BS ISO 13400-2:2012

BSI Standards Publication

Road vehicles - Diagnostic communication over Internet Protocol (DoIP)

Part 2: Transport protocol and network layer services

raising standards worldwide™

National foreword

This British Standard is the UK implementation of ISO 13400-2:2012.

The UK participation in its preparation was entrusted to Technical Committee AUE/16, Electrical and electronic equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 69653 4

ICS 43.040.10; 43.180

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2012.

Amendments issued since publication

Date	Text affected

BS ISO 13400-2:2012

INTERNATIONAL STANDARD

ISO 13400-2

First edition
2012-06-01

Road vehicles — Diagnostic communication over Internet Protocol (DoIP) —

Part 2: Transport protocol and network layer services

Véhicules routiers — Communication de diagnostic au travers du protocole internet (DoIP) —

Partie 2: Protocole de transport et services de la couche réseau

Reference number
ISO 13400-2:2012(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 13400-2 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 13400 consists of the following parts, under the general title *Road vehicles — Diagnostic communication over Internet Protocol (DoIP)*:

— *Part 1: General information and use case definition*

— *Part 2: Transport protocol and network layer services*

— *Part 3: Wired vehicle interface based on IEEE 802.3*

The following parts are under preparation:

— *Part 4: Ethernet diagnostic connector*

— *Part 5: Conformance test specification*

Introduction

Vehicle diagnostic communication has been developed starting with the introduction of the first legislated emissions-related diagnostics and has evolved over the years, now covering various use cases ranging from emission-related diagnostics to vehicle-manufacturer-specific applications like calibration or electronic component software updates.

With the introduction of new in-vehicle network communication technologies, the interface between the vehicle's electronic control units and the external test equipment has been adapted several times to address the specific characteristics of each new network communication technology requiring optimized data link layer definitions and transport protocol developments in order to make the new in-vehicle networks usable for diagnostic communication.

With increasing memory size of electronic control units, the demand to update this increasing amount of software and an increasing number of functions provided by these control units, technology of the connecting network and buses has been driven to a level of complexity and speed similar to computer networks. New applications (x-by-wire, infotainment) require high band-width and real-time networks (like FlexRay, MOST), which cannot be adapted to provide the direct interface to a vehicle. This requires gateways to route and convert messages between the in-vehicle networks and the vehicle interface to external test equipment.

The intent of ISO 13400 (all parts) is to describe a standardized vehicle interface which

— separates in-vehicle network technology from the external test equipment vehicle interface requirements to allow for a long-term stable external vehicle communication interface,

— utilizes existing industry standards to define a long-term stable state-of-the-art communication standard usable for legislated diagnostic communication as well as for manufacturer-specific use cases, and

— can easily be adapted to new physical and data link layers, including wired and wireless connections, by using existing adaptation layers.

To achieve this, all parts of ISO 13400 are based on the Open Systems Interconnection (OSI) Basic Reference Model specified in ISO/IEC 7498-1 and ISO/IEC 10731, which structures communication systems into seven layers. When mapped on this model, the services specified by ISO 14229-1, ISO 14229-2 and ISO 14229-5 are divided into

a) unified diagnostic services (layer 7), specified in ISO 14229-1, ISO 14229-5, ISO 27145-3,

b) presentation (layer 6):

   1) for enhanced diagnostics, specified by the vehicle manufacturer,

   2) for WWH-OBD (World-Wide Harmonized On-Board Diagnostics), specified in ISO 27145-2, SAE J1930-DA, SAE J1939:2011, Appendix C (SPNs), SAE J1939-73:2010, Appendix A (FMI), SAE J1979-DA, SAE J2012-DA,

c) session layer services (layer 5), specified in ISO 14229-2,

d) transport protocol (layer 4), specified in this part of ISO 13400,

e) network layer (layer 3) services, specified in this part of ISO 13400, and

f) physical and data link services (layers 1 and 2), specified in ISO 13400-3,

in accordance with Table 1.

Table 1 — Enhanced and legislated WWH-OBD diagnostic specifications applicable to the OSI layers

Applicability	OSI 7 layers	Vehicle manufacturer enhanced diagnostics	WWH-OBD document reference
Seven layers according to ISO/IEC 7498-1 and ISO/IEC 10731	Application (layer 7)	ISO 14229-1/ISO 14229-5	ISO 14229-1/ISO 27145-3
	Presentation (layer 6)	Vehicle manufacturer specific	ISO 27145-2, SAE J1930-DA, SAE J1939:2011, Appendix C (SPNs), SAE J1939-73:2010, Appendix A (FMIs), SAE J1979-DA, SAE J2012-DA
	Session (layer 5)	ISO 14229-2	ISO 14229-2
	Transport (layer 4)	ISO 13400-2	ISO 13400-2
	Network (layer 3)		
	Data link (layer 2)	ISO 13400-3	ISO 13400-3
	Physical (layer 1)		

The application layer services covered by ISO 14229-5 have been defined in compliance with diagnostic services established in ISO 14229-1, but are not limited to use only with them.

The transport and network layer services covered by this part of ISO 13400 have been defined to be independent of the physical layer implemented.

For other application areas, ISO 13400-3 can be used with any Ethernet physical layer.

INTERNATIONAL STANDARD ISO 13400-2:2012(E)

Road vehicles — Diagnostic communication over Internet Protocol (DoIP) —

Part 2:
Transport protocol and network layer services

1 Scope

1.1 This part of ISO 13400 specifies the requirements for diagnostic communication between external test equipment and vehicle electronic components using Internet Protocol (IP) as well as the transmission control protocol (TCP) and user datagram protocol (UDP). This includes the definition of vehicle gateway requirements (e.g. for integration into an existing computer network) and test equipment requirements (e.g. to detect and establish communication with a vehicle).

1.2 This part of ISO 13400 specifies features that can be used to detect a vehicle in a network and enable communication with the vehicle gateway as well as with its sub-components during the various vehicle states. These features are separated into two types: mandatory and optional.

1.3 This part of ISO 13400 specifies the following mandatory features:

— vehicle network integration (IP address assignment);

— vehicle announcement and vehicle discovery;

— vehicle basic status information retrieval (e.g. diagnostic power mode);

— connection establishment (e.g. concurrent communication attempts), connection maintenance and vehicle gateway control;

— data routing to and from the vehicle's sub-components;

— error handling (e.g. physical network disconnect).

1.4 This part of ISO 13400 specifies the following optional features:

— DoIP entity status monitoring;

— DoIP entity firewall capabilities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3779, *Road vehicles — Vehicle identification number (VIN) — Content and structure*

ISO 13400-1, *Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 1: General information and use case definition*

ISO 13400-3, *Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 3: Wired vehicle interface based on IEEE 802.3*

IEEE 802.3, *IEEE Standard for Information Technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

IETF RFC 147, *The Definition of a Socket*

IETF RFC 768, *User Datagram Protocol*

IETF RFC 791 (September 1981), *Internet Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 792, *Internet Control Message Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 793, *Transmission Control Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 826, *An Ethernet Address Resolution Protocol*

IETF RFC 1122, *Requirements for Internet Hosts — Communication Layers*

IETF RFC 2131, *Dynamic Host Configuration Protocol*

IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) — Specification*

IETF RFC 2375, *IPv6 Multicast Address Assignments*

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

IETF RFC 3484, *Default Address Selection for Internet Protocol version 6 (IPv6)*

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local Addresses*

IETF RFC 4291, *IP Version 6 Addressing Architecture*

IETF RFC 4443, *Internet Control Message Protocol (ICMP v6) for the Internet Protocol Version 6 (IPv6) Specification*

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option*

IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13400-1 and the following apply.

3.1.1
diagnostic power mode
abstract vehicle internal power supply state which affects the diagnostic capabilities of all ECUs on the in-vehicle networks and which identifies the state of all ECUs of all gateway sub-networks that allow diagnostic communication

NOTE The intent is to provide information to the external test equipment about whether diagnostics can be performed on the connected vehicle or whether the vehicle needs to be put into a different diagnostic power mode (i.e. technician interaction required). In this part of ISO 13400, the following states are relevant: Not Ready (not all ECUs accessible via DoIP can communicate), Ready (all ECUs accessible via DoIP can communicate) and Not Supported (the Diagnostic Information Power Mode Information Request message is not supported).

3.1.2
DoIP edge node
host inside the vehicle, where an Ethernet activation line in accordance with ISO 13400-3 is terminated and where the link from the first node/host in the external network is terminated

NOTE Adapted from ISO 13400-3:2011, 3.1.2.

3.1.3
network node
component which is connected to the IP-based network (e.g. Ethernet) and which communicates using Internet Protocol but does not implement the DoIP protocol

NOTE 1 Ethernet is an example of an IP-based network.

NOTE 2 Some network nodes might also be connected to a vehicle sub-network, but they are not DoIP gateways as they don't implement the DoIP protocol. Consequently, these network nodes do not interact with (e.g. respond to) DoIP-compliant external test equipment.

3.1.4
host
node connected to the IP-based network

3.1.5
invalid source address
source address that is outside the range reserved for testers

3.1.6
logical address
means of identifying a diagnostics application layer entity

3.1.7
socket
unique identification, as defined in IETF RFC 147, to or from which information is transmitted in the network

3.1.8
unknown source address
source address that is not listed in the connection table entry

3.1.9
vehicle sub-network
vehicle network which is not directly connected to the IP-based network

NOTE Data can only be sent to and from a vehicle sub-network through the connecting DoIP gateway.

3.2 Symbols

<d> payload length, given in bytes

<m> number of concurrent DoIP TCP sessions that the external test equipment is required to support in order to connect to one or more DoIP entities

<n> number of concurrent DoIP TCP sessions that the DoIP entity needs to support in order to accept one up to n concurrent connections to one or more items of external test equipment

<u>, <v> number of individual ECUs in a vehicle sub-network

<w> number of individual DoIP gateways in a vehicle network

<x> number of individual in-vehicle network nodes

<y> number of individual vehicle DoIP nodes in a vehicle network

<z> number of individual vehicle external network nodes

3.3 Abbreviated terms

Alt	alternative
ARP	address resolution protocol
ASCII	American standard code for information interchange
Auto-MDI(X)	automatic medium-dependent interface crossover
CAN	controller area network
DHCP	dynamic host control protocol
DNS	domain name system
DoIP	diagnostic communication over Internet Protocol
ECU	electronic control unit
EID	entity identification (see Table 19)
FMI	failure mode indicator
GID	group identification (see Table 19)
GUI	graphical user interface
IANA	internet assigned numbers authority (see References [13] and [14])
ICMP	internet control message protocol
IETF RFC	Internet Engineering Task Force Request for Comments
IP	Internet Protocol
IPv4	Internet Protocol version 4 (see IETF RFC 791)
IPv6	Internet Protocol version 6 (see IETF RFC 2460)
MAC	media access control
MSC	message sequence chart
NDP	neighbour discovery protocol
OEM	original equipment manufacturer
OSI	Open Systems Interconnection
SA	source address
SDU	service data unit
SPN	suspect parameter number
TA	target address
TCP	transmission control protocol
UDP	user datagram protocol
VIN	vehicle identification number (see ISO 3779)
XOR	exclusive or

4 Conventions

ISO 13400 is based on the conventions discussed in the OSI Service Conventions (as specified in ISO/IEC 10731) as they apply to diagnostic services.

5 Document overview

All parts of ISO 13400 are applicable to vehicle diagnostic systems implemented on an IP communication network.

ISO 13400 has been established in order to define common requirements for vehicle diagnostic systems implemented on an IP communication link.

Although primarily intended for diagnostic systems, ISO 13400 has been developed to also meet requirements from other IP-based systems needing a transport protocol and network layer services.

Figure 1 illustrates the most applicable application implementations utilizing DoIP.

