	Handle	Word	Varies	The number of this structure in the table.
04h	Location	Byte	Enum	03h = System board or motherboard.
05h	Use	Byte	Enum	03h = System

				memory.
06h	Memory Error Correction	Byte	Enum	See the System Management BIOS Reference Specification, Version 3.5.0, Section 7.17.3. This field is set to Multi-bit ECC.
07h	Maximum Capacity	DWord	Varies	The maximum memory capacity, in KB, for this array. Value 1TB or greater must be represented in the Extended Maximum Capacity field.
0Bh	Memory Error Handle Information	Word	0FFFEh	Type 18 is not supported.
0Dh	Number of Memory Devices	Word	Varies	The number of sockets available for memory devices in this array.
0Fh	Extended Maximum Capacity	Qword	Varies	The maximum memory capacity, in bytes, for this array. This filed is only valid when the Maximum Capacity field contains 8000_0000h.

2.6.10 Type 17 Structure –Memory Device

Offset	Name	Length	Value	Description
00h	Type	Byte	11h	Memory device type.
01h	Length	Byte	Varies	Length varies, minimum of 15h.
02h	Handle	Word	Varies	The number of this structure in the table.
06h	Memory Error Information Handle	Word	0FFFEh	Type 18 is not supported.
08h	Total Width	Word	Varies	Total width, in bits, of this memory device, including any check or ECC bits. If no error-correction bit, total width = data width.
0Ah	Data Width	Word	Varies	The data width in bits.
0Ch	Size	Word	Varies	The size of the memory device in MB if bit[15] = 0, or in KB if bit[15] = 1. If the socket is empty or there is an error, this should be 0.
0Eh	Form Factor	Byte	Enum	09h = DIMM
0Fh	Device Set	Byte	Varies	Identifies when the memory device is

				one of a set of memory devices that must be populated with all devices of the same type and size, and the set to which this device belongs. A value of 0 indicates that the device is not part of a set; a value of FFh indicates that the attribute is unknown. The device sets are based on the lock-stepped operation concept. Therefore, a DDR-3 DIMM will always belong to a unique lock-stepped pair (or device set). Note: A device set number must be unique within the context of the memory array containing this memory device.
10h	Device Locator	Byte	String	The string number of the string that identifies the physically-labeled (from the label on the server board) socket or board position where the memory device is located, e.g., “DIMM_A1”.
11h	Bank Locator	Byte	String	The string number of the string that identifies the physically labeled bank where the memory device is located.
12h	Memory Type	Byte	Enum	Type of memory used in this device; 22h = DDR5
13h	Type Detail	Word	Bit Field	Additional details on the memory device type. Bit 7 = 1 (Synchronous).
15h	Speed	Word	Varies	Identifies the maximum capable frequency of the device, in MHz.
17h	Manufacturer	Byte	String	The string number manufacturer of this memory device.
18h	Serial Number	Byte	String	The string number for the serial number of this memory device.

				This value is set by the manufacturer and normally not changeable.
19h	Asset Tag	Byte	String	The string number for the asset tag of this device.
1Ah	Part Number	Byte	String	The string number for the part number of this memory device. This value is set by the manufacturer and normally not changeable.
1Bh	Attributes	Byte	Varies	Bit 7:4 0 = Reserved Bits 3:0 Rank number of this memory device.
1Ch	Extended Size	DWord	Varies	The extended size of this memory device, intended to represent memory devices larger than 32767 MB (32GB) which cannot be described using the Size field. For compatibility with older SMBIOS parsers, memory devices smaller than 32GB should be represented using their size in the Size field, leaving the Extended Size field set to 0.
20h	Configured Memory Clock Speed	Word	Varies	Indentifies the configured clock speed of the memory device, in MHz.

2.6.11 Type 19 Structure –Memory Array Mapped Address

The SMBIOS Type 19 structure describes the attributes of each contiguous memory address range in the server. There is one Type 19 structure present for each address range.

2.6.12 Type 41 Structure – Onboard Devices Extended Information

Offset	Name	Length	Value	Description
00h	Type	Byte	29h	Onboard Devices Extended Information.
01h	Length	Byte	0Bh	Number of bytes in this type structure.

