Document Identifier: DSP0270

Date: 2023-08-03

Version: 1.3.1

Redfish Host Interface Specification

Supersedes: 1.3.0

Document Class: Normative

Document Status: Published

Document Language: en-US

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. Members and non-members may reproduce DMTF specifications and documents, provided that correct attribution is given. As DMTF specifications may be revised from time to time, the particular version and release date should always be noted.

Implementation of certain elements of this standard or proposed standard may be subject to third party patent rights, including provisional patent rights (herein "patent rights"). DMTF makes no representations to users of the standard as to the existence of such rights, and is not responsible to recognize, disclose, or identify any or all such third party patent right, owners or claimants, nor for any incomplete or inaccurate identification or disclosure of such rights, owners or claimants. DMTF shall have no liability to any party, in any manner or circumstance, under any legal theory whatsoever, for failure to recognize, disclose, or identify any such third party patent rights, or for such party's reliance on the standard or incorporation thereof in its product, protocols or testing procedures. DMTF shall have no liability to any party implementing such standard, whether such implementation is foreseeable or not, nor to any patent owner or claimant, and shall have no liability or responsibility for costs or losses incurred if a standard is withdrawn or modified after publication, and shall be indemnified and held harmless by any party implementing the standard from any and all claims of infringement by a patent owner for such implementations.

For information about patents held by third-parties which have notified DMTF that, in their opinion, such patent may relate to or impact implementations of DMTF standards, visit http://www.dmtf.org/about/policies/disclosures.php.

This document's normative language is English. Translation into other languages is permitted.

CONTENTS

Foreword

The Redfish Host Interface Specification was prepared by DMTF's Redfish Forum.

DMTF is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. For information about DMTF, see http://www.dmtf.org.

Acknowledgments

DMTF acknowledges the following individuals for their contributions to this document:

- Jeff Autor — Hewlett Packard Enterprise
- Jeff Bobzin — Insyde Software Corp
- Patrick Caporale — Lenovo
- Phil Chidester — Dell Technologies
- Chris Davenport — Hewlett Packard Enterprise
- Samer El-Haj-Mahmoud — Lenovo
- Jeff Hilland — Hewlett Packard Enterprise
- John Leung — Intel Corporation
- Edward Newman — Hewlett Packard Enterprise
- Michael Raineri — Dell Technologies
- Hemal Shah — Broadcom Limited
- Paul Vancil — Dell Technologies

1 Abstract

This specification defines functional requirements for Redfish host interfaces. In the context of this document, the term "host interface" refers to interfaces that can be used by software running on a computer system to access the Redfish service that is used to manage that computer system.

The target audience for this specification is system manufacturers that are providing Redfish host interfaces within computer systems, system and component manufactures that are providing devices or firmware that include or support Redfish host interfaces, and system firmware and software writers that are creating software or firmware that uses Redfish host interfaces.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated or versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies. For references without a date or version, the latest published edition of the referenced document (including any corrigenda or DMTF update versions) applies.

- DMTF DSP0134 System Management BIOS Reference Specification (SMBIOS), https://www.dmtf.org/standards/smbios
- UEFI Unified Extensible Firmware Interface Specifications (UEFI), http://www.uefi.org/specifications
- DMTF DSP0239 Management Component Transport Protocol (MCTP) IDs and Codes, Version 1.4, http://www.dmtf.org/sites/default/files/standards/documents/DSP0239_1.4.pdf
- DMTF DSP0266 Redfish Scalable Platforms Management API Specification, http://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.0.pdf
- ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, http://isotc.iso.org/livelink/livelink.exe?func=ll&objId=4230456&objAction=browse&sort=subtype
- PCI Firmware Specification, PCI SIG http://pcisig.com/specifications/conventional/pci_firmware
- IETF RFC4122, A Universally Unique IDentifier (UUID) URN Namespace, The Internet Society, July 2005, http://www.ietf.org/rfc/rfc4122.txt

3 Terms and definitions

In this document, some terms have a specific meaning beyond the normal English meaning. Those terms are defined in this clause.

The terms "shall" ("required"), "shall not", "should" ("recommended"), "should not" ("not recommended"), "may", "need not" ("not required"), "can" and "cannot" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 7. The terms in parenthesis are alternatives for the preceding term, for use in exceptional cases when the preceding term cannot be used for linguistic reasons. Note that ISO/IEC Directives, Part 2, Clause 7 specifies additional alternatives. Occurrences of such additional alternatives shall be interpreted in their normal English meaning.

The terms "clause", "subclause", "paragraph", and "annex" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 6.

The terms "normative" and "informative" in this document are to be interpreted as described in ISO/IEC Directives, Part 2, Clause 3. In this document, clauses, subclauses, or annexes labeled "(informative)" do not contain normative content. Notes and examples are always informative elements.

The following additional terms are used in this document.