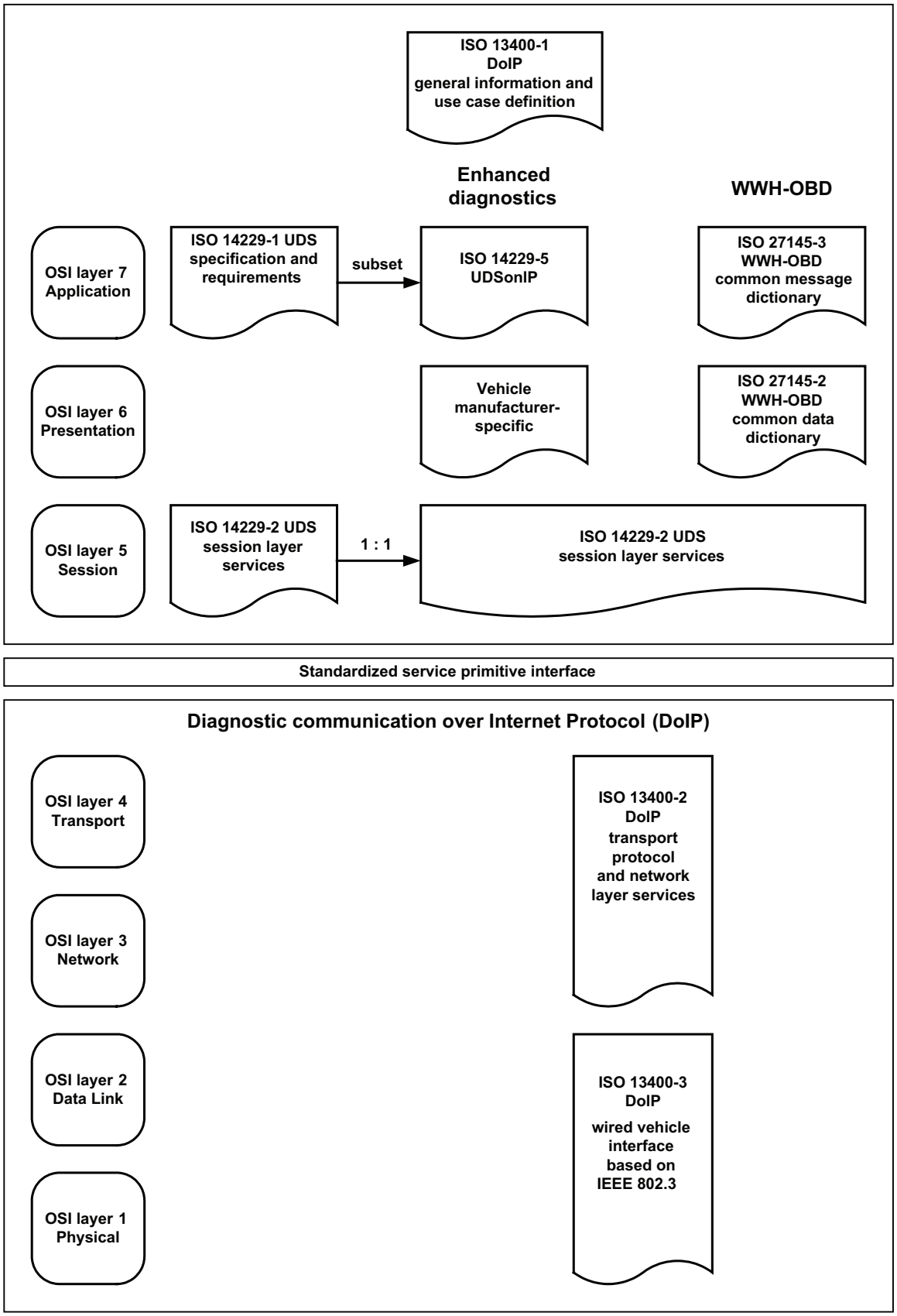


Figure 1 — DoIP document reference according to OSI model

6 Basic requirements for implementation of internet protocols

6.1 General considerations

Subclauses 6.2 to 6.5 specify the requirements that shall be implemented by a vehicle in order to allow for communication between the vehicle and external test equipment. Usually, this protocol standard is implemented by one or more DoIP entities, depending on the vehicle's network architecture. Figure 2 shows an example of the vehicle network architecture.

In this part of ISO 13400, the requirements are assigned a unique number of the form "DoIP-yyy", allowing for easier requirement tracking and test case specification in ISO 13400-5.

NOTE Requirements in this part of ISO 13400 are not numbered sequentially because the order of individual requirements changed during document development.

Requirements formulated as "The vehicle shall implement…" imply that all DoIP entities shall implement the required functionality if not explicitly stated otherwise. If multiple DoIP entities are present on a vehicle network, implementation details may differ slightly for each DoIP entity (e.g. for identification purposes), so that the external test equipment is able to identify the individual DoIP gateways that support this protocol standard.

Where reference is made to RFC documents, note that the forms "must/must not" are used to express requirements in these documents.

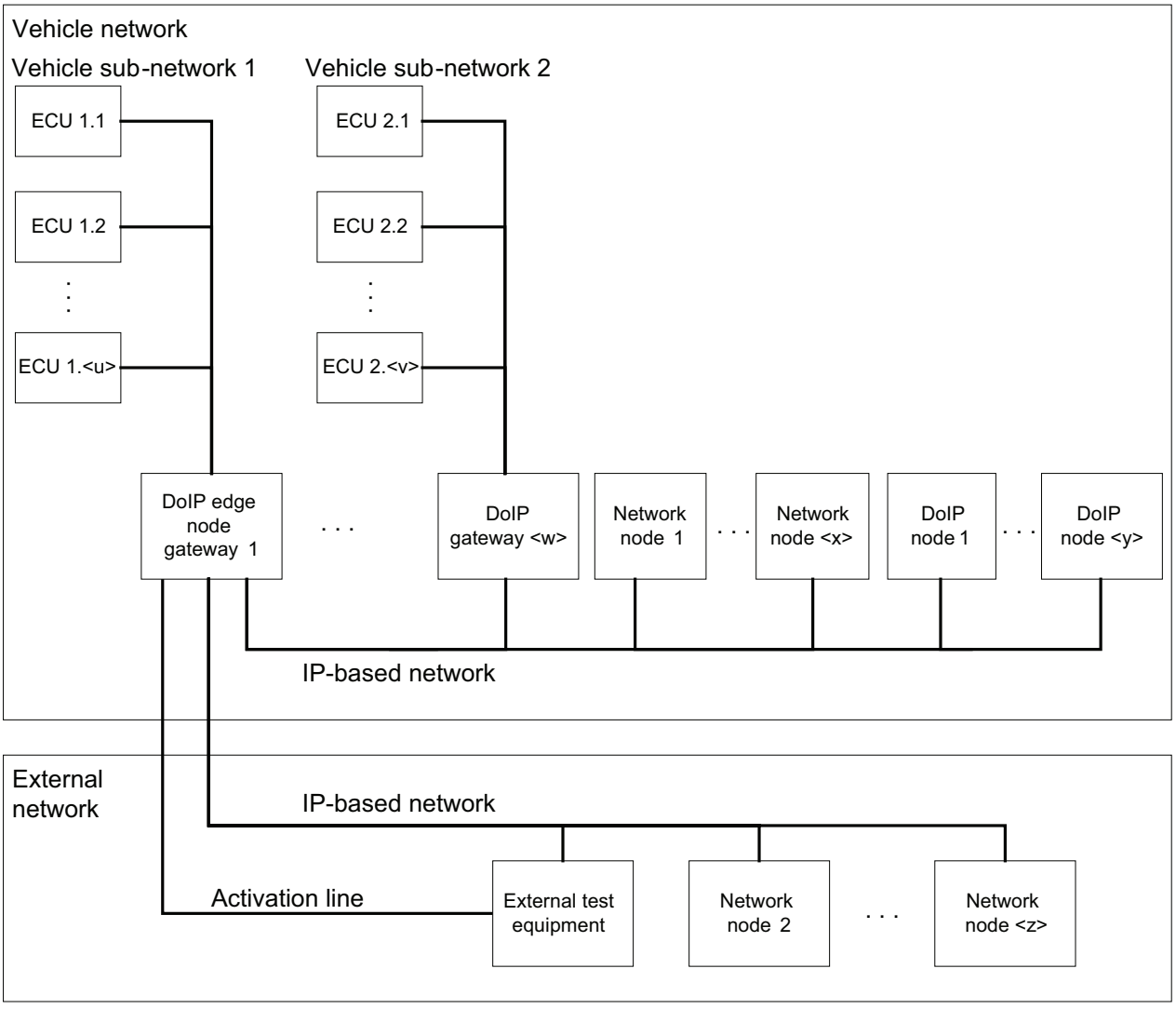


Figure 2 — Vehicle network architecture schematics (functional view)

[DoIP-108] Each DoIP entity on a vehicle network shall implement the protocol standard specified in this part of ISO 13400.

6.2 Network layer requirements

6.2.1 MAC-layer

[DoIP-146] MAC addresses shall be unique and in accordance with IEEE 802.3.

The MAC layer may limit the maximum transport unit (MTU). For IEEE 802.3 based systems, the limit is usually approximately 1 500 Bytes. In IEEE 802.3 based systems, there is no provision for fragmentation at this layer, so the upper layer (IP) will have to handle fragmentation (i.e. send a single data packet in multiple IP packets which fit into the MTU size of the Ethernet frames).

6.2.2 Internet Protocol (IP)

The protocol specified in this part of ISO 13400 is based on the Internet Protocol standards known as IPv4 (see IETF RFC 791) and IPv6 (see IETF RFC 2460). Although the mandatory features of this part of ISO 13400 are intended to be based on IPv6 only, use of IPv4 is specified for applications of this communication protocol in network areas where backward compatibility to IPv4 is required. The Internet Protocol is datagram based, unreliable and located on the network layer in accordance with the OSI layered architecture model (see Table 2). IP is the first transmission-medium-independent protocol.

The process of how a node acquires an IP address is described in 6.4.2.

Table 2 — IPv4/IPv6 on OSI layers

OSI layer	Protocol	
Network	IPv6 (IETF RFC 2460; preferred)	IPv4 (IETF RFC 791; for backward compatibility reasons only)
Data link / Physical	e.g. Ethernet (IEEE 802.3)	

[DoIP-109] All DoIP entities on a vehicle wireline network shall implement the same Internet Protocol version, either IPv4 in accordance with IETF RFC 791 or IPv6 in accordance with IETF RFC 2460.

It is recommended that IPv6 be used in order to benefit from the advantages (e.g. link local IP address assignment; faster forwarding through routers) of this protocol version. IPv4 may only be used for backward compatibility reasons (e.g. for integration into existing dealership IP networks). The support of Jumbograms for IPv6 is optional and consequently compliance with IETF RFCs related to Jumbograms is not required in this part of ISO 13400.

NOTE Interaction of the vehicle wireline DoIP entities with a future wireless IPv6 entity will form the subject of future International Standards.

In accordance with 6.2.1, the MAC layer is not responsible for fragmentation.

6.2.3 Address resolution protocol (IPv4) and neighbour discovery for IP version 6 (IPv6)

The address resolution protocol (ARP) and the neighbour discovery protocol (NDP) are methods for determining a host's hardware (MAC) address when only the host's IP address is known. They are also used to verify whether an IP address is in use by another host. ARP is located on the network layer, in accordance with the OSI layered architecture model (see Table 3).

Table 3 — ARP on OSI layers

OSI layer	Protocol
Network	IPv4: ARP (IETF RFC 826) IPv6: NDP (IETF RFC 4861)
Data link / Physical	e.g. Ethernet (IEEE 802.3)

[DoIP-110] If IPv4 is used, each DoIP entity shall implement ARP as defined in IETF RFC 826.

NOTE Usually, each host that implements IPv4 also implements ARP, as it is an essential part of IPv4 communication over Ethernet-based networks. Implementation of the reverse address resolution protocol (RARP) is not required as this requires a RARP server as part of the network, which is not mandatory in IPv4 networks.

[DoIP-111] If IPv6 is used, each DoIP entity shall implement NDP as defined in IETF RFC 4861.

6.2.4 Internet control message protocol (ICMP)

The internet control message protocol (ICMP) is part of the IP suite and is used to send error messages, e.g. to indicate that a requested service is not available or that a host could not be reached. Consequently, ICMP is a mandatory part of an IP stack implementation and is located on the network layer, in accordance with the OSI layered architecture model (see Table 4).

Table 4 — ICMP on OSI layers

OSI layer	Protocol
Network	IPv4: ICMP (IETF RFC 792) IPv6: ICMP v6 (IETF RFC 4443)
Data link / Physical	e.g. Ethernet (IEEE 802.3)

[DoIP-112] If IPv4 is used, each DoIP entity shall implement ICMP as specified in IETF RFC 792.

[DoIP-113] If IPv6 is used, each DoIP entity shall implement ICMPv6 as specified in IETF RFC 4443.

6.3 Transport Layer requirements

6.3.1 Transmission control protocol (TCP)

The transmission control protocol (TCP) is a connection-oriented protocol, where applications on networked hosts can establish connections to one another, over which data can be exchanged. The protocol guarantees reliable and in-order delivery of sender-to-receiver data. Additionally, TCP provides flow control and congestion control and also provides for various algorithms in order to handle congestion and influence flow control. This part of ISO 13400 does not specify the specific algorithm that should be used. TCP is located on the transport layer, in accordance with the OSI layered architecture model (see Table 5).