02h	Handle	Word	Varies	The number of this structure in the table.
04h	Reference Designation	Byte	String	String number of the onboard device reference designation. It is typically the silkscreen label.
05h	Device type	Byte	ENUM	Bit 7 – Device Status: 1 – Device Enabled 0 – Device Disabled Bits 6:0 – Type of Device (see 7.42.2)
06h	Device Type Instance	Byte	Varies	Device Type Instance is a unique value (within a given onboard device type) used to indicate the order the device is designated by the system. It is aligned with typically the silkscreen label.
07h	Segment Group Number	Word	Varies	The value is 0h for single-segment topology.
09h	Bus Number	Byte	Varies	Bus Number of the onboard device.
0Ah	Device/Function number	Byte	Varies	Device/Function Number of the onboard device. Bits 7:3 – Device number Bits 2:0 – Function number

2.6.13 Type 127 Structure –End-of-Table

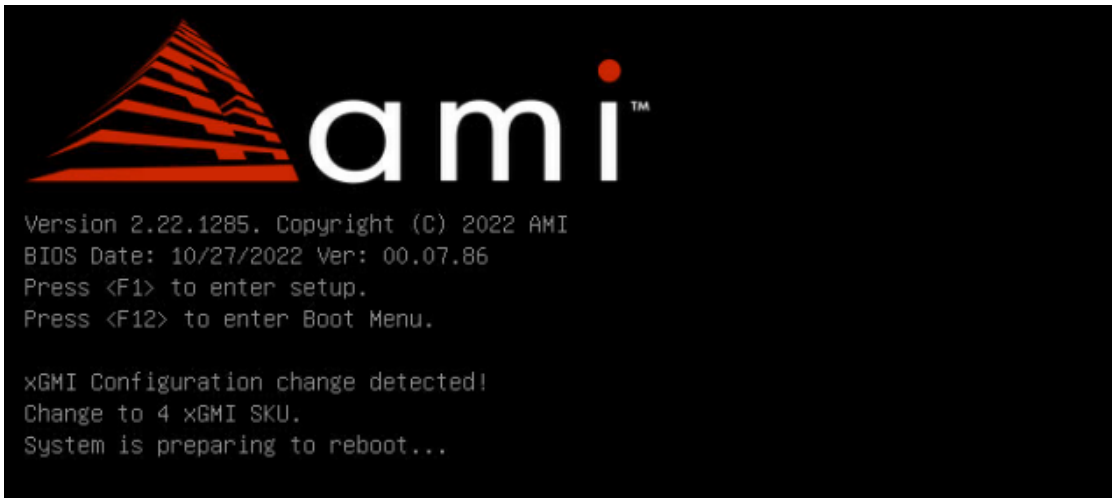
The SMBIOS Type 127 structure identifies the end of the structure table that might be earlier than the last byte within the buffer specified by the structure. To ensure backward compatibility with management software written to previous versions of the SMBIOS specification, the structure table is still reported as a fixed-length and the entire length of the table is still able to be indexed. If the end-of-table indicator is used in the last physical structure in a table, the field's length is encoded as 4.

2.7 Auto xGMI Configuration

BIOS support 3 xGMI or 4 xGMI configuration automatically. User can follow below step to change the xGMI configuration easily.

3 xGMI to 4 xGMI:

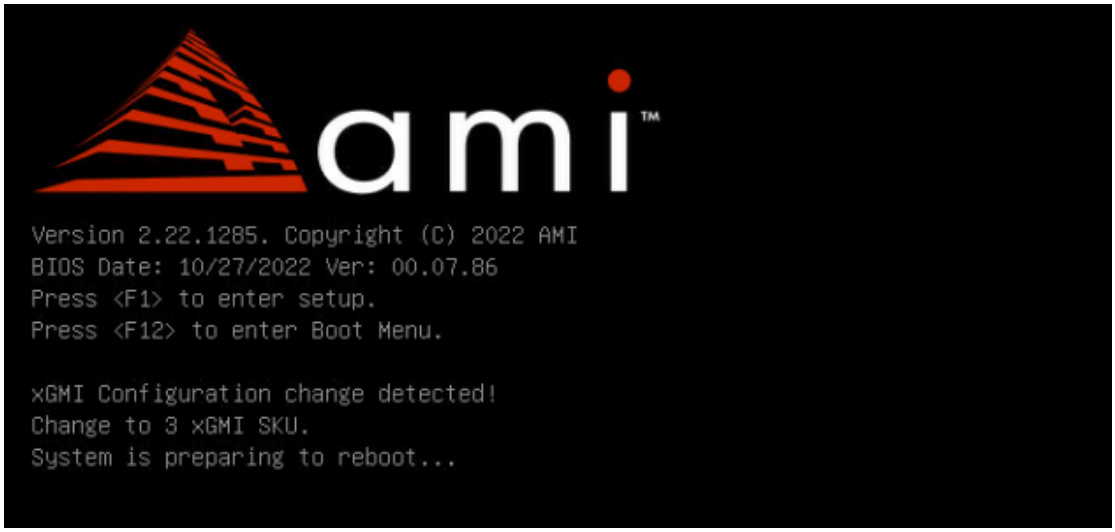
1. AC power off system
2. Connect xGMI cable on MCIO connector JP86, JP87, JP88, JP92 well. (Follow cable routing document)
3. AC power on system.
4. System will perform a reset during POST, then it will be 4 xGMI at next boot.