Term	Definition
Host	The computer system that is managed by a Redfish service.
Host software	The software running on the host computer system, including operating system and its software components (such as drivers or applications), as well as pre-boot software such as UEFI or BIOS drivers and applications.
Redfish service	Also referred to as the "service". The collection of functionality that implements the protocols, resources, and functions that deliver the interface defined by the Redfish Specification and its associated behaviors for one or more managed systems.
Redfish service entry point	Also referred to as "service entry point". The interface through which a particular instance of a Redfish service is accessed. A Redfish service may have more than one service entry point.
Redfish manager	Also referred to as "manager". The entity that manages a computer system and other peripherals through a Redfish service.

4 Symbols and abbreviated terms

The following additional abbreviations are used in this document.

Term	Definition
BIOS	Basic I/O System. Name for system firmware typically used for initialization and launching the boot of an ISA (Industry Standard Architecture), aka "x86" or "PC", architecture-based computer system.
BSP	Board Support Package. Name for system firmware typically used for initialization and launching the boot of Linux in a computer system that uses a non-ISA architecture, but may be used for booting other types of operating systems or runtime software.
SMBIOS	System Management BIOS. Refers to DSP0134. Defines memory mapped tables, typically implemented by system firmware/BIOS and mapped into system firmware/BIOS memory space, that provide inventory and management information for the computer system.
UEFI	Unified Extensible Firmware Interface. A modern firmware standard that defines the interfaces between hardware and operating systems in a computer system. UEFI is supported on multiple processor architectures, including x86, x64, ia64, and AARCH64.
HI	Host interface.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol over TLS.
IP	Internet Protocol.
IPMI	Intelligent Platform Management Interface.
NIC	Network interface controller.
PCI	Peripheral Component Interconnect.
PCIe	Peripheral Component Interconnect Express.
TCP	Transmission Control Protocol.
UUID	Universally Unique Identifier.

5 Introduction

Redfish is a flexible system management tool that can be successfully applied to various system architectures. One important architecture consists of one or more CPUs assigned to the system application (the host CPUs) and a separate CPU or CPUs assigned solely to management including publishing the Redfish interface. In many management schemes, it is necessary to provide standardized Redfish-based communication between the host CPU and the Redfish service in the management unit. This communication is in addition to the Redfish services available via the external network. Implementation of the Redfish host interface is optional for the system designer. If provided, this interface may be used in both the pre-boot (firmware) stage and by drivers and applications within the host operating system and is designed to be available without use of external networking. This specification provides design details for several methods of host-to-service communication. Additional methods may be added in future revisions of this specification.

5.1 Scope

This specification is targeted to system manufacturers that are providing Redfish host interfaces within computer systems, system and component manufactures that are providing devices or firmware that include or support Redfish host interfaces, and system firmware and software writers that are creating software or firmware that uses Redfish host interfaces.

The specification covers host accessible physical and logical communication paths and protocols that are used to access the Redfish service that manages that host.

The specification also defines certain supporting elements in the host, such as SMBIOS extensions, that enable inventory and discovery functions.

The specification does not seek to place specific hardware implementation requirements. However, it does specify how hardware-specific interfaces are identified for host software, such as with SMBIOS structures.

The specification defines connectivity between a Redfish service and a host. Any network routing or other connectivity beyond the Redfish service or other networks is out of scope.

5.2 Goals

The following are the goals for the Redfish host interface:

- Implementable with existing management controller technology.
- Easily integrated into products.

- Host interface and out-of-band API must be the same, where possible, so that client applications have minimal, if any, change to adapt.
- Support authentication, confidentiality, and integrity:
  - Support environments where users do not want to solely rely on host or OS access control mechanisms.
  - Provide mechanisms to optionally, if configured, pass credentials to an OS kernel for sensor monitoring, with configurable privilege.
- Support multi-service to multi-host architectures:
  - For example, blade systems with a chassis manager as well as sled management controller on each blade, each with a host interface.
- Support security requirements with authentication and confidentiality.

6 Protocol details

A Redfish host interface shall support one of the following protocols:

- Network host interface: Redfish HTTP requests/responses over a TCP/IP network connection between a Host and Redfish service.

6.1 Network host interface protocol details

Implementations that support the network host interface protocol shall implement the following requirements:

- Implementations shall provide a TCP/IP network connection that route TCP/IP traffic between a Redfish client executing on the host and the Redfish service.
- Implementations may provide any link-level driver and interconnect that implements a TCP/IP network connection between a host and a Redfish service. Example implementations include:
  - A USB Network Connection between a host and a Redfish service.
  - A host PCIe NIC that connects to a manager NIC.
  - A host PCIe NIC that connects to a management LAN that connects to a Redfish service.
- Implementations shall provide DSP0266-defined authentication and privilege authorization equivalent to the out-of-band Redfish interface.
  - Implementations shall allow authentication credentials that are valid on the external Redfish interface from the host interface.
  - Implementations may optionally support a configurable `AuthNone` authentication mode (no authentication required) that is configurable on the Redfish service for use on the host interface. If implemented, enablement of `AuthNone` shall be configurable, and the `RoleId` assumed by `AuthNone` requests shall be configurable as described by the Redfish `HostInterface` schema.
  - Implementations may optionally support auto-generation and delivery of host interface-only credentials that may be used by the firmware or the OS to authenticate with the service.
  - If supported, auto-generated credentials for the host shall be delivered by using UEFI-based mechanism described in a later section of this document.
  - The permissions granted to any auto-generated credentials shall be configurable with a defined `RoleId` assigned.

