MOST

Media **O**riented **S**ystems **T**ransport

Multimedia and Control
Networking Technology

Diagnostic Protocols Adaptation Specification
Rev 3.1
06/2016

See page 3 for the terms of disclosure

MOST® COOPERATION

Legal Notice

SUPPORT AND FURTHER INFORMATION

For more information on the MOST technology, please contact:

MOST Cooperation
Administration
Emmy-Noether-Str. 14
76131 Karlsruhe
Germany

Tel: (+49) (0) 721 966 50 00
E-mail: contact@mostcooperation.com
Web: www.mostcooperation.com

This Specification is Confidential Information of the MOST Cooperation. It may only be disclosed to member companies. Member companies wishing to discuss these Specifications with suppliers or other third parties must ensure that a commercially standard form of non-disclosure agreement has been previously executed by the party receiving such Specifications. Use of these Specifications may only be for purposes for which they are intended by the MOST Cooperation. Unauthorized use or disclosure is a violation of law.

Contents

Document History

Revision 3.1

Change Ref.	Section	Changes
3V1_001	General	Removed DAP over Control Channel and MOST High Protocol.

Revision 1.0

Change Ref.	Section	Changes
1V0_001	General	Initial Version.

1 Introduction

1.1 References

All documents, which are referenced by this MOST document, are listed here along with their versions.

	Document	Revision
[1]	IETF: Internet Protocol, RFC 791	
[2]	IETF: Transmission Control Protocol, RFC 793	
[3]	IETF: User Datagram Protocol, RFC 768	
[4]	ISO: ISO/DIS 14229-1 - Road vehicles -- Unified diagnostic services (UDS) -- Part 1: Specification and requirements	
[5]	ISO: ISO/DIS 15765-2, Road vehicles -- Diagnostics on CAN -- Part 2: Network layer services	
[6]	MOST Cooperation: MOST Specification	3.1

Table 1-1: Document references

1.2 Scope

This document defines requirements for the adaptation of diagnostic protocols, e.g., UDS (Unified Diagnostic Services [4]) to MOST [6].

1.3 Definitions

Term	Description
API	Application Programming Interface
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
DAP	Diagnostic Adaptation Protocol
DoIP	Diagnostics on TCP/IP over Ethernet
GW	Gateway
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	IP Version 4
ISO	International Organization for Standardization
MOST	Media Oriented Systems Transport
OBD	On-Board Diagnostics
PDU	Protocol Data Unit
RFC	Request For Comments
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UDS	Unified Diagnostic Services

2 Overview

This document defines the usage of TCP (Transmission Control Protocol) for transporting physically addressed diagnostic messages over the Packet Data Channel of MOST. Furthermore, it defines the usage of UDP (User Datagram Protocol) for transmitting functionally addressed diagnostic messages on MOST.

The definition of an own diagnostic transport protocol—in the following called DAP (Diagnostic Adaptation Protocol)—is required in order to realize the adaptation from a diagnostic application protocol to the actual MOST transport and transmission protocols. This document defines necessary requirements while taking into account to keep DAP as simple as possible.

3 Technical Bases

In this chapter, the services and communication protocols that are relevant for this document are described.

3.1 UDS (Unified Diagnostic Services)

The UDS have been standardized by the ISO in [4]. This standard defines a diagnostic application layer protocol for the exchange of diagnostic data between vehicular devices and diagnostic test tools.

The definitions are independent on the used bus and communication system. The basic concept of this standard is that diagnostic services reside on devices. A diagnostic service can be used by transferring a request message from a diagnostic test tool to a device. In other words, the device contains several diagnostic servers, and the diagnostic test tool acts as client. After completion of the service execution, the device may send a response message back to the client.

The applicable ISO standards define two different addressing methods, called physical addressing [4] and functional addressing [4]. Physical addressing is used if there is a point-to-point communication between client and server. Functional addressing is used by the client if it does not know the physical server address or if a server is implemented in a distributed manner in several devices. In these cases, there is a broadcast communication between the client as sender and several servers as receivers.

3.2 TCP (Transmission Control Protocol)

The TCP has been standardized by the IETF in [2]. It is a transport protocol of the Internet protocol suite that provides reliable, in-order delivery of a stream of bytes by using services of the Internet protocol [1].

3.3 UDP (User Datagram Protocol)

The UDP has been standardized by the IETF in [3]. It allows the delivery of messages (datagrams) by using services of the Internet Protocol [1]. UDP does not guarantee reliability or message ordering.

4 Initial Situation

This chapter describes the topology and components which are the prerequisite for the applicability of the definitions made in this document. Furthermore, this chapter specifies the conditions for a proper transport protocol that is responsible for the delivery of diagnostic messages.