4 xGMI to 3 xGMI:

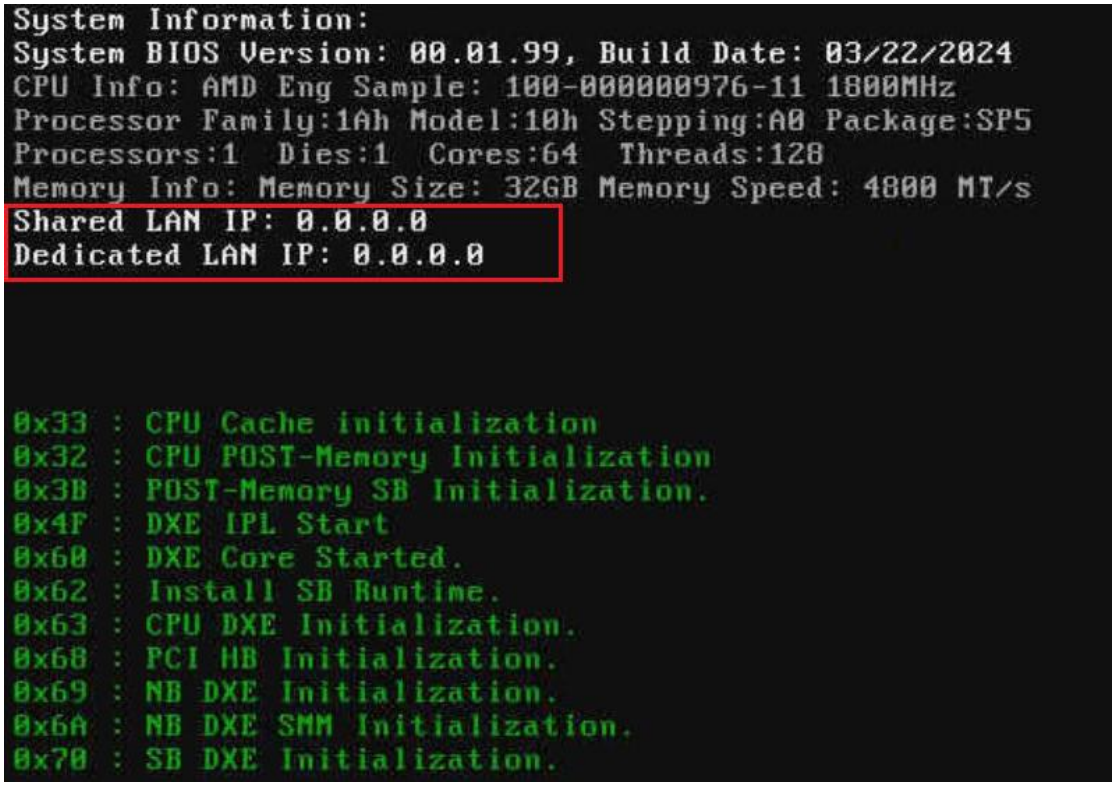
1. AC power off system
2. **Clear CMOS** by JP51 jumper. (short JP51 pin 2-3 for 5 second)
3. Un-connect xGMI cable on MCIO connector JP86, JP87, JP88, JP92 . (Follow cable routing document)
4. AC power on system.

System will perform a reset during POST, then it will be 3 xGMI at next boot.



2.8 Show BMC IP in early video

System can show BMC IP address at early POST phase



2.9 Display Logo Support

The BIOS support display customer logo at POST time.

If Quiet Boot is enabled in the BIOS setup, a “splash screen” is displayed with a logo image, which may be the standard Logo Screen or a customized OEM logo screen. By default, Quiet Boot is disabled in the BIOS setup. If the logo is displayed during POST, the user can press <TAB> to hide the logo.