- Services shall require HTTPS encryption for the network host interface with the same requirements as out-of-band network interfaces:
  - Session login with HTTP `POST` operations shall use HTTPS.
  - HTTP `PATCH` requests that contain sensitive data shall use HTTPS.
  - HTTP Basic authentication requests shall require HTTPS.
- Implementations that support SMBIOS shall provide an SMBIOS Type 42 structure that describes each host interface as defined by the SMBIOS standard and the SMBIOS support clause of this document.

DEPRECATED

- Implementations that support automatically generating and sending credentials to the host OS kernel or firmware using UEFI runtime variables shall be implemented as defined within the Delivery of credentials via UEFI runtime variables clause of this document.
  - If the kernel authentication interface is implemented, the Redfish service shall implement a configuration option that allows customers to disable the kernel authentication as described by the Redfish `HostInterface` schema.
  - If the kernel authentication interface is implemented, the Redfish service shall implement a configurable role for the kernel authentication interface as described by the Redfish `HostInterface` schema.

END DEPRECATED

---

7 SMBIOS support

Information in the SMBIOS structure shall allow host software to discover the Redfish service entry point supported and to initialize the driver stack on the host.

For network host interfaces, the structure shall contain the mechanism to discover or obtain the Redfish service entry point IP address.

All SMBIOS structures referenced in this specification shall assume a little-endian ordering convention, unless explicitly specified otherwise, i.e., multi-byte numbers (word, dword, etc.) are stored with the low-order byte at the lowest address and the high-order byte at the highest address. Unless otherwise noted, strings in these structures follow the "text strings" pattern described in the SMBIOS Specification.

7.1 SMBIOS Type 42 structure general layout

The SMBIOS Type 42 structure describes a management controller host interface. It consists of standard SMBIOS entry information, followed by interface descriptors, which describes the physical interface to the Redfish service, and protocol descriptors, which describes the supported payload encoding between the host and Redfish service. The following table shows the general format of the SMBIOS Type 42 structure:

```
-------------------------
Type 42 header
-------------------------
Interface specific data
  - Device description
  - (1 of 5 types)
-------------------------
  Protocol record header
-------------------------
  - Protocol specific data
-------------------------
```

Further details about the SMBIOS type 42 structure can be found in the SMBIOS Specification.

The remaining sections document how the SMBIOS type 42 structure is defined for use by the Redfish host interface.

7.2 Table 1: SMBIOS type 42 structure definition for Redfish

host interfaces

The following describes the SMBIOS management controller host interface (type 42) structure. Offsets 00h to 04h contain the type 42 header. Starting at offset 05h is the interface-specific data.

Offset	Name	Length	Value	Description
00h	Type	Byte	42	Management controller host interface structure indicator.
01h	Length	Byte	Varies	Length of the structure, a minimum of 09h.
02h	Handle	Word	Varies	
04h	Interface type	Byte	Enum	Management controller interface type. Network host interface is 40h.
05h	Interface-specific data length (N)	Byte	N	Number of bytes (N) containing interface-specific data. If 0, there is no interface-specific data.
06h	Interface-specific data	N bytes	Varies	Management controller host interface data as specified by the interface type. See Table 2 for the network host interface definitions.
06h+N	Protocol count	Byte	X	X number of protocol records for this host interface. This is typically 1.
07h+N	Protocol records	M bytes	Varies	Protocol records for each protocol supported. See Table 10 for the record format.

7.3 Table 2: Interface-specific data for interface type 40h

The interface-specific data starts at offset 06h of the SMBIOS type 42 structure. This table defines the interface-specific data for interface type 40h. There are several types of device descriptors defined in Table 3. However, a single type 42 table instance only allows for one interface-specific descriptor.

Offset	Name	Length	Value	Description
00h	Device type	Byte	Enum	The device type of the interface. The value of this field determines how the device descriptor data is decoded. See Table 3.
01h	Device descriptor data	N-1 bytes	Varies	The device descriptor data formatted based on the device type. See Table 4, Table 5, Table 6, Table 7, and Table 8.

7.3.1 Table 3: Device type values

The following table defines the possible values for the device type field found in Table 2.

Value	Description
02h	USB network interface. See Table 4.
03h	PCI/PCIe network interface. See Table 5.
04h	USB network interface v2. See Table 6.
05h	PCI/PCIe network interface v2. See Table 7.
80h-FFh	OEM. See Table 8.
Others	Reserved.

7.3.2 Table 4: Device descriptor data for device type 02h, USB network interface

The following table defines the device descriptor data format when the device type field is 02h, which indicates the device is a USB network interface.