4.1 Topology

The topology depicted in Figure 4-1 is the background of the definitions in this document.

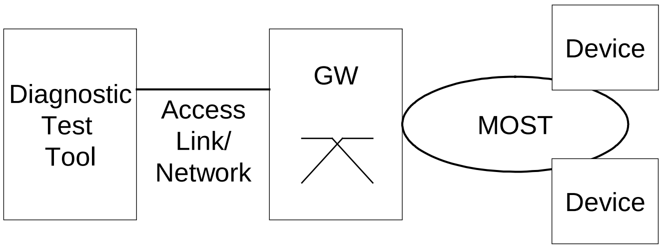

Figure 4-1: Basic topology

Diagnostic requests (e.g., UDS requests) are transferred from a diagnostic test tool via a GW (gateway) to the target devices that are connected on a MOST network and the diagnostic responses are transferred vice versa. The test tool is connected to a GW by a so called access link or access network. This link or network can be realized by one or more CANs or even by Fast Ethernet.

In case of an external test tool, the access network contains the vehicular OBD (On-Board Diagnostics) connector. The GW has to forward diagnostic requests via MOST to the devices. In the other direction, it has to forward diagnostic responses to the test tool via the access link or access network.

4.2 Store-And-Forward Gateway versus Pass-Through Gateway

A simple store-and-forward GW completely receives and reassembles a diagnostic message (request or response) before forwarding it. A CAN access link may use the transport protocol ISO 15765-2 [5]. In this case the GW has to reassemble all CAN frames to a diagnostic request, and afterwards it has to forward the whole request. In order to forward the request, it must segment it according to the used MOST transport protocol.

A pass-through GW directly forwards the received segments into the other network. The GW does not reassemble the segments to the diagnostic message and vice versa it does not divide the diagnostic message into segments.

In any case, one prerequisite of this specification is that the GW has to have end-points of the transport protocols of all connected networks. In the MOST network, the usage of ISO 15765-2 is not recommended. Rather, the DAP should be used in the MOST network.

4.3 Address Resolution

Normally, in order to forward the diagnostic message into the MOST network, the GW has to resolve applicative diagnosis addresses. This specification assumes that the GW works with an applicable address resolution algorithm. It is not the focus of this specification to define such an algorithm.

4.4 Conditions for the Transport of Diagnostic Messages on MOST

The protocols for transporting diagnostic messages on a MOST network have to provide mechanisms for segmenting diagnostic messages in appropriate packets/messages that are used for the actual transmission and vice versa the reassembly of them to diagnostic messages. Furthermore, they have to provide mechanisms that give the diagnostic application the ability to detect transport errors or even to avoid transport errors.

For functional addressing (broadcast), a suitable transport protocol has to provide a CRC on receiver side in order to give the receiver the ability to detect bit errors of the received diagnostic message.

For physical addressing (point-to-point), a suitable protocol has additionally to provide an acknowledgement mechanism in order to give the sender the ability to detect a successful reception. In case of no reception or an unsuccessful reception, a retry mechanism on sender side has to be provided. Moreover, a suitable protocol has to perform a flow control mechanism by controlling the transmission rate of the sender in order to avoid overloading a slow receiver.

5 Definitions

The following definitions consider the transport of diagnostic messages on MOST and the interface the device must offer.

5.1 Transport Protocols for Message Transfer

The applicable ISO standards define two different addressing methods, called physical addressing [4] and functional addressing [4].

Physical addressing

A MOST device has to use TCP (Transmission Control Protocol) for exchanging physically addressed UDS messages over the Packet Data Channel.

TCP uses services of the Internet protocol.

Functional addressing

UDP (User Datagram Protocol) over the Packet Data Channel is used for the exchange of functionally addressed diagnostic messages on MOST.

UDP uses services of the Internet protocol.

The responses to functionally addressed requests are sent using physical addressing.

Note: *Apart from the nominal transport channel capacity, there might be other limiting factors to the available bandwidth, for example, I/O interfaces; those, however, are outside the scope of this specification.*

5.2 DAP (Diagnostic Adaptation Protocol)

There is the need for introducing the DAP in order to realize the adaptation from a diagnostic application protocol (e.g., UDS) to the actual MOST transport and transmission protocols. For instance, UDS does not provide explicit information for the receiver about the length of the message by its transmission. For TCP and UDP the separation between two transmitted diagnostic messages on receiver side is generally unclear. A simple encapsulation of one diagnostic message in one TCP packet or UDS datagram defines a clear message separation. This solution leads to unintended message length limitation. Therefore, an explicit information about the message length is introduced by DAP.