Table 5 — TCP on OSI layers

OSI layer	Protocol
Transport	TCP (IETF RFC 793)
Network	IP (IPv4, IPv6)
Data link / Physical	e.g. Ethernet (IEEE 802.3)

[DoIP-114] Each DoIP entity (IPv4 and IPv6) shall implement TCP as specified in IETF RFC 793.

[DoIP-115] Each DoIP entity shall implement the TCP-related requirements specified in IETF RFC 1122.

[DoIP-145] Each DoIP entity (IPv6 only) shall implement the TCP retransmission timer computation defined in IETF RFC 6298.

TCP uses a pair of port numbers (one sending, called remote port, and one receiving, called local port) to identify a connection. The sending port on one host will be the receiving port on the other and vice versa. The ports listed in Table 6 are the receiving ports on the DoIP entities that shall be used for TCP connections between external test equipment and DoIP entities.

Table 6 — Supported TCP ports

Name	Protocol	Port number	Description	Support condition
TCP_DATA	TCP (unicast)	13400 (see Reference [13] for further information)	DoIP routing messages from the external test equipment to the vehicle ECUs (e.g. diagnostic requests) and vice versa (e.g. diagnostic responses)	mandatory

[DoIP-001] Each DoIP entity shall listen to port TCP_DATA as specified in Table 6 in order to establish communication with external test equipment trying to connect on the TCP port.

[DoIP-002] Each DoIP entity shall support <n+1> TCP data sockets, where <n> is the number of concurrent TCP data connections supported by the respective DoIP entity.

[DoIP-003] The external test equipment shall be capable of supporting <m> TCP data connections (TCP data sockets). The local port (i.e. source port) will usually be chosen automatically during socket creation; the remote port is defined by the TCP_DATA port on the vehicle.

Figure 3 shows the TCP socket states.

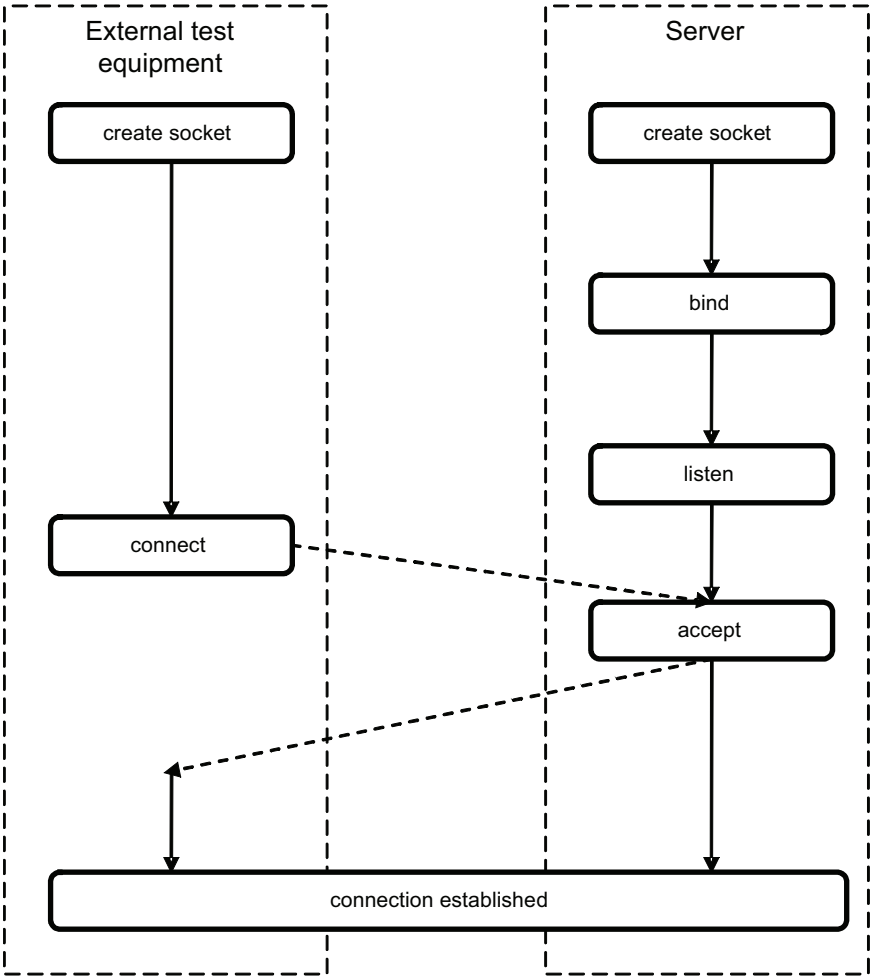


Figure 3 — TCP socket states

6.3.2 User datagram protocol (UDP)

The user datagram protocol (UDP) is a connectionless protocol. UDP does not provide the reliability and ordering guarantees that TCP does. Packets may arrive out of order or may be lost without notification of the sender or receiver. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes. UDP is located on the transport layer of the OSI layered architecture model (see Table 7).

Table 7 — UDP on OSI layers

OSI layer	Protocol
Transport	UDP (IETF RFC 768)
Network	IP (IPv4, IPv6)
Data link / Physical	e.g. Ethernet (IEEE 802.3)

[DoIP-006] Each DoIP entity shall implement UDP as specified in IETF RFC 768.

[DoIP-007] Each DoIP entity shall implement the UDP-related requirements in IETF RFC 1122.

UDP ports are used to identify the specific usage of UDP packets. The UDP ports specified in Table 8 are used for vehicle information services and control commands sent using UDP packets (e.g. when broadcasting requests to a local network).

Table 8 — UDP ports

Name	Protocol	Port number	Description	Support condition
UDP_DISCOVERY	UDP	13400 (see Reference [13] for further information)	Used for vehicle information requests and control commands from the external test equipment to the vehicle's DoIP entities. This port is used as the destination port in UDP packets sent by the external test equipment. Used for UDP packets sent by the DoIP entities without having received a request (e.g. Vehicle Announcement message). This port is used as the destination port in these UDP packets. The source port for these UDP packets may be UDP_DISCOVERY but can also be assigned dynamically.	mandatory
UDP_TEST_EQUIPMENT_REQUEST	UDP	dynamically assigned	This port is assigned dynamically by the external test equipment and used as the source port in UDP packets when transmitting messages (destination port set to UDP_DISCOVERY) to DoIP entities. This port will be used as the destination port in UDP packets sent by the DoIP entities as response to the corresponding message. The source port for these UDP packets may be set to UDP_DISCOVERY but can also be assigned dynamically.	mandatory

NOTE 1 Table 8 does not list the UDP ports which are needed to implement other standard protocols specified in this part of ISO 13400. Only the additional ports utilized by DoIP communication are specified.

[DoIP-008] Each DoIP entity shall listen to port UDP_DISCOVERY as specified in Table 8.

[DoIP-009] Each DoIP entity shall transmit UDP packets with the destination port set to UDP_DISCOVERY as specified in Table 8 in order to send unsolicited DoIP messages (e.g. Vehicle Announcement message).

[DoIP-010] The external test equipment shall listen to port UDP_DISCOVERY as specified in Table 8 in order to be able to receive unsolicited DoIP messages.

NOTE 2 As unsolicited messages will always be transmitted to the one listening port at the external test equipment (i.e. UDP_DISCOVERY), some kind of middleware might be required to distribute the gathered information (e.g. Vehicle Announcement) to all interested applications that can be reached by the same IP address. Alternatively, the local port can be used by multiple applications located on the external test equipment by using a reuse port option (e.g. SO_REUSEPORT) as long as only multicast messages are expected.

[DoIP-011] The external test equipment shall transmit UDP messages to the DoIP entity with the UDP destination port set to UDP_DISCOVERY.

[DoIP-135] The external test equipment shall transmit UDP messages to the DoIP entity with the UDP source port UDP_TEST_EQUIPMENT_REQUEST dynamically assigned within the dynamic port range (49 152…65 535).

[DoIP-136] The external test equipment shall listen to port UDP_TEST_EQUIPMENT_REQUEST specified in Table 8 for at least the time A_DoIP_Ctrl after the request has been transmitted in order to be able to receive responses to the previous UDP request messages. The port UDP_TEST_EQUIPMENT_REQUEST shall be in the listen state before sending a DoIP request message on this port to DoIP entities.

[DoIP-137] Each DoIP entity shall transmit UDP packets with the destination port set to UDP_TEST_EQUIPMENT_REQUEST as specified in Table 8 in order to respond to messages which were received through port UDP_DISCOVERY.

Depending on the implementation of the external test equipment, either the dynamically assigned UDP_TEST_EQUIPMENT_REQUEST port will be assigned once during or before the first transmission of a UDP packet to a DoIP entity or it can be dynamically re-assigned for each individual UDP request message and response. Also, depending on whether messages are sent repeatedly, response messages might arrive asynchronously and might no longer be associated with the specific corresponding request. In this case, it is up to the application of the external test equipment to ensure that it can handle these situations (e.g. keep transmitting vehicle identification request messages until the first vehicle identification response message arrives and then ignore the remaining arriving vehicle identification responses). In the case of multiple external test equipment instances behind one IP address, it is recommended that the different applications select different UDP_TEST_EQUIPMENT_REQUEST port numbers, in order to simplify mapping the response to the matching request message.

Figure 4 depicts the UDP port usage for unsolicited DoIP messages.

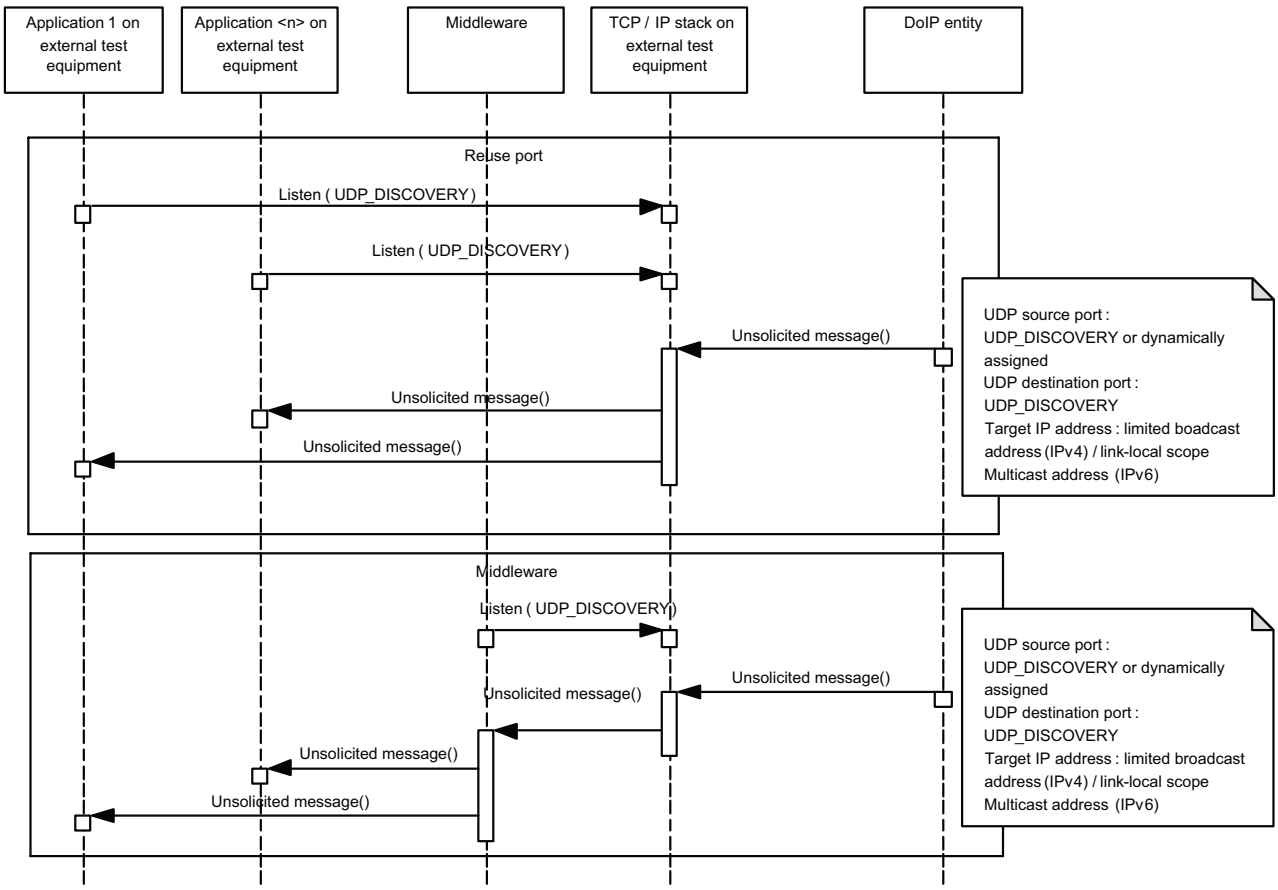


Figure 4 — UDP port usage for unsolicited DoIP messages

Figure 5 depicts the UDP port usage for DoIP request and response messages.