Offset	Name	Length	Value	Description
00h	Vendor ID	Word	Varies	The vendor identifier of the device, as read from the "idVendor" field of the USB descriptor, LSB first.
02h	Product ID	Word	Varies	The product identifier of the device, as read from the "idProduct" field of the USB descriptor, LSB first.
04h	Serial number descriptor length	Byte	Varies	The number of bytes of the serial number, serial number descriptor type, and serial number descriptor length, as read from the "iSerialNumber.bLength" field of the USB descriptor. This field has a minimum value of 02h.
05h	Serial number descriptor type	Byte	03h	The descriptor type of the serial number, as read from the "iSerialNumber.bDescriptorType" field of the USB descriptor. This is always 03h to indicate that the descriptor is a string.
06h	Serial number	Varies	Varies	The serial number of the device as a Unicode string without a NULL terminator, as read from the "iSerialNumber.bString" field of the USB descriptor. This string does not follow typical string patterns found elsewhere in SMBIOS definitions.

Examples type 02h descriptors:

- The vendor identifier is 0xAABB, the product identifier is 0xCCDD, and the serial number is "SN00001": `0xBB 0xAA 0xDD 0xCC 0x10 0x03 0x53 0x00 0x4E 0x00 0x30 0x00 0x30 0x00 0x30 0x00 0x30 0x00 0x31 0x00`.
- The vendor identifier is 0xAABB, the product identifier is 0xCCDD, but there is no serial number: `0xBB 0xAA 0xDD 0xCC 0x02 0x03`.

7.3.3 Table 5: Device descriptor data for device type 03h, PCI/PCIe network interface

The following table defines the device descriptor data format when the device type field is 03h, which indicates the device is a PCI/PCIe network interface.

Offset	Name	Length	Value	Description
00h	Vendor ID	Word	Varies	The vendor identifier of the PCI/PCIe device as read from the "Vendor ID" field of its PCI configuration space, LSB first.
02h	Device ID	Word	Varies	The device identifier of the PCI/PCIe device as read from the "Device ID" field of its PCI configuration space, LSB first.
04h	Subsystem vendor ID	Word	Varies	The subsystem vendor identifier of the PCI/PCIe device as read from the "Subsystem vendor ID" field of its PCI configuration space, LSB first.
06h	Subsystem ID	Word	Varies	The subsystem identifier of the PCI/PCIe device as read from the "Subsystem ID" field of its PCI configuration space, LSB first.

Examples type 03h descriptors:

- The vendor identifier is 0xAABB, the device identifier is 0xCCDD, the subsystem vendor identifier is 0x0011, and the subsystem identifier is 0x2233: `0xBB 0xAA 0xDD 0xCC 0x11 0x00 0x33 0x22`.

7.3.4 Table 6: Device descriptor data for device type 04h, USB network interface v2

The following table defines the device descriptor data format when the device type field is 04h, which indicates the device is a USB network interface, version 2.

Offset	Name	Length	Value	Description
00h	Length	Byte	Varies	Length of the structure, including the device type and length fields. The length is dependent on the version of the Redfish Host Interface Specification supported: • 11h for 1.3. • 0Dh for 1.2 and older.
01h	Vendor ID	Word	Varies	The vendor identifier of the device, as read from the "idVendor" field of the USB descriptor, LSB first.
03h	Product ID	Word	Varies	The product identifier of the device, as read from the "idProduct" field of the USB descriptor, LSB first.
05h	Serial number	Byte	String	The string number for the serial number of the device. The string data is read from the "iSerialNumber.bDescriptorType" field of the USB descriptor, and is converted from Unicode to ASCII and is NULL terminated. See "text strings" in the SMBIOS Specification for how this field is constructed.
06h	MAC address	6 bytes	Varies	The MAC address of the USB network device, most significant octet first.
0Ch	Device characteristics	Word	Varies	Additional characteristics for the device. See Table 9.
0Eh	Credential bootstrapping handle	Word	Varies	Handle of the interface to be used for credential bootstrapping via IPMI commands. The value is FFFFh if not supported.

7.3.5 Table 7: Device descriptor data for device type 05h, PCI/PCIe network interface v2

The following table defines the device descriptor data format when the device type field is 05h, which indicates the device is a PCI/PCIe network interface, version 2.

Offset	Name	Length	Value	Description
00h	Length	Byte	Varies	Length of the structure, including the device type and length fields. The length is dependent on the version of the Redfish Host Interface Specification supported: • 11h for 1.3. • 0Dh for 1.2 and older.
01h	Vendor ID	Word	Varies	The vendor identifier of the PCI/PCIe device as read from the "Vendor ID" field of its PCI configuration space, LSB first.

Offset	Name	Length	Value	Description
03h	Device ID	Word	Varies	The device identifier of the PCI/PCIe device as read from the "Device ID" field of its PCI configuration space, LSB first.
05h	Subsystem vendor ID	Word	Varies	The subsystem vendor identifier of the PCI/PCIe device as read from the "Subsystem vendor ID" field of its PCI configuration space, LSB first.
07h	Subsystem ID	Word	Varies	The subsystem identifier of the PCI/PCIe device as read from the "Subsystem ID" field of its PCI configuration space, LSB first.
09h	MAC address	6 bytes	Varies	The MAC address of the PCI/PCIe network device, most significant octet first.
0Fh	Segment group number	Word	Varies	The segment group number of the PCI/PCIe device as defined in the PCI Firmware Specification. The value is 0 for a single-segment topology.
11h	Bus number	Byte	Varies	The bus number of the PCI/PCIe device.
12h	Device/ function number	Byte	Varies	The device/function Number of the PCI/PCIe device. Bits 7:3 - Device number Bits 2:0 - Function number.
13h	Device characteristics	Word	Varies	Additional characteristics for the device. See Table 9.
15h	Credential bootstrapping handle	Word	Varies	Handle of the interface to be used for credential bootstrapping via IPMI commands. The value is FFFFh if not supported.