2.10 System Event during POST Phase

During POST stage, BIOS will detect below system event show and send SEL to BMC if event happened.

POST Event	No Keyboard detected
	RTC Error
	USB Port over current detected

2.11 USB OC

During POST stage, BIOS will detect whether system USB port occur over current event, if occurred, BIOS will prompt below message and send SEL to BMC.

3.Setup menu

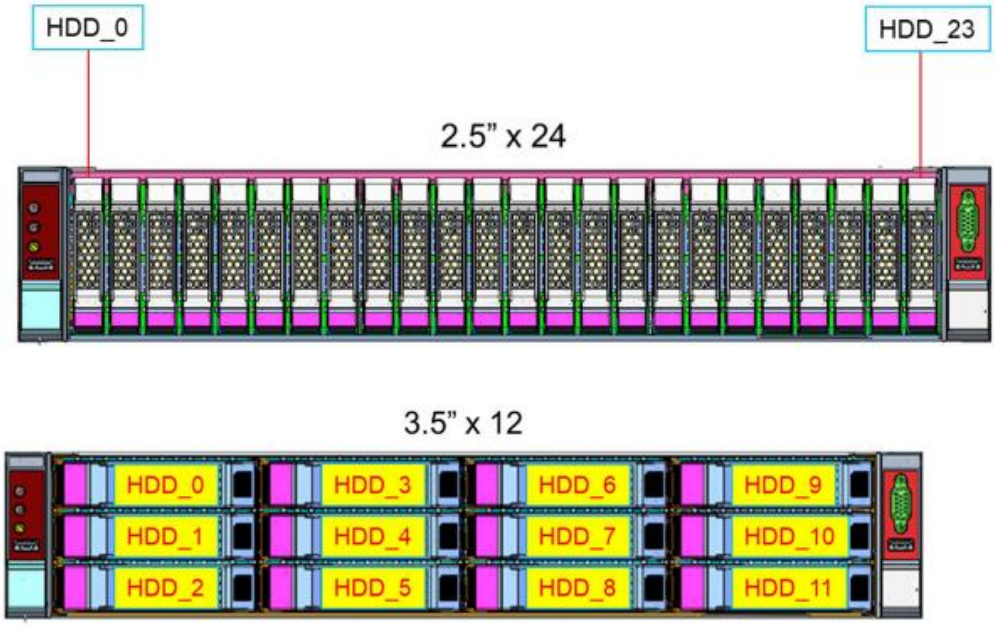
Please refer to SR124-2A/SR224-2A BIOS Setup Manual document.

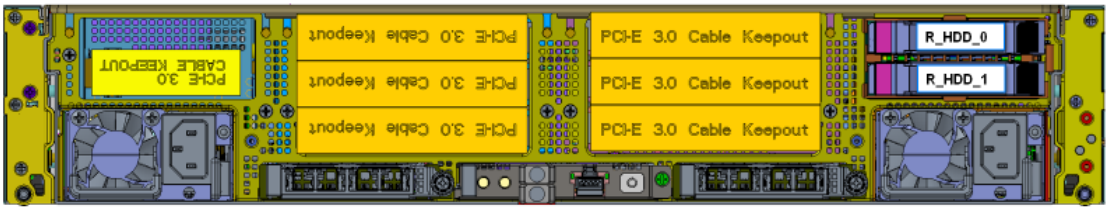
4.SW Slot Number

4.1 IO device slot ordering

Please refer to SR124-2A Specification/ SR224-2A Specification for detail of IO device slot ordering.

4.2 NVME slot number:





Front NVME:

HDD number	HDD_0	HDD_1	HDD_#	HDD_23
SW Slot Number	40	41	# + 40	63

Rear NVME:

HDD number	R_HDD_0	R_HDD_1
SW Slot Number	64	65

4.3 OCP slot number:

OCP	OCP slot1 x16	OCP slot2 x8
SW Slot Number	30	31

4.4 M.2 slot number:

M.2	CPU0 M.2_0	CPU0 M.2_1
SW Slot Number	20	21

5.POST CODE

POST code is a value used to indicate progress during the boot phase. These values are typically output to I/O port 80h.

Noticed: AGESA post code

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

SEC Phase	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded
PEI Phase	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL
0x31	Memory Installed

0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AMI error codes
DXE Phase	
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)

0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable

0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL
0xAB	Setup Input Wait
0xAC	Reserved for ASL
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (Load Image returned error)
0xDA	Boot Option is failed (Start Image returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available