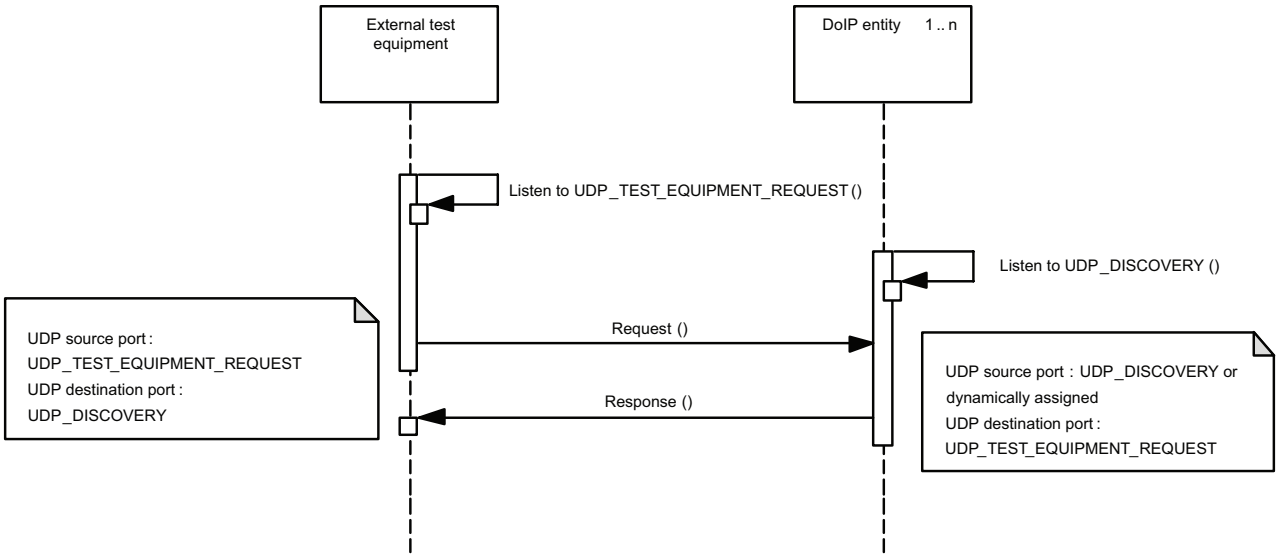


Figure 5 — UDP port usage for DoIP request and response messages

6.4 Application layer requirements — Dynamic host control protocol (DHCP)

6.4.1 General

The dynamic host configuration protocol is a client-server networking protocol that provides a mechanism for allocation of IP addresses using the UDP transport protocol. DHCP provides the mechanism for a client to acquire all of the IP configuration parameters that it needs in order to communicate successfully over the local network. DHCP is an application layer protocol in accordance with the OSI layered architecture model (see Table 9).

[DoIP-101] It shall be ensured that none of the DoIP entities provides DHCP server services on the link that is connected to the external test equipment, in order to avoid disturbing the external test equipment network (e.g. sending DHCP_OFFER messages and providing different IP gateway and DNS server addresses).

Table 9 — DHCP on OSI layers

OSI layer	Protocol
Application	IPv4: DHCP (IETF RFC 2131) IPv6: DHCPv6 (IETF RFC 3315)
Transport	UDP
Network	IP (IPv4, IPv6)
Data link / Physical	Ethernet (IEEE 802.3)

[DoIP-014] If IPv4 is used, each DoIP entity shall implement the DHCP client behaviour as specified in IETF RFC 2131.

[DoIP-015] If IPv6 is used, each DoIP entity shall implement the DHCPv6 client behaviour as specified in IETF RFC 3315.

NOTE 1 When supporting either DoIP-014 or DoIP-015, considering DoIP-109 is important.

[DoIP-016] Each DoIP entity shall implement either the “host name option” as defined in IETF RFC 2132, or the “fully qualified domain name” as defined in IETF RFC 4702

[DoIP-017] The host name option shall contain at minimum “`DoIP-<manufacturer_specific>`”, where the `<manufacturer_specific>` part can be replaced with any text that meets the specific requirements of the manufacturer.

NOTE 2 The host name option is used to allow for detection of a DoIP-compliant vehicle in a network which currently uses a DHCP-assigned IP address. An example of the implementation of requirement DoIP-017 is the host name option “`DoIP-VIN12345678901234567`” or simply “`DoIP-`” if the manufacturer-specific part is left empty.

[DoIP-138] Each DoIP entity shall start the IP address assignment process when the DoIP activation line is active as specified in ISO 13400-3.

NOTE 3 Additional mechanisms might be required for vehicle network architectures containing more than one DoIP entity, in order to ensure that all DoIP entities start assigning a valid IP address once the activation line is activated.

6.4.2 IP address assignment

6.4.2.1 General

Subclause 6.4.2 specifies how a DoIP entity acquires a valid IP address in order to communicate over an IP-based network. In general, the following parameters are needed for IP addressing:

— IP address (IPv4, IPv6);

— subnet mask (IPv4 only);

— prefix length (IPv6 only).

If the DoIP entity is integrated into a network infrastructure, the additional parameter default gateway address (= IP address of the default router) (IPv4, IPv6) is needed.

Based on the communication scenarios specified in ISO 13400-1, the network infrastructure provides dynamically assigned IP addresses or requires the DoIP entity to independently assign an IP address which does not conflict with the IP addresses of other nodes on the local network.

6.4.2.2 IPv4 address assignment

Depending on whether a DoIP entity is in an infrastructure environment or whether it operates in a direct peer to peer connection, IP addresses need to be assigned taking into consideration the specifics of IPv4. This subclause describes how an IP address can be configured in a minimum of time, to ensure fast connection establishment.

[DoIP-099] Each DoIP entity shall implement the dynamic configuration of IPv4 link-local addresses as specified in IETF RFC 3927.

To speed up the process of assigning an IP address on a direct peer-to-peer connection, it is recommended that the values listed in Table 10 be used by the DoIP entity when verifying the link-local IP address as specified in IETF RFC 3927. In the best case scenario, when using the values from Table 10, the DoIP entity will have an IP address configured in two seconds. For external test equipment using the performance values recommended by this part of ISO 13400 (listed in Table 10), in the best case scenario an IP address will be configured after seven seconds.

IMPORTANT — If the external test equipment is based on standard operating systems, the overall time to acquire an IP address depends on the configuration and the IP address assignment algorithms of these operation systems, and may range from several seconds up to minutes.

Table 10 defines the IETF RFC 3927 adapted timings.

Table 10 — IETF RFC 3927 adapted timings

Parameter	ISO 13400-2 recommended performance values	IETF RFC 3927 value	Description/rationale
PROBE_WAIT	1 s	1 s	Time before first probe message after link becomes active (initial delay)
PROBE_NUM	1 message	3 messages	Number of probe messages
PROBE_MIN	1 s	1 s	Minimum time between ARP probe messages
PROBE_MAX	1 s	2 s	Maximum time between ARP probe messages
ANNOUNCE_WAIT	1 s	2 s	Delay before announcing locally configured IP address
ANNOUNCE_NUM	1 message	2 messages	Number of announcement messages
ANNOUNCE_INTERVAL	1 s	2 s	Time between announcement messages

[DoIP-018] For improved IPv4 address-assignment performance, each DoIP entity shall perform the AutoIP-based and DHCP-assigned IP address assignment concurrently, as specified in Figure 6, when a data-link connection is detected (for the DoIP edge node) or when remotely invoked.

[DoIP-019] Each DoIP entity shall configure either an AutoIP-based IP address or a DHCP-based IP address, depending on which IP address assignment results in a valid IP address first.

[DoIP-020] DHCP-assigned IP addresses supersede AutoIP-assigned IP addresses, implying that the reception of a DHCP-assigned IP address will overwrite any previously configured link-local IP address (deviation from IETF RFC 3927).

[DoIP-021] Each DoIP entity shall use the first DHCP_OFFER message with an IP other than 0.0.0.0 to configure a DHCP-assigned IP address.

[DoIP-023] Each DoIP entity shall restart (DHCP_DISCOVER) the attempt to configure a DHCP-assigned IP address if no valid DHCP-configured IP address could be configured after a total of 10 s.

NOTE This requirement defines an overall timeout for triggering the re-start of the DHCP-based IP address assignment. The value chosen (10 s), differs from the recommended retransmission logic in the related RFC to allow for faster IP address assignment when using DHCP. This part of ISO 13400 does not specify the timing of the individual steps of the DHCP process. It is the vehicle manufacturer's responsibility to specify the timing and retry requirements needed to meet the overall time requirement in DoIP-023.

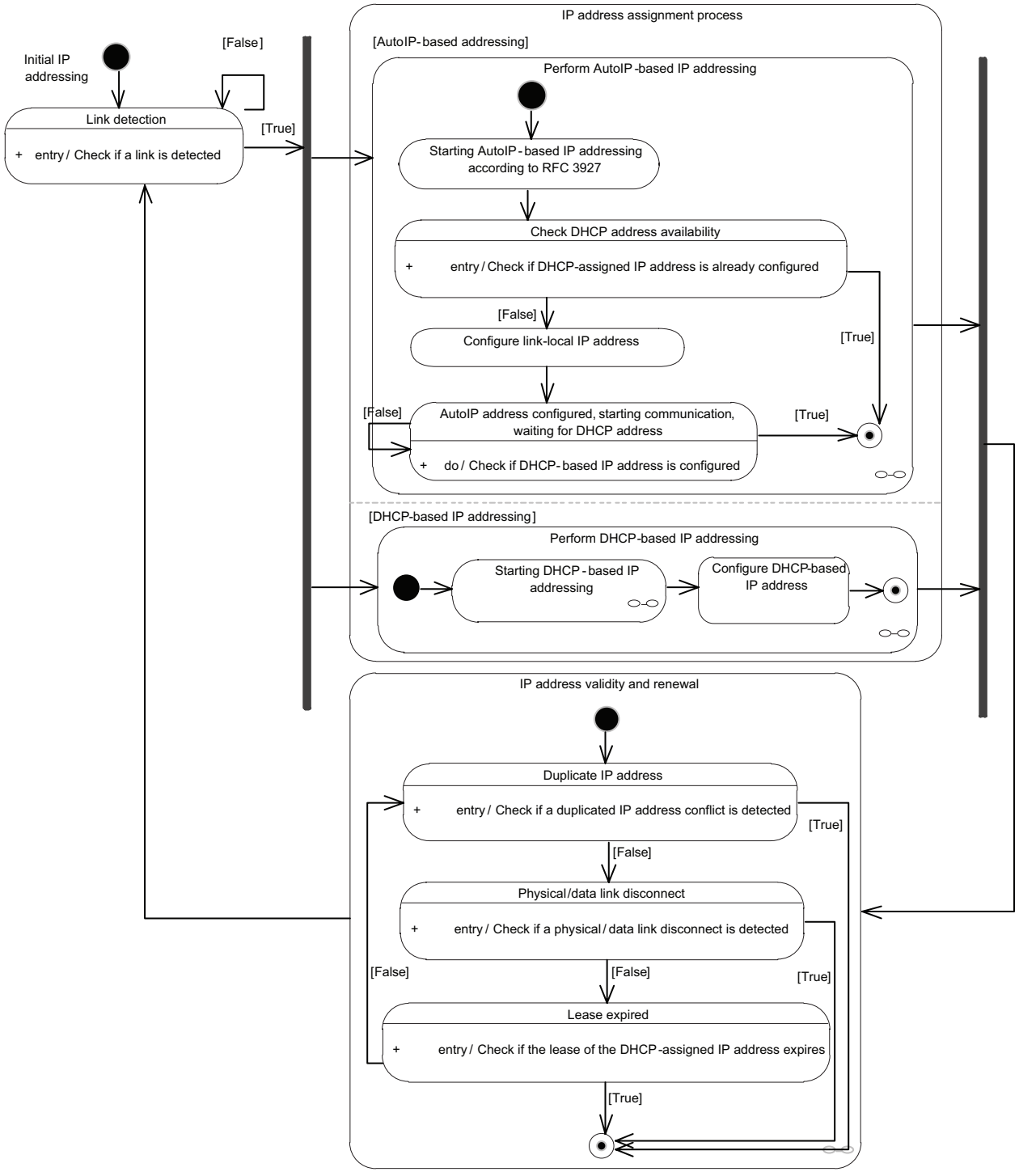


Figure 6 — Concurrent IPv4 AutoIP-based and DHCP-based IP address configuration

6.4.2.3 IPv6 address assignment

Due to the capabilities of the IPv6 protocol, the IP address assignment process differs slightly from the IPv4-based process. Specifically, the assignment of an IPv6 address for a direct peer-to-peer connection is considerably simpler and faster than the AutoIP-based address assignment of IPv4 as it uses the hardware address of the network interface.