7.3.6 Table 8: Device descriptor data for device types 80h-FFh, OEM device

The following table defines the device descriptor data format when the device type field is 80h-FFh, which indicates the device is an OEM device.

Offset	Name	Length	Value	Description
00h	Vendor IANA	4 bytes	Varies	The IANA code for the vendor, MSB first.
04h	Vendor data	Varies	Varies	OEM defined data.

7.3.7 Table 9: Device characteristics

The following table defines the bit field for the device characteristics field found in Table 6 and Table 7.

Word bit position	Description
Bit 0	Credential bootstrapping via IPMI commands is supported.
Bits 1:15	Reserved.

7.4 Table 10: Protocol record data format

The protocol records start at offset 07h+N of the SMBIOS type 42 structure. The following table defines the general protocol record layout for Redfish over IP.

Offset	Name	Length	Value	Description
00h	Protocol type	Byte	Enum	The protocol type. Redfish over IP is 04h.
01h	Protocol-specific data length	Byte	P	The length of the protocol-specific record data field.
02h	Protocol-specific record data	P bytes	Varies	The data for the protocol as defined by the protocol type. See Table 11 for Redfish over IP definition.

7.4.1 Table 11: Redfish over IP protocol-specific record data

The protocol-specific record data starts at offset 02h of the protocol record structure. The following table defines the protocol specific data when the protocol type field is 04h, which indicates the protocol is Redfish over IP.

Offset	Name	Length	Value	Description
00h	Service UUID	16 bytes	Varies	Same as the Redfish service UUID in the Redfish service root. Set to all 0s if the UUID is not supported or is unknown.
10h	Host IP assignment type	Byte	Enum	The method for how the host IP address is assigned. See Table 12.

Offset	Name	Length	Value	Description
11h	Host IP address format	Byte	Enum	The format of the host IP address. See Table 13.
12h	Host IP address	16 bytes	Varies	Used for "static" and "auto configure". For IPv4, use the first 4 bytes and zero fill the remaining bytes. For IPv6, use all 16 bytes.
22h	Host IP mask	16 bytes	Varies	Used for "static" and "auto configure". For IPv4, use the first 4 bytes and zero fill the remaining bytes. For IPv6, use first byte for the prefix length and zero fill the remaining bytes.
32h	Redfish service IP discovery type	Byte	Enum	The method for how the Redfish service IP address is discovered. See Table 12.
33h	Redfish service IP address format	Byte	Enum	The format of the Redfish service IP address. See Table 13.
34h	Redfish service IP address	16 bytes	Varies	Used for "static" and "auto configure". For IPv4, use the first 4 bytes and zero fill the remaining bytes. For IPv6, use all 16 bytes. If this IP address is not known, this field shall be zero filled. Clients should refer to the "Redfish Service Hostname" field in this case.
44h	Redfish service IP mask	16 bytes	Varies	Used for "static" and "auto configure". For IPv4, use the first 4 bytes and zero fill the remaining bytes. For IPv6, use first byte for the prefix length and zero fill the remaining bytes.
54h	Redfish service IP port	Word	Varies	Used for "static" and "auto configure".
56h	Redfish service VLAN ID	Dword	Varies	Used for "static" and "auto configure". Values outside of the range 1 to 4094 shall indicate VLAN is disabled.

Offset	Name	Length	Value	Description
5Ah	Redfish service hostname length	Byte	Varies	The length in bytes of the Redfish service hostname field, including any NULL characters in the field.
5Bh	Redfish service hostname	Varies	Varies	The hostname of Redfish service. This string may end with zero or more NULL characters. This string does not follow typical string patterns found elsewhere in SMBIOS definitions.

The UUID is 128 bits long. Its format is described in RFC4122. Although RFC4122 recommends network byte order for all fields, the PC industry, including the ACPI, UEFI, and Microsoft specifications, has consistently used little-endian byte encoding for the first three fields: "time_low", "time_mid", "time_hi_and_version". The same encoding, also known as wire format, should also be used for the SMBIOS representation of the UUID.

- For example, the UUID {00112233-4455-6677-8899-AABBCCDDEEFF} is represented as: `0x33 0x22 0x11 0x00 0x55 0x44 0x77 0x66 0x88 0x99 0xAA 0xBB 0xCC 0xDD 0xEE 0xFF`.

In the above table, the host IP address, host IP mask, Redfish service IP address, and Redfish service IP mask fields shall be stored in network byte order.