5.2.1 Mechanisms of the DAP

Diagnostic messages must be transported only by using the DAP that is precisely defined in this document.

Figure 5-1 shows the protocol stacks that realize a diagnostic message exchange as defined in this document.

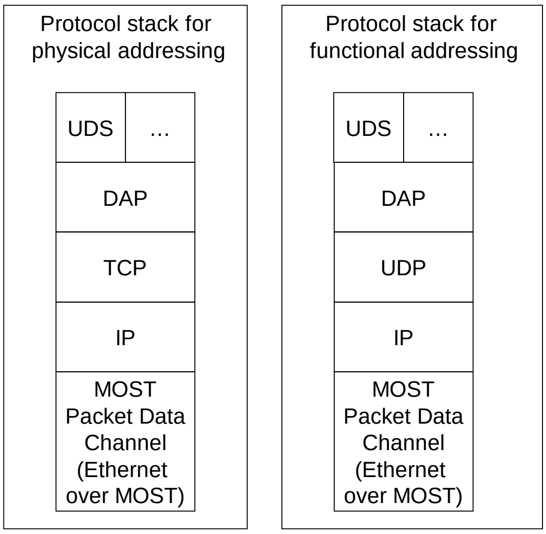

Figure 5-1: Protocol Stacks

The DAP provides a service that takes data from a diagnostic application protocol entity and passes it with additional information to an appropriate MOST transport/transmission protocol entity for immediate transfer from sender to receiver.

Furthermore, the DAP provides a service that takes data from an appropriate MOST transport/transmission protocol entity and passes the received diagnostic application-related data to the corresponding diagnostic application protocol entity.

Each diagnostic message must be transferred from sender to receiver as payload of one DAP PDU.

5.2.2 Structure of a DAP PDU

A DAP PDU has the following structure:

Byte Order	Data Field	Len (Byte)	Value
1	**Version of DAP Header**	1	Version 1: 0x01 Reserved for future use: 0x00; 0x02 – 0xFF
2 – 5	**Payload Length**	4	n
6	**Type of Service**	1	System Integrator specific: 0x00 UDS: 0x01 KWP2000: 0x02 Reserved for future use: 0x03 – 0xBF System integrator specific: 0xC0 – 0xFF
7 - 8	**System Integrator Part**	2	Default: 0xFFFF
9 – 10	**Source Address**	2	e.g., Diagnostic test tool address Default: 0xFFFF
11 – (10+n)	**Payload**	n	

Table 5-1: Structure of a DAP PDU

The first data field identifies the version of the DAP header as 0x01. After the data field “Payload Length” there is the data field “Type of Service”. Beside the familiar applicative diagnostic services UDS and KWP2000, on this place a system integrator can appoint the assignment of this PDU to another diagnostic or even non-diagnostic application.

The data field “Source Address” can be used to identify the test tool that has sent a request. A server device has to copy the data of this field – that describes the applicative diagnostic address of the test tool according to section 4.1 - from a diagnostic request to the corresponding diagnostic response. By this a GW can assign and forward the incoming diagnostic response to the appropriate test tool. This can be necessary if more than one test tools exist (e.g., one onboard test tool and one external test tool).

The data field “System Integrator Part” is set to 0xFFFF by default. However, the data field can be used by the system integrator, e.g., in order to work with sequence numbers if needed. Alternatively, it can be used for a 32-bit source addressing scheme. The “System Integrator Part” field can contain the source address’ higher 16 bits and the “Source Address” itself the lower 16 bits.

If a data field of a DAP PDU header contains a value that is reserved for future use, the DAP PDU has to be discarded by the receiver.

5.3 Application Interface Definitions

There is the need to assign received diagnostic messages to the proper diagnostic application of the device. By this view, DAP is part of this diagnostic application.

5.3.1 Interface Definition if TCP or UDP is used

The interface of all physically addressed diagnostic services of a device is given by the TCP service port 49152. This means that on this port a MOST device has to listen for requesting the establishment of the TCP connection by the GW.

On UDP port 49152 a MOST device has to listen for UDP datagrams that encapsulate functionally addressed diagnostic requests.

6 Application of DAP

The following sections contain DAP application examples.

6.1 Segmentation of PDUs

Figure 6-1 depicts PDU encapsulation examples in case of using TCP or UDP.