NOTE An IPv6 host will usually have multiple IP addresses assigned to a physical network interface. The rules for prioritization of the different IPv6 addresses are specified in the referenced RFCs.

[DoIP-024] For IPv6, each DoIP entity shall support the configuration of a link-local IPv6 unicast address as specified in IETF RFC 4291.

[DoIP-025] The interface ID of the link-local address of a DoIP entity shall be generated from its IEEE 48 bit MAC identifier as defined in IETF RFC 4291.

[DoIP-139] If present in the network, an IPv6 address shall be derived from the router advertisement messages in accordance with IETF RFC 4862.

[DoIP-140] If present in the network, an IPv6 address shall be gathered from a DHCPv6 server.

[DoIP-141] IPv6 source address selection shall be performed in accordance with IETF RFC 3484.

6.4.3 IP address validity and renewal

This subclause specifies the requirements for when to discard a configured IP address and how to renew it. The IP address discarding and renewal process and criteria are depicted in Figure 6.

[DoIP-028] Each DoIP entity shall discard its IP address when any one of the following conditions occurs:

- the lease of the DHCP-assigned IP address expires, including DHCPNAK messages or a new DHCP-assigned IP address is received (for further details, see IETF RFC 2131 for IPv4 and IETF RFC 4291 for IPv6);
- the external test equipment disconnects (if the physical layer can detect this event) or the activation line is in the “deactivation criteria fulfilled” state;
- a duplicate IP address conflict is detected;
- the IP address is remotely invalidated (optional; vehicle-manufacturer-specific implementation).

[DoIP-029] Each DoIP entity shall attempt to configure a new IP address as specified in 6.4.2.2 for IPv4 or 6.4.2.3 for IPv6 if it has discarded its IP address due to one of the reasons in requirement DoIP-028.

If a DHCP-assigned IP address is available and the lease time hasn’t expired a DoIP node may verify and re-use (if the IP address is still available) its previously allocated IP address (see IETF RFC 2131). This applies to requirements [DoIP-028] and [DoIP-029].

[DoIP-030] Each DoIP entity shall close and reset all TCP sockets, including any authentications (e.g. routing activation) on these sockets, when the underlying IP stack discards or invalidates its current IP address.

6.5 Application layer requirements — Data transmission order

[DoIP-147] The big-endian network byte order of IP shall be used for DoIP messages in accordance with IETF RFC 791 (September 1981), Annex B.

7 DoIP protocol — Technical description

7.1 IP-based vehicle communication protocol

7.1.1 General information

The following general requirements apply to the handling of UDP packets and TCP data.

[DoIP-031] Any packets with a multi- or broadcast address as the source IP address shall be ignored.

[DoIP-122] Only one DoIP message shall be transmitted per UDP datagram.

The tables in 7.1.2 to 7.1.9 describe each message under the following column headings:

— Item:

This is a short name for the message element. This name will be used when the message element is referenced in this part of ISO 13400.

— Pos.:

This is the position (byte number) of each individual message element in a DoIP message. The byte position always starts with zero (0) and is counted from the beginning of the individual message element, i.e. it does not include any bytes of protocol overhead from lower layers.

— Len:

This is the length (number of bytes) of the respective message element.

— Description:

This column contains a more detailed description of each individual message element and its purpose.

— Values:

This column lists the supported value range and meaning of individual values of the respective message element.

— Support:

This column contains information on whether a specific message or message element shall be supported by a DoIP entity. Even if a message itself is defined as optional, it may contain mandatory elements that shall be implemented if the message itself is supported.

— Port and protocol:

This column specifies on which underlying protocol a specific payload type is supported and which port it uses.

7.1.2 Generic DoIP protocol message structure

This subclause specifies the generic structure of each DoIP message. This means that all messages which are sent or received over TCP_DATA or UDP_TEST_EQUIPMENT_REQUEST or UDP_DISCOVERY contain the generic header specified in Table 11. The Generic DoIP header will be processed and negatively acknowledged as depicted in Figure 7.

[DoIP-036] Each DoIP entity shall implement the generic DoIP header structure for all DoIP messages, as specified in Table 11. This part of the message is located at the beginning of each DoIP message.

[DoIP-156] Each DoIP entity shall support the protocol version default value for vehicle identification request messages as specified in Table 11. This means that a DoIP entity shall always ignore the protocol version default value in vehicle identification request messages.

EXAMPLE If external test equipment supports multiple protocol versions at the same time, and there is no information regarding the DoIP versions supported by the DoIP entities, this default value is used by the test equipment in the vehicle identification request messages.

NOTE 1 For UDP datagram-based messages, this implies that the generic header is located in the first bytes of the payload. For TCP-based data, the header separates the individual DoIP messages within the data stream.

The generic DoIP header uses four bytes to encode the payload size, limiting the number of bytes in the payload to 4 GB (4 294 967 295 bytes).

NOTE 2 The maximum allowed payload length will also be limited by the specific transport layer that is used in the vehicle (e.g. 4 kB for CAN).

Table 11 defines the generic DoIP header structure.

Table 12 provides an overview of the payload types that are specified for DoIP.

NOTE 3 For easier understanding, debugging and optimized implementations, DoIP payload types are grouped according to their message contents. Groups are Node Management (0x0XXX), Vehicle Information (0x4XXX) and Diagnostics (0x8XXX).

[DoIP-037] Each DoIP entity shall process the generic DoIP header structure for all DoIP messages in the order specified in Figure 7.

Table 11 — Generic DoIP header structure

Item	Pos.	Len.	Description	Values
Generic DoIP header synchronization pattern				
Protocol version	0	1	Identifies the protocol version of DoIP packets.	0x00: reserved 0x01: DoIP ISO/DIS 13400-2:2010 0x02: DoIP ISO 13400-2:2012 0x03…0xFE: reserved by this part of ISO 13400 0xFF: default value for vehicle identification request messages
Inverse protocol version	1	1	Contains the bit-wise inverse value of the protocol version, which is used in conjunction with the DoIP protocol version as a protocol verification pattern to ensure that a correctly formatted DoIP message is received.	Equals the <Protocol_Version> XOR 0xFF (e.g. 0xFE for protocol version 0x01).
Generic DoIP header payload type and payload length				
Payload type (GH_PT)	2	2	Contains information about how to interpret the data following the generic DoIP header (e.g. gateway command, diagnostic message, etc.)	See Table 12 for a complete list of currently specified payload type values.
Payload length (GH_PL)	4	4	Contains the length of the DoIP message payload in bytes (i.e. excluding the generic DoIP header bytes). Some payload types do not require any additional parameters (payload length is 0), some require a fixed DoIP message length while others allow for dynamic length DoIP messages.	0…4 294 967 295 bytes (= <d>)
Payload type specific message content	8	…	The payload type specific message content starts here. NOTE This implies that, for example, byte position 0 of the payload type-specific part of the message (see 7.1.1) means byte position 8 in the context of the overall DoIP message.	

Table 12 — Overview of DoIP payload types

Payload type value	Payload type name	Specified in subclause	Support (DoIP gateways)	Support (DoIP nodes)	Port and protocol
0x0000	Generic DoIP header negative acknowledge	7.1.2	mandatory	mandatory	UDP_DISCOVERY UDP_TEST_EQUIPMENT_REQUEST TCP_DATA
0x0001	Vehicle identification request message	7.1.4	mandatory	mandatory	UDP_DISCOVERY
0x0002	Vehicle identification request message with EID	7.1.4	optional	optional	UDP_DISCOVERY
0x0003	Vehicle identification request message with VIN	7.1.4	mandatory	mandatory	UDP_DISCOVERY
0x0004	Vehicle announcement message/vehicle identification response message	7.1.4	mandatory	mandatory	UDP_DISCOVERY UDP_TEST_EQUIPMENT_REQUEST
0x0005	Routing activation request	7.1.5	mandatory	mandatory	TCP_DATA
0x0006	Routing activation response	7.1.5	mandatory	mandatory	TCP_DATA
0x0007	Alive check request	7.1.7	mandatory	mandatory	TCP_DATA
0x0008	Alive check response	7.1.7	mandatory	mandatory	TCP_DATA
0x0009 to 0x4000	Reserved by this part of ISO 13400				
0x4001	DoIP entity status request	7.1.9	optional	optional	UDP_DISCOVERY
0x4002	DoIP entity status response	7.1.9	optional	optional	UDP_TEST_EQUIPMENT_REQUEST
0x4003	Diagnostic power mode information request	7.1.8	mandatory	mandatory	UDP_DISCOVERY
0x4004	Diagnostic power mode information response	7.1.8	mandatory	mandatory	UDP_TEST_EQUIPMENT_REQUEST
0x4005 to 0x8000	Reserved by this part of ISO 13400				
0x8001	Diagnostic message	7.1.6	mandatory	mandatory	TCP_DATA
0x8002	Diagnostic message positive acknowledgement	7.1.6	mandatory	mandatory	TCP_DATA
0x8003	Diagnostic message negative acknowledgement	7.1.6	mandatory	mandatory	TCP_DATA
0x8004 to 0xEFFF	Reserved by this part of ISO 13400				
0xF000 to 0xFFFF	Reserved for manufacturer-specific use	—	optional	optional	—

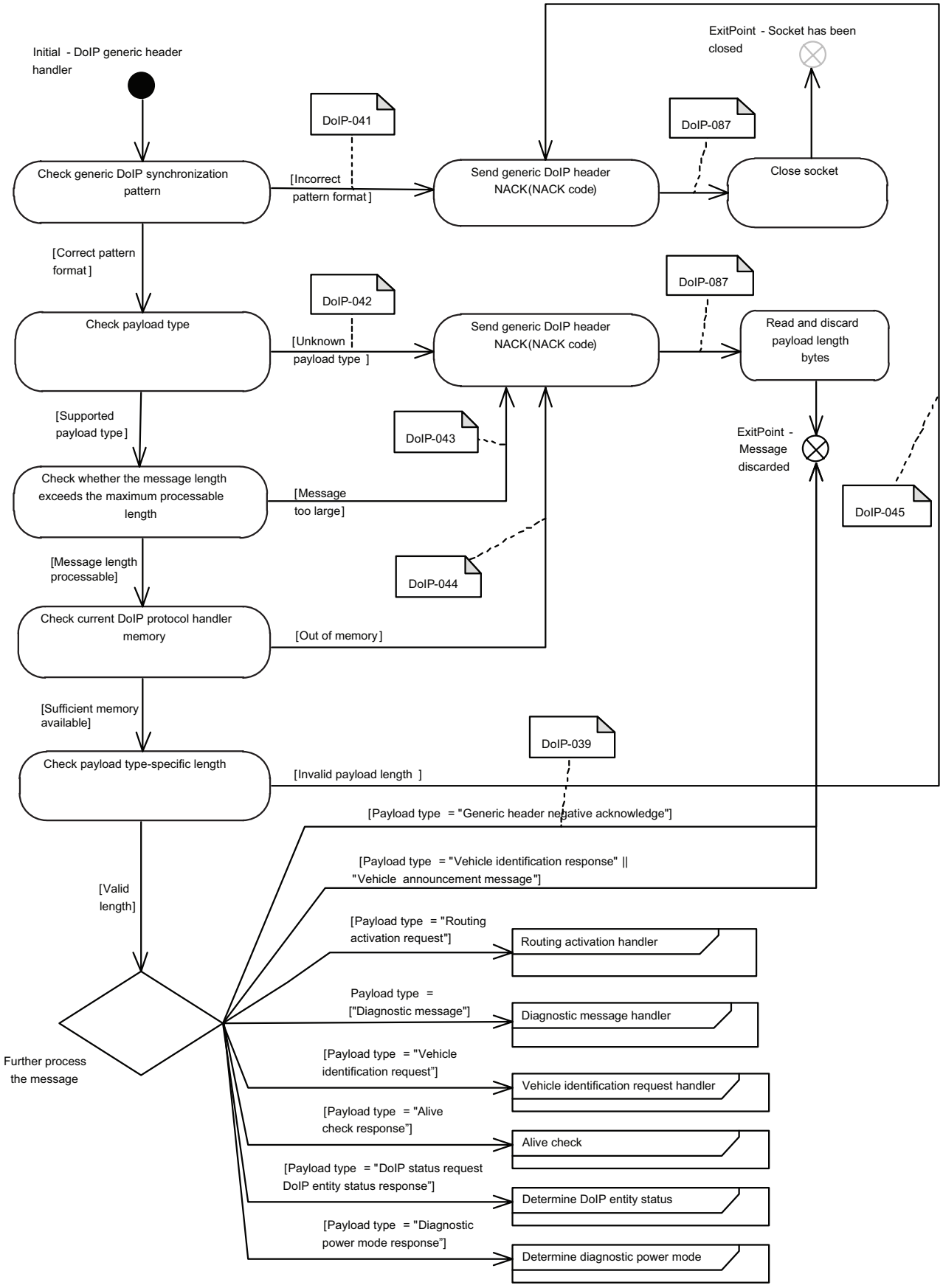


Figure 7 — DoIP generic header handler

As generic header negative acknowledge messages are also DoIP messages, they need to include the generic header part as specified in Table 11.

[DoIP-038] Each DoIP entity shall support the generic DoIP header negative acknowledge structure as specified in Table 13.

[DoIP-087] Each DoIP entity shall perform the required action specified in Table 14 after having sent the generic DoIP header negative acknowledge message.

[DoIP-039] Each DoIP entity shall ignore received generic DoIP header negative acknowledge messages.

[DoIP-040] The external test equipment shall not send generic DoIP header negative acknowledge messages upon receipt of an incorrect DoIP message from a DoIP entity. The generic DoIP header negative acknowledge message may only be used for determining the error condition for a previously sent DoIP message.

External test equipment may use DoIP header negative acknowledge messages during the development phase to verify correct implementation of DoIP messages in a DoIP entity. However, external test equipment in series production shall not send negative acknowledge messages, in order to prevent DoIP messages from bouncing back and forth between the external test equipment and the DoIP entities.

Table 13 defines the generic DoIP header negative acknowledge structure.

Table 13 — Generic DoIP header negative acknowledge structure

Item	Pos.	Len.	Description	Values
DoIP header NACK code				
Generic DoIP header NACK code	0	1	The generic header negative acknowledge code indicates the specific error that was detected in the generic DoIP header or it indicates an unsupported payload or a memory overload condition.	See Table 14.

Table 14 defines the generic DoIP header NACK codes.

Table 14 — Generic DoIP header NACK codes

Value	Description	Required action	Support
0x00	Incorrect pattern format	Close socket	mandatory
0x01	Unknown payload type	Discard DoIP message	mandatory
0x02	Message too large	Discard DoIP message	mandatory
0x03	Out of memory	Discard DoIP message	mandatory
0x04	Invalid payload length	Close socket	mandatory
0x05 to 0xFF	Reserved by this part of ISO 13400	—	—

[DoIP-041] Each DoIP entity shall send a generic DoIP header negative acknowledge message with NACK code set to 0x00 if the protocol version or inverse protocol version (synchronization pattern) does not match the format specified in Table 11.

[DoIP-042] Each DoIP entity shall send a generic DoIP header negative acknowledge message with NACK code set to 0x01 if the payload type is not supported by the DoIP entity.

[DoIP-043] Each DoIP entity shall send a generic DoIP header negative acknowledge message with NACK code set to 0x02 if the payload length exceeds the maximum DoIP message size supported by the DoIP entity regardless of the current memory utilization.

[DoIP-044] Each DoIP entity shall send a generic DoIP header negative acknowledge message with NACK code set to 0x03 if the payload length exceeds the currently available DoIP protocol handler memory of the DoIP entity.

[DoIP-045] Each DoIP entity shall send a generic DoIP header negative acknowledge message with NACK code set to 0x04 if the payload length parameter does not match the expected length for the specific payload type. This includes payload-type-specific minimum length, fixed length and maximum length checks.

7.1.3 Supported payload types over TCP and UDP ports

Table 15 provides an overview of all TCP ports and UDP ports defined in this part of ISO 13400 and their intended use.

Table 15 — UDP and TCP port usage

Use case	Payload type	Sender	Source port	Receiver	Destination port	Pro-tocol	Addressing
Vehicle discovery	Vehicle identification request	External test equipment	UDP_TEST_ EQUIPMENT_ REQUEST	DoIP entity	UDP_ DISCOVERY	UDP	Multi- or unicast
Vehicle discovery	Vehicle identification response	DoIP entity	UDP_ DISCOVERY or dynamically assigned	External test equipment	UDP_TEST_ EQUIPMENT_ REQUEST	UDP	Unicast
Vehicle discovery	Vehicle announcement	DoIP entity	UDP_ DISCOVERY or dynamically assigned	External test equipment	UDP_ DISCOVERY	UDP	Multicast
Data trans-mission	e.g. Routing activation request	External test equipment	Dynamically assigned	DoIP entity	TCP_DATA	TCP	Unicast
Data trans-mission	e.g. Routing activation response	DoIP entity	TCP_DATA	External test equipment	Dynamically assigned	TCP	Unicast

7.1.4 Vehicle identification request message and vehicle announcement

This subclause specifies the requirements to be implemented in order to identify a vehicle or its DoIP entities in a network. In order for the external test equipment to communicate meaningfully with a DoIP entity, it needs to know its IP address as well as in which vehicle it is installed. If the IP addresses are known by the external test equipment, the vehicle identification request can be used to retrieve the VIN/GID and DoIP entities logical addresses from a specific vehicle (see 9.4.1). Therefore, the following scenarios are supported:

— vehicle with VIN not yet configured (e.g. during assembly phase or after reprogramming);

— vehicle with VIN configured and VIN/EID/GID unknown to the external test equipment;

— vehicle with VIN configured and VIN/EID/GID known to the external test equipment;

— multiple DoIP entities installed on the same vehicle;

— IP addresses of DoIP entities known.

In the case that IP addresses are unknown and VINs are not yet configured, it is impossible to associate DoIP entities with a single vehicle based on the VIN. An alternative approach to this association problem is defined in 9.4.1.

Figure 24 in Clause 11 depicts the typical message sequence of DoIP entities announcing their presence or being identified using the specified requests and responses.

[DoIP-046] Each DoIP entity shall support the vehicle identification request message as specified in Table 16.

Table 16 — Payload type vehicle identification request message

Item	Pos.	Len.	Description	Values	Support condition
Payload type vehicle identification request message					
No message parameters					

[DoIP-047] If supported each DoIP entity shall implement the Vehicle Identification Request Message with additional EID parameter as specified in Table 17.

Table 17 — Payload type vehicle identification request message with EID

Item	Pos.	Len.	Description	Values	Support condition
Payload type vehicle identification request message with EID					
EID	0	6	This is the DoIP entity's unique ID (e.g. network interface's MAC address) that shall respond to the vehicle identification request message.	If MAC address is used, in accordance with IEEE EUI-48™	mandatory

[DoIP-048] Each DoIP entity shall support the vehicle identification request message with an additional VIN parameter as specified in Table 18.

Table 18 — Payload type vehicle identification request message with VIN

Item	Pos.	Len.	Description	Values	Support condition
Payload Type Vehicle Identification Request Message with VIN					
VIN	0	17	This is the vehicle's identification number as specified in ISO 3779. This parameter is only present if the external test equipment intends to identify the DoIP entities of an individual vehicle, the VIN of which is known to the external test equipment.	ASCII	mandatory

[DoIP-049] Each DoIP entity shall support the vehicle announcement/vehicle identification response message as specified in Table 19.

Table 19 — Payload type vehicle announcement/vehicle identification response message

Item	Pos.	Len.	Description	Values	Support condition
Vehicle Identification number					
VIN	0	17	This is the vehicle's vehicle identification number (VIN) as specified in ISO 3779. If the VIN is not configured at the time of transmission of this message, this should be indicated using the invalidity value specified in Table 40. In this case, the GID is used to associate DoIP nodes with a certain vehicle (see 9.4.1).	ASCII See Table 40	mandatory
DoIP entity logical address information					
Logical Address	17	2	This is the logical address that is assigned to the responding DoIP entity (see 7.4 for further details). The logical address can be used, for example, to address diagnostic requests directly to the DoIP entity.	See Table 39	mandatory
Entity identification					
EID	19	6	This is a unique identification of the DoIP entities in order to separate their responses even before the VIN is programmed to or recognized by the DoIP devices (e.g. during the vehicle assembly process). It is recommended that the MAC address information of the DoIP entity's network interface be used (one of the interfaces if multiple network interfaces are implemented).	If MAC address is used, in accordance with IEEE EUI-48™	mandatory
Group identification					
GID	25	6	This is a unique identification of a group of DoIP entities within the same vehicle in the case that a VIN is not configured for that vehicle. The VIN/GID synchronization process between DoIP nodes of a vehicle is defined in 9.4.1. If the GID is not available at the time of transmission of this message, this shall be indicated using the specific invalidity value as specified in Table 40.	See Table 40	mandatory
Further action required	31	1	This is the additional information to notify the external test equipment that there are either DoIP entities with no initial connectivity or that a centralized security approach is used.	See Table 20	mandatory
VIN/GID sync. status	32	1	This is the additional information to notify the external test equipment that all DoIP entities have synchronized their information about the VIN or GID of the vehicle.	See Table 21	optional

NOTE 1 The information that indicates whether further actions are required can be used to signal that certain in-vehicle synchronization procedures have not yet finished and/or additional steps are required (e.g. security measures) in order to allow all DoIP nodes to announce their presence on the network.

[DoIP-050] Each DoIP entity shall send the vehicle announcement message as specified in Table 19 A_DoIP_Announce_Num times with A_DoIP_Announce_Interval seconds inter-message time between each transmission starting immediately after configuration of a valid IP address.

NOTE 2 The reason for transmitting this message multiple times is to compensate for the fact that there is no guarantee that the message will be delivered correctly over the network, due to the use of UDP. Multiple transmissions increase the probability that at least one message will be received correctly by the external test equipment.

Table 20 defines the further action code values.

Table 20 — Definition of further action code values

Value	Description	Support
0x00	No further action required	mandatory
0x01 to 0x0F	Reserved by this part of ISO 13400	mandatory
0x10	Routing activation required to initiate central security.	optional
0x11 to 0xFF	Available for additional OEM-specific use.	optional

[DoIP-144] When a vehicle announcement/vehicle identification response message with a further action code of 0x10 (see Table 20: routing activation required) is received from a DoIP entity, the external test equipment may send a routing activation request message (see Table 22) with the activation type set to 0xE0 (see Table 23) to that DoIP entity and determine the specific action from the OEM-specific field in the routing activation response message (see Table 24).

Table 21 defines the VIN/GID sync. status code values.

Table 21 — Definition of VIN/GID sync. status code values

Value	Description	Support
0x00	VIN and/or GID are synchronized	mandatory
0x01…0x0F	Reserved by this part of ISO 13400	mandatory
0x10	Incomplete: VIN and GID are NOT synchronized.	mandatory
0x11…0xFF	Reserved by this part of ISO 13400	mandatory

[DoIP-125] In the case of a vehicle announcement (not the vehicle identification response), the UDP message shall always be sent with the target IPv4 address set to the limited broadcast address.

[DoIP-155] In the case of a vehicle announcement (not the vehicle identification response), the UDP message shall always be sent with the target IPv6 address set to the link-local scope multicast address (FF02::1) as described in IETF RFC 2375.

[DoIP-123] Each DoIP entity shall be uniquely identifiable by either the VIN, the EID or both at any time.

[DoIP-142] If it cannot be guaranteed that a vehicle can be identified by the VIN at any time, support for EID and GID shall be provided.

Figure 8 shows the generation of vehicle identification response messages, depending on the payload type of the vehicle identification request.

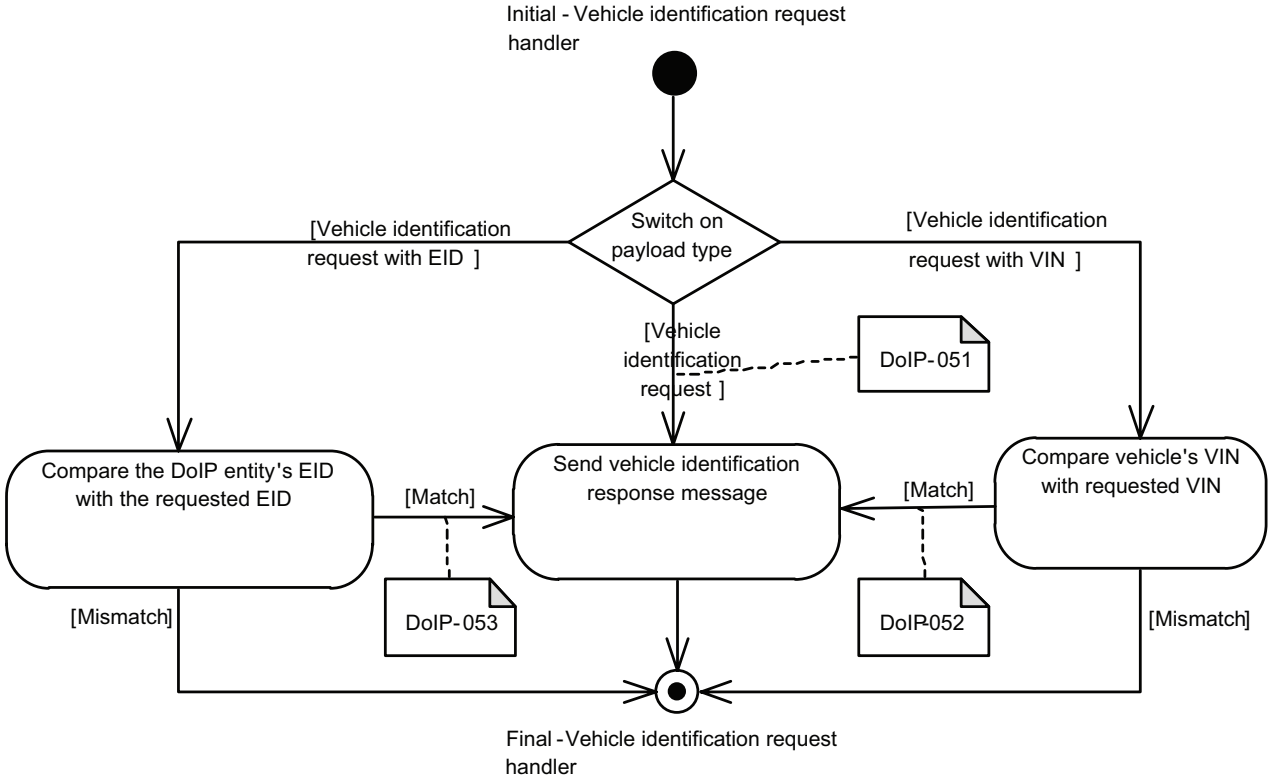


Figure 8 — Vehicle identification request handler

[DoIP-051] Each DoIP entity shall send a delayed (A_DoIP_Announce_Wait as specified in Table 38) vehicle identification response message as specified in Table 19 after receipt of a vehicle identification request message as specified in Table 16.

NOTE 3 The additional delay before responding to a vehicle identification request is necessary in order to avoid UDP packet bursts on the network if many DoIP entities are connected to the same network. In such a case, the random delay of the vehicle identification announcement response allows for UDP packets that were dropped due to high network utilization to reach the external test equipment on subsequent vehicle identification request broadcasts.

[DoIP-052] Each DoIP entity shall send the vehicle identification response message as specified in Table 19 after receipt of a vehicle identification request message with VIN (see Table 18), if the VIN from the request message matches the DoIP entity's programmed VIN.

[DoIP-053] Each DoIP entity shall send the vehicle identification response message as specified in Table 19 after receipt of a vehicle identification request message with EID (see Table 17), if the EID from the request message matches the DoIP entity's EID (e.g. one of the MAC addresses, if the DoIP entity implements multiple network interfaces).

7.1.5 Routing activation request and response

This subclause specifies the DoIP messages that are necessary to activate routing on a TCP_DATA socket. For deactivation of routing on a TCP_DATA socket, no additional payload types are defined as this can be achieved simply by closing the TCP_DATA socket. Figure 25 in Clause 11 shows an example sequence of external test equipment trying to activate routing on a newly established TCP_DATA socket.

[DoIP-057] Each DoIP entity shall support the routing activation request message as specified in Table 22.

Table 22 — Payload type routing activation request

Item	Pos.	Len.	Description	Values	Support condition
External test equipment address information					
Source address (SA)	0	2	Address of the external test equipment that requests routing activation. This is the same address that is used by the external test equipment when sending diagnostic messages on the same TCP_DATA socket.	See Table 39	mandatory
Activation type	2	1	Indicates the specific type of routing activation that may require different types of authentication and/or confirmation.	See Table 23	mandatory
Reserved and OEM specific data					
Reserved by this part of ISO 13400	3	4	Reserved for future standardization use.	Default 0x00000000	mandatory
Reserved for OEM-specific use	7	4	Available for additional OEM-specific use.	Defined by vehicle manufacturer/ not present	optional

[DoIP-100] Each DoIP entity shall process the routing activation request message as specified in Figure 9.

Table 23 defines the routing activation request activation types.

Table 23 — Routing activation request activation types

Value	Description	Required action	Support
0x00	Default	none	mandatory
0x01	WWH-OBD	none	mandatory
0x02 to 0xDF	ISO/SAE reserved		
0xE0	Central security	OEM-specific	optional
0xE1 to 0xFF	Available for additional OEM-specific use	OEM-specific	optional

Figure 9 depicts the DoIP routing activation handler.

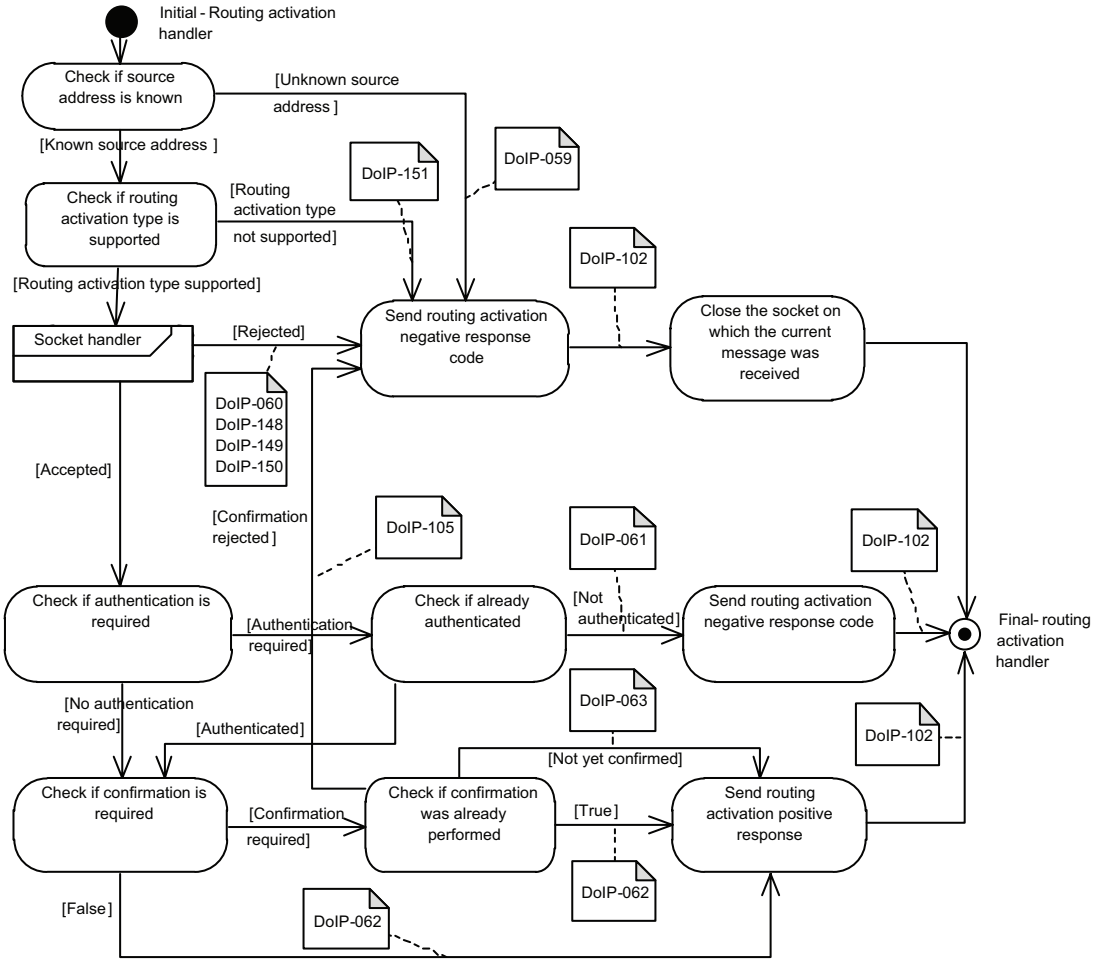


Figure 9 — DoIP routing activation handler

[DoIP-058] Each DoIP entity shall support the routing activation response message as specified in Table 24.

Table 24 — Payload type routing activation response

Item	Pos.	Len.	Description	Values	Support condition
External test equipment address information					
Logical address of external test equipment	0	2	Logical address of the external test equipment that requested routing activation.	See Table 39	mandatory
Routing activation status information					
Logical address of DoIP entity	2	2	Logical address of the responding DoIP entity.	See Table 39	mandatory
Routing activation response code	4	1	Response by the DoIP gateway. Routing activation denial will result in the TCP_DATA connection being reset by the DoIP gateway. Successful routing activation implies that diagnostic messages can now be routed over the TCP_DATA connection.	See Table 25	mandatory
Reserved by this part of ISO 13400	5	4	Reserved for future standardization use.	Default 0x00000000	mandatory
Reserved for OEM-specific use	9	4	Available for additional OEM-specific use.	—	optional

[DoIP-102] Each DoIP entity shall perform the required action as specified in Table 25 after having sent the corresponding routing activation response.

Table 25 — Routing activation response code values

Value	Description	Required action	Support
0x00	Routing activation denied due to unknown source address.	Do not activate routing and close this TCP_DATA socket.	mandatory
0x01	Routing activation denied because all concurrently supported TCP_DATA sockets are registered and active.	Do not activate routing and close this TCP_DATA socket.	mandatory
0x02	Routing activation denied because an SA different from the table connection entry was received on the already activated TCP_DATA socket.	Do not activate routing and close this TCP_DATA socket.	mandatory
0x03	Routing activation denied because the SA is already registered and active on a different TCP_DATA socket.	Do not activate routing and close this TCP_DATA socket.	mandatory
0x04	Routing activation denied due to missing authentication.	Do not activate routing and register.	optional
0x05	Routing activation denied due to rejected confirmation.	Do not activate routing and close this TCP_DATA socket.	optional
0x06	Routing activation denied due to unsupported routing activation type.	Do not activate routing and close this TCP_DATA socket.	mandatory
0x07 – 0x0F	Reserved by this part of ISO 13400.	—	—
0x10	Routing successfully activated.	Activate routing and register SA on this TCP_DATA socket.	mandatory
0x11	Routing will be activated; confirmation required.	Only activate routing after confirmation from within the vehicle.	optional
0x12 – 0xDF	Reserved by this part of ISO 13400.	—	—
0xE0 – 0xFE	Vehicle-manufacturer specific.	—	optional
0xFF	Reserved by this part of ISO 13400.	—	—

[DoIP-059] Each DoIP entity shall send the routing activation response message with the response code set to 0x00 after having received a routing activation request message if the source address in the request message is unknown.

[DoIP-060] Each DoIP entity shall send the routing activation response message with the response code set to 0x01 after having received a routing activation request message if the TCP_DATA socket is unavailable according to the socket handler requirements in 7.2.4.

[DoIP-149] Each DoIP entity shall send the routing activation response message with the response code set to 0x02 after having received a routing activation request message if the SA differs from the table connection entry that was received on the already activated TCP_DATA socket.

[DoIP-150] Each DoIP entity shall send the routing activation response message with the response code set to 0x03 after having received a routing activation request message if SA is already registered and active on a different TCP_DATA socket.

NOTE 1 It is up to the vehicle manufacturer's discretion how many concurrent source addresses are supported. This depends on how many concurrent TCP_DATA sockets are allowed with a DoIP entity. The maximum number of concurrent TCP_DATA sockets allowed with a DoIP entity can be retrieved by the DoIP entity status request specified in 7.1.9.

[DoIP-061] If supported, each DoIP entity shall send the routing activation response message with the response code set to 0x04 after having received a routing activation request message if additional authentication is required prior to the routing activation request.

[DoIP-105] If supported, each DoIP entity shall send the routing activation response message with the response code set to 0x05 after having received a routing activation request message that requires confirmation from within the vehicle but the confirmation was meanwhile rejected.

[DoIP-151] Each DoIP entity shall send the routing activation response message with the response code set to 0x06 after having received a routing activation request message with a routing activation type that is not supported by the DoIP entity.

[DoIP-062] Each DoIP entity shall send the routing activation response message with the response code set to 0x10 after having received a routing activation request message if all of the following conditions are met:

— logical source address from the routing activation request message is known to the DoIP entity;

— TCP_DATA socket is available according to the socket handler requirements in 7.2.4;

— no additional authentication steps are required;

— no confirmation from within the vehicle is required.

[DoIP-063] If supported, each DoIP entity shall send the routing activation response message with the response code set to 0x11 after having received a routing activation request message if all of the following conditions are met:

— logical source address from the routing activation request message is known to the DoIP entity;

— TCP_DATA socket is available according to the socket handler requirements in 7.2.4;

— no additional authentication steps are required;

— additional confirmation from within the vehicle is required (e.g. via confirming an information message in the instrument cluster display).

NOTE 2 This implies that once the additional confirmation from within the vehicle has been performed, this response code will not be sent anymore and the DoIP entity will activate routing as requested. Thus external test equipment can periodically send the routing activation request message to determine whether confirmation has been successfully completed.

7.1.6 Diagnostic message and diagnostic message acknowledgement

This subclause specifies the message format that allows for routing of diagnostic messages (i.e. diagnostic requests) onto the vehicle networks and from the vehicle networks (i.e. diagnostic responses) back to the external test equipment. If the diagnostic message is sent by the external test equipment, DoIP entities will always acknowledge (positively or negatively) these messages. Diagnostic messages can also be sent by the DoIP entities, for example when transmitting a diagnostic response or an unsolicited message (e.g. response on event) from an ECU to the external test equipment. In this case, the diagnostic messages will not be acknowledged by the external test equipment.

[DoIP-064] Each DoIP entity shall support the diagnostic message structure as specified in Table 26 for incoming (i.e. requests) and outgoing (i.e. responses) diagnostic messages.

Table 26 — Payload type diagnostic message structure

Item	Pos.	Len.	Description	Values	Support condition
Logical address information					
Source address (SA)	0	2	Contains the logical address of the sender of a diagnostic message (e.g. the external test equipment address).	See Table 39	mandatory
Target address (TA)	2	2	Contains the logical address of the receiver of a diagnostic message (e.g. a specific ECU on the vehicle's networks).	See Table 39	mandatory
Diagnostic message data					
User data (UD)	4	d-4	Contains the actual diagnostic data (e.g. a ISO 14229-1 diagnostic request) which shall be routed to the destination (e.g. the ECM).	See Table 27 for an example	mandatory

[DoIP-065] Each DoIP entity shall receive and process diagnostic messages on its TCP_DATA sockets in the order specified in Figure 10.

Table 27 gives an example of how an ISO 27145-3 diagnostic message is transported by a DoIP diagnostic message frame.

Table 27 — Example of ISO 27145-3 request message transported by a DoIP message frame

Message direction:	client → vehicle		
Message type:	Functionally addressed request message (read protocol identification InfoType identifier)		
Data byte	**Description**	**Byte value**	**Mnemonic**
0	ISO 13400 – protocol version	0x01	—
1	ISO 13400 – inverse protocol version	0xFE	—
2	ISO 13400 – payload type	0x8001	GH_PT
3	ISO 13400 – payload type		GH_PT
4	ISO 13400 – payload length	7	GH_PL
5	ISO 13400 – payload length		GH_PL
6	ISO 13400 – payload length		GH_PL
7	ISO 13400 – payload length		GH_PL
8	ISO 13400 – source address	e.g. 0x0E00	SA
9	ISO 13400 – source address		SA
10	ISO 13400 – target address	0xE000	TA
11	ISO 13400 – target address		TA
12	ISO 13400 – user data / ISO 27145-3 – ReadDataByIdentifier request SID	0x22	UD / RDBI
13	ISO 13400 – user data / ISO 27145-3 – DataIdentifier #1 (HB) = ITID = protocol identification	0xF8	UD / DID_HB
14	ISO 13400 – user data / ISO 27145-3 – DataIdentifier #1 (LB) = ITID = protocol identification	0x10	UD / DID_LB

Figure 10 depicts the DoIP diagnostic message handler.

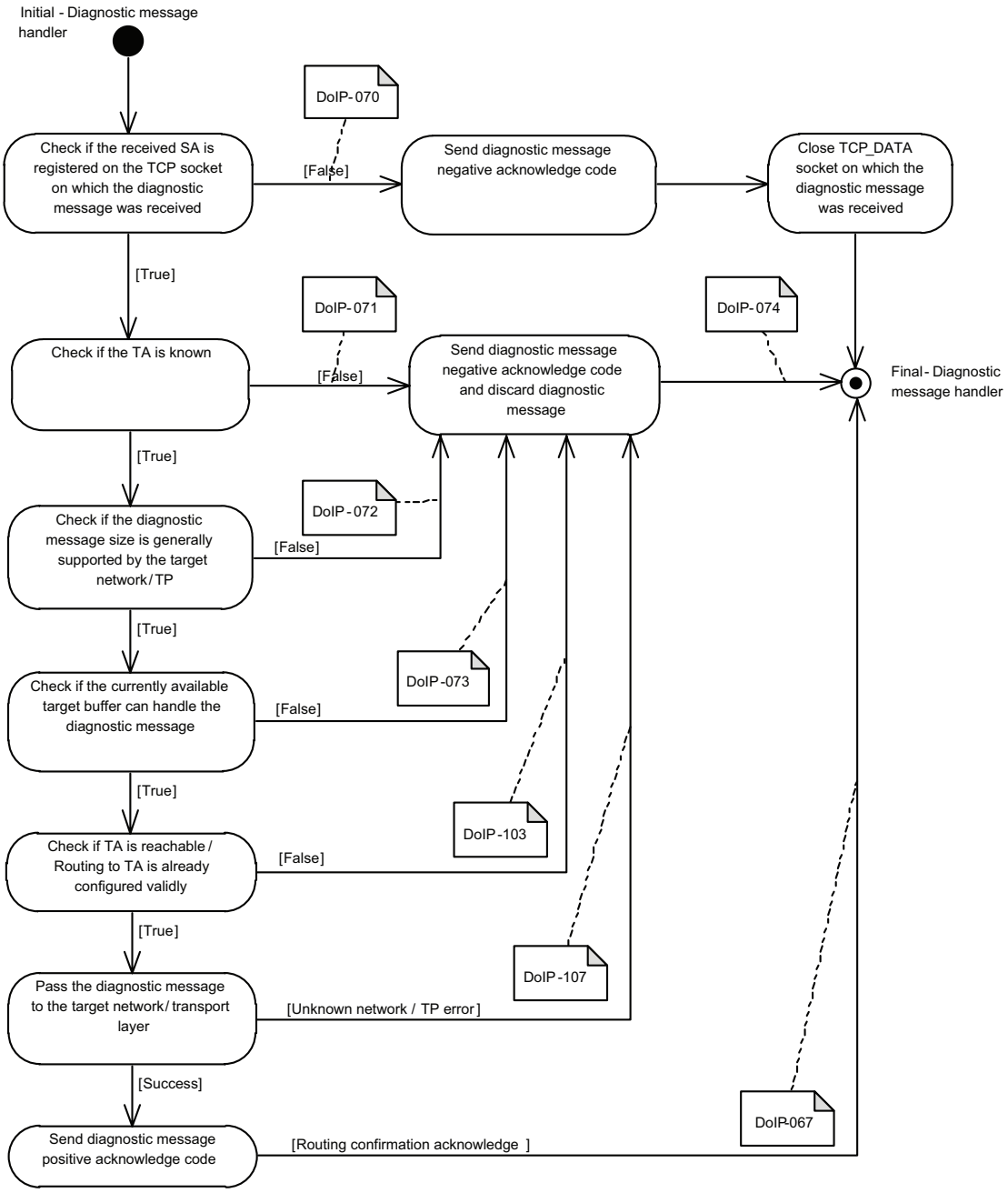


Figure 10 — DoIP diagnostic message handler

[DoIP-066] Each DoIP entity shall support the diagnostic message positive acknowledgement as specified in Table 28.

Table 28 — Payload type diagnostic message positive acknowledgment structure

Item	Pos.	Len.	Description	Values	Support
Logical address information					
Source address (SA)	0	2	Contains the logical address of the (intended) receiver of the previous diagnostic message (e.g. a specific ECU on the vehicle's networks).	See Table 39	mandatory
Target address (TA)	2	2	Contains the logical address of the sender of the previous diagnostic message (i.e. the external test equipment address).	See Table 39	mandatory
Diagnostic message acknowledge information					
ACK code	4	1	Contains the diagnostic message positive acknowledge code.	See Table 29	mandatory
Previous diagnostic message data	5	0 to <d-5>	May contain a copy of up to <d-5> bytes of the diagnostic message (max. size <d-4>) that is currently acknowledged. This may aid in troubleshooting communication problems.		optional

Table 29 — Diagnostic message positive acknowledge codes

Value	Description	Support
0x00	Routing confirmation acknowledge (ACK) message indicating that the diagnostic message was correctly received, processed and put into the transmission buffer of the destination network.	mandatory
0x01…0xFF	Reserved by this part of ISO 13400.	—

[DoIP-067] Each DoIP entity shall send the diagnostic message positive acknowledgement with ACK code set to 0x00 (see Table 29) immediately after the diagnostic message has been correctly processed and copied into the destination network transmission buffer.

[DoIP-068] Each DoIP entity shall support the diagnostic message negative acknowledgement as specified in Table 30.

Table 30 — Payload type diagnostic message negative acknowledgment structure

Item	Pos.	Len.	Description	Values	Support
Logical address information					
Source address (SA)	0	2	Contains the logical address of the (intended) receiver of the previous diagnostic message (e.g. a specific ECU on the vehicle's networks).	See Table 39	mandatory
Target address (TA)	2	2	Contains the logical address of the sender of the previous diagnostic message (i.e. the external test equipment address).	See Table 39	mandatory
Diagnostic message acknowledge information					
NACK code	4	1	Contains the diagnostic message negative acknowledge code.	See Table 31	mandatory
Previous diagnostic message data	5	0 to <d-5>	May contain a copy of up to <d-5> bytes (only limited by the maximum supported DoIP message size) of the diagnostic message that is currently acknowledged. This may aid in troubleshooting communication problems and is up to the manufacturer to select a feasible number of bytes to repeat.	HEX	optional

[DoIP-070] Each DoIP entity shall send the diagnostic message negative acknowledgement with NACK code set to 0x02 (see Table 31) and close the TCP_DATA socket when the diagnostic message contains a source address which is not activated on the TCP_DATA socket on which the diagnostic message is received.

[DoIP-071] Each DoIP entity shall send the diagnostic message negative acknowledgement with NACK code set to 0x03 (see Table 31) when the diagnostic message contains an unknown target address (e.g. ECU not connected to the addressed DoIP gateway).

[DoIP-072] Each DoIP entity shall send the diagnostic message negative acknowledgement with NACK code set to 0x04 (see Table 31) when the diagnostic message exceeds the maximum supported length of the transport protocol of the target network or target ECU (e.g. messages larger than 4095 bytes on CAN or when an ECU-specific message size limit is exceeded).

NOTE 1 This implies that a NACK is also sent if a functionally addressed DoIP message has to be routed to different subnetworks (e.g. TA is set to WWH-OBD functional group address 0xE000) and one or more subnetworks do not support the diagnostic message payload length.

EXAMPLE If a functionally addressed DoIP message shall be routed to several subnetworks including a CAN subnetwork and the DoIP diagnostic message payload size exceeds 7 bytes, the limitation for functionally addressed requests on CAN applies (only single frames). The DoIP GW sends a NACK with NACK code = 0x04 and discards the DoIP diagnostic request message.

[DoIP-073] Each DoIP entity shall send the diagnostic message negative acknowledgement with NACK code set to 0x05 (see Table 31) when the diagnostic message is too large to be copied into the destination buffer (e.g. the transport protocol refuses the request to provide the necessary buffer).

NOTE 2 This can be a temporary problem if a DoIP gateway uses