- IPv4 Example: 10.12.110.57 is stored, from lowest offset first, as `0x0A 0x0C 0x6E 0x39 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00`.
- IPv6 Example: 2001:db8:63b3:1::3490 is stored, from lowest offset first, as `0x20 0x01 0x0D 0xB8 0x63 0xB3 0x00 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x34 0x90`.

7.4.2 Table 12: Assignment and discovery type values

The following table defines the possible values for the assignment and discovery type fields found in Table 11.

Value	Description
00h	Unknown.
01h	Static.
02h	DHCP.
03h	Auto configure.
04h	Host selected.

Value	Description
Others	Reserved.

7.4.3 Table 13: IP address format values

The following table defines the possible values for the host IP sddress format and Redfish service IP address format fields found in Table 11.

Value	Description
00h	Unknown.
01h	IPv4.
02h	IPv6.
Others	Reserved.

7.5 Multiple protocol records

The SMBIOS type 42 structure allows for multiple protocol records within a given type 42 entry. For Redfish, this could be used to describe both IPv4 and IPv6 information for a single Redfish service. However, due to the size of the Redfish over IP structure, it is likely not possible to use two protocol records in a single type 42 entry without going beyond the limit of the length field of the type 42 structure found at offset 01h. If multiple protocol records are needed to describe a single Redfish service, there should be a type 42 entry for each of the protocol records. The interface-specific data portion of each type 42 entry shall be identical if they map to the same Redfish service. Clients should interpret multiple type 42 entries with identical interface-specific data as a single Redfish service with multiple protocols.

This methodology also allows for multiple Redfish services to be described by multiple Type 42 entries. Clients should interpret type 42 entries with different interface-specific data as different Redfish services.

8 Credential bootstrapping via IPMI commands

Services may support provisioning a temporary account for the host interface using IPMI commands. This is to allow a host with no initial knowledge of the Redfish interface to create an initial account from which it can create a permanent account for the life of the system.

Services that support credential bootstrapping via IPMI commands shall:

- Implement the `CredentialBootstrapping` property defined in the `HostInterface` schema.
- Implement the `CredentialBootstrappingRole` property in the `Links` property defined in the `HostInterface` schema.

8.1 IPMI command definitions

The following clause defines IPMI commands added to the "group extension" NetFn (2Ch, 2Dh). The defining body code for Redfish is 52h.

The service shall implement the IPMI commands defined in this clause. The IPMI commands defined in this clause shall be rejected on interfaces that are not the system interface.

8.1.1 Get manager certificate fingerprint (NetFn 2Ch, Command 01h)

This command is used to get the fingerprint for the manager's TLS certificate for the host interface. In most cases, the manager will only have one certificate available. Clients should use the response data from this command when connecting over the host interface to verify the service's certificate matches.

Request data:

Byte	Data field
1	Group extension identification (52h).
2	Certificate number (1 based).

Response data:

Byte	Data field
1	Completion code: • 00h: Command completed normally. • 80h: Credential bootstrapping via IPMI commands is disabled. • CBh: Certificate number is invalid.
2	Group extension identification (52h).
3	Fingerprint hash algorithm: • 01h: SHA-256. The length of the fingerprint will be 32 bytes. • Others: Reserved.
4:N	Fingerprint of the manager's TLS certificate.

8.1.2 Get bootstrap account credentials (NetFn 2Ch, Command 02h)

This command is used to get the user name and password of the bootstrap account. When the manager receives this command, it shall generate a new user name and password for the bootstrap account, store the credentials in a manner consistent with other Redfish accounts, and provide the credentials in the response data to the host. The manager shall generate a unique user name, and shall randomly generate the password.

The user name and password shall:

- Be valid UTF-8 strings consisting of printable characters.
- Not include single quote (') or double quote (") characters.
- Not include backslash (\) characters.
- Not include whitespace characters.
- Not include control characters.
- Be at most 16 characters long.

Upon normal completion of this command, the `Enabled` property within the `CredentialBootstrapping` property of the host interface resource shall be set to `false`, unless the "disable credential bootstrapping control" parameter of the command contains the value `A5h`.

Request data:

Byte	Data field
1	Group extension identification (52h).

Byte	Data field
2	Disable credential bootstrapping control: • A5h: Keep credential bootstrapping enabled. • Other values: Disable credential bootstrapping upon normal completion of this command.

Response data:

Byte	Data field
1	Completion code: • 00h: Command completed normally. • 80h: Credential bootstrapping via IPMI commands is disabled.
2	Group extension identification (52h).
3:18	The user name as a UTF-8 string. Strings with fewer than 16 characters are terminated with a null (00h) character and 00h padded to 16 bytes.
19:34	The password as a UTF-8 string. Strings with fewer than 16 characters are terminated with a null (00h) character and 00h padded to 16 bytes.

8.2 Account life cycle

If the `Enabled` property within the `CredentialBootstrapping` property of the host interface resource is `false`, the get manager certificate fingerprint and get bootstrap account credentials commands shall be rejected and respond with the completion code 80h.

If the get bootstrap account credentials command has been issued and responds with the completion code 00h, a bootstrap account shall be added to the manager's account collection and enabled. If the get bootstrap account credentials command is sent subsequent times and responds with the completion code 00h, a new account shall be created based on the newly generated credentials. Any existing bootstrap accounts shall remain active.

Bootstrap accounts shall be usable only on the host interface.

Services shall delete all bootstrap accounts:

- On any reset of the service.
- On any reset of the host. Implementers may need to provision for the necessary mechanisms in order to detect a host reset, which could be hardware-based, UEFI-based, or a mixture of the two.

If the `EnableAfterReset` property within the `CredentialBootstrapping` property of the host interface resource is `true`, services shall set the `Enabled` property within the `CredentialBootstrapping` property of the host interface resource to `true`:

- On any reset of the service.
- On any reset of the host.

8.3 Recommendations for hosts

Anyone with root or administrative access to the host is able to make use of this mechanism for provisioning an account. However, it is recommended that this mechanism only be used during initial provisioning of a host. The overall workflow for using this interface is recommended to be:

1. Use this mechanism to create a bootstrap account. When issuing the get bootstrap account credentials command, do not set the "disable credential bootstrapping control" parameter of the command to `A5h`.
2. Using the bootstrap account, create a permanent account for the host in the manager account collection found in the account service.
3. Perform an HTTP `DELETE` on the `ManagerAccount` resource representing the bootstrap account.

9 Delivery of credentials via UEFI runtime variables

> **DEPRECATED:** This entire clause has been deprecated in favor of other credential negotiation mechanisms described in this specification, such as credential bootstrapping via IPMI commands.

DEPRECATED

This clause defines an optional mechanism for automatically generating and sending credentials to the Host OS kernel and/or firmware by using UEFI runtime variables. Services that implement the kernel authentication mechanism shall comply with the following subclauses:

9.1 Credential generation and management for use by firmware and OS kernel

Opening a Redfish session on the host interface may be accomplished by use of any authorized Redfish credentials consisting of a valid username and password. However in some situations, it may be difficult to pre-provision the system with valid Redfish credentials for use by OS and firmware clients of Redfish. Examples of this include early provisioning of new systems and systems where firmware does not have secure storage to hide the credentials.

To provide for situations of this type, systems supporting the Redfish service may optionally be configured to provide temporary login credentials for use by firmware pre-boot elements or the OS. If implemented, the credentials shall follow these requirements:

- The credentials shall be auto-generated by the Redfish service and provided to firmware and OS by using the UEFI variable interface variables described herein at the initiation of each system boot.
- The generation of both firmware and OS credentials shall be user-configurable with the option to disable or enable generation of the credentials separately for both firmware and OS kernel.
- The permissions of the resulting session shall be configurable through the Redfish service configuration as described by the Redfish `HostInterface` schema.
- The supplied credentials shall be in the form of a user id and password, both auto-generated by the Redfish service.
- Only one session using these auto-generated credentials shall be allowed at a time.
- The session associated with the auto-generated credentials shall not timeout or expire.
- The Redfish service may close the session if it resets or for other policy reasons in which case the

host may re-open the session using the same credentials.

- Any open session started with firmware credentials shall be closed and the credentials invalidated at UEFI `ExitBootServices()` event.
- Any open session started with OS credentials shall be closed and new credential passwords generated when a host restart is detected by the Redfish service.
- The firmware credentials shall be made available for any agent or driver that operates within the UEFI pre-boot prior to the `ExitBootServices()` call. This may include local system ROM firmware or utility firmware applications downloaded from external sources.

9.2 Security considerations for protecting auto-generated credentials

It is recommended that system designers protect the credentials from unauthorized access. The use of UEFI Secure Boot to protect access to credentials is recommended. Because of the difficulty of defining a security procedure for legacy-booting OS, delivery of credentials to a legacy OS is not described by this specification and any legacy OS support for this feature is OEM-specific.

The system OS is provided with a method of disabling further retrieval of the credentials after initial authorized retrieval. System designers are encouraged to implement such a scheme of retrieve, store, and disable to avoid unauthorized reading of the credential variables

9.3 UEFI implementation

Implementations that present a Redfish host interface for use by system firmware and OS shall use the UEFI variables defined in this section to deliver credentials for the Redfish host interface.

The design of this delivery mechanism is compatible with any UEFI version starting with 2.3.1. Refer to the specifications available at www.uefi.org for details on using the UEFI variable calls described here.

9.3.1 Prototype

```
#define EFI_REDFISH_INFORMATION_GUID \
    {0x16faa37e, 0x4b6a, 0x4891, {0x90, 0x28, 0x24, 0x2d, 0xe6, 0x5a, 0x3b, 0x70 }}
#define EFI_REDFISH_INFORMATION_INDICATIONS         L"RedfishIndications"
#define EFI_REDFISH_INFORMATION_FW_CREDENTIALS      L"RedfishFWCredentials"
#define EFI_REDFISH_INFORMATION_OS_CREDENTIALS      L"RedfishOSCredentials"
```

9.3.2 Related definitions

```
#define EFI_REDFISH_INDICATIONS_FW_CREDENTIALS      0x00000001
#define EFI_REDFISH_INDICATIONS_OS_CREDENTIALS      0x00000002
```

9.3.3 Description

This GUID and these variable names are used when calling the UEFI Runtime Service `GetVariable()`. See the UEFI Specification for details on use of this interface. As described below, the `SetVariable()` interface can be used to disable further access to the credential information.

The variables defined in this section have the following attributes:

- `EFI_REDFISH_INFORMATION_INDICATIONS` and `EFI_REDFISH_INFORMATION_OS_CREDENTIALS` have attributes `EFI_VARIABLE_BOOTSERVICE_ACCESS` and `EFI_VARIABLE_RUNTIME_ACCESS`.
- `EFI_REDFISH_INFORMATION_FW_CREDENTIALS` has attribute `EFI_VARIABLE_BOOTSERVICE_ACCESS`

The variable `EFI_REDFISH_INFORMATION_INDICATIONS` shall return a 32-bit value, and provides information if any credentials are provided for the Host Software use. The bits defined with this variable shall be interpreted as follows:

- If `EFI_REDFISH_ INDICATIONS_FW_CREDENTIALS` bit is 1, the Redfish Host Interface is configured to provide credentials for use by system firmware.
- If `EFI_REDFISH_ INDICATIONS_OS_CREDENTIALS` bit is 1, the Redfish Host Interface is configured to provide a credentials for use by system OS.
- All other bits in `EFI_REDFISH_INDICATIONS_HOST_IF` are reserved.

When the Redfish implementation provides credentials for firmware use, the variable `EFI_REDFISH_INFORMATION_FW_CREDENTIALS` shall contain a UTF-8 character array formatted as described in the next clause. If this session is not available as defined by current system policy, this variable shall return `EFI_NOT_FOUND`.

When the Redfish implementation provides credentials for OS use, the variable `EFI_REDFISH_INFORMATION_OS_CREDENTIALS` a UTF-8 character array formatted as described in the next clause. If these credentials are not available as defined by current system policy, this variable shall return `EFI_NOT_FOUND`.

The password contained in these variables shall be recalculated so as to be unique and not easily predicted on each boot.

If the variables `EFI_REDFISH_INFORMATION_FW_CREDENTIALS` or `EFI_REDFISH_INFORMATION_OS_CREDENTIALS` are

accessed using the `SetVariable()` function with a *DataSize* of zero, the variable contents shall be hidden until the next system restart and not be available for retrieval by future `GetVariable()` calls. After such `SetVariable()` access any `GetVariable()` attempt shall return `EFI_NOT_FOUND` error. Calls to `SetVariable()` with nonzero *DataSize* shall be processed as if *DataSize* is zero.

9.3.4 Variable format

The UEFI variables for delivery of temporary credentials shall contain an array of UTF-8 characters in the format `Username:Password` where the `:` character shall act as separator. The final byte of the array shall be 0x00 as terminator and the size of the variable shall be length of `Username` plus length of `Password` plus 2. Characters shall be chosen from the set elsewhere defined as legal for Redfish username and password and neither field may contain the `:` character.

For convenience when identifying the auto-generated credentials when active and for the purpose of editing permissions, the following username strings shall be used:

Usage	Username
Default firmware auto username.	HostAutoFW
Default OS auto username.	HostAutoOS

END DEPRECATED

10 ANNEX A (informative) Change log

Version	Date	Description
1.3.1	2023-08-03	Made many changes for style consistency, grammar, and general clarity. Except for the following additions, no normative changes were made. Any clarifications that inadvertently altered the normative behavior are considered errata, and will be corrected in future revisions to the specification.
		Clarified the behavior for populating the "Redfish service IP address" field if only the hostname is known.
		Updated the "Redfish service VLAN ID" field to describe how to populated it if VLAN is disabled.
		Updated the "Host IP mask" and "Redfish service IP mask" fields to describe how to populated them for IPv6.
1.3.0	2020-08-04	Added clauses for bootstrapping credentials via IPMI.
		Deprecated credential reporting via UEFI variables.
		Extended USB network interface v2 and PCI/PCIe network interface v2 descriptors to include device characteristics and credential bootstrapping handle fields.
1.2.0	2019-10-11	Added clause to allow for multiple SMBIOS Type 42 structures in order to specify multiple protocol records.
1.1.0	2019-05-16	Clarified the byte ordering in SMBIOS structures.
		Clarified the data shown in the device descriptor table.
		Clarified the format of the hostname field.
		Added example device descriptors.
		Added version 2 of the USB and PCI/PCI-e device descriptors.
		Clarified the format of the UUID.
1.0.1	2017-12-11	Errata release. Numerous terminology clarifications and typographical corrections.
		Terminology for "host", "manager", and "service" were edited for consistency.
		Added additional wording about the SMBIOS type 42 structure to describe its purpose.
		Added references to the UEFI Specification.
		Clarified byte ordering of IPv4 and IPv6 addresses in the SMBIOS type 42 structure.
		Added missing case for what to use for the UUID in the SMBIOS type 42 structure if it is unknown or not supported.

Version	Date	Description
1.0.0	2016-12-30	Initial release.