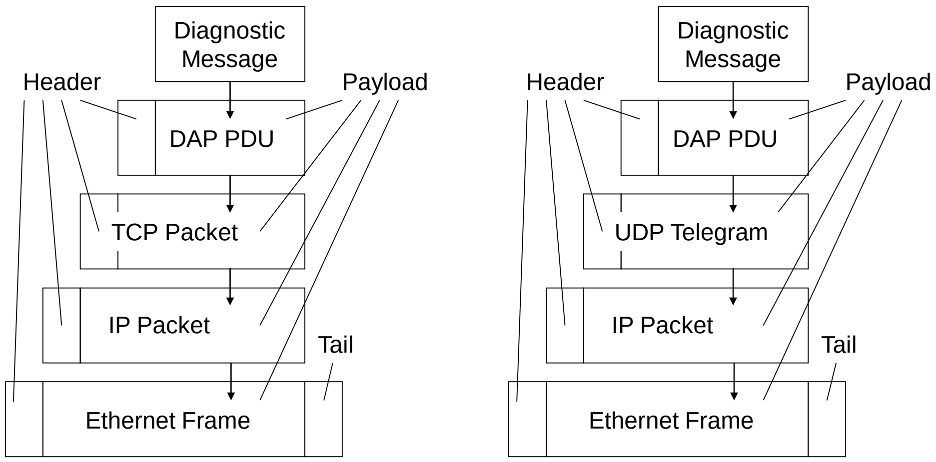

Figure 6-1: Encapsulation of a diagnostic message in one transport PDU

A diagnostic message is encapsulated in one DAP PDU. This is further encapsulated in a TCP packet or an UDP telegram.

Segmentation of DAP PDUs is needed if the length of the PDU of the subjacent layer that encapsulates the DAP PDU is limited. It is also needed if the gateway provides “Pass Through” functionality. In this case it inherently has to transmit segments of a diagnostic request as defined in this section.

6.1.1 Segmentation in TCP Packets

The TCP API (Application Programming interface) is stream-oriented. PDU encapsulations as depicted in Figure 6-3 are possible. A separation of DAP PDUs received in one data stream is possible by analysing the data field “Payload Length” of the DAP header.

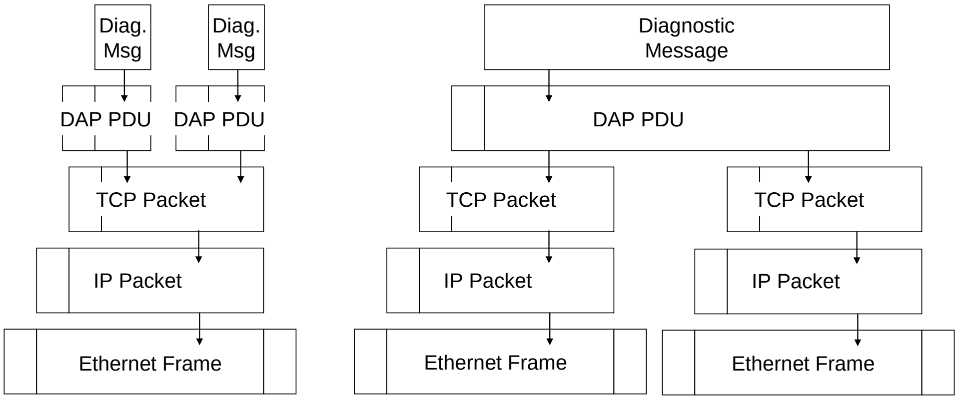

Figure 6-2: Encapsulation examples by using TCP

6.1.2 Segmentation in UDP Telegrams

To simplify matters, a DAP PDU does not contain a CRC. Because UDP is unreliable, packet losses are possible. Therefore, for UDP the condition of Section 4.4 “there is to give the receiver the ability to detect bit errors of the received diagnostic message” can only be met if a functionally addressed diagnostic message is exchanged by only one UDP datagram (= UDP packet). In this case, the UDP datagram CRC can be utilized in order to detect bit errors of the PDU. It is still possible that an UDP datagram can contain more than one diagnostic message.

Because the maximum length of an Ethernet frame payload is 1500 bytes, the maximum length of an UDP packet payload (encapsulated in an IPv4 packet) is 1476 bytes, and the maximum length of a DAP payload (= diagnostic message) is 1466 bytes.

6.2 Connection Handling

In the case of TCP there are the following definitions for the connection establishment and termination:

After start-up of the network and before the TCP transport of the first physically addressed diagnostic message from a sender device to a receiver device, a connection must be established.

Only this TCP connection must be used by these two devices to exchange physically addressed diagnostic messages (both, requests and responses).

This is possible, because a TCP connection is bidirectional.

Notes:

7 Appendix A: Index of Figures

8 Appendix B: Index of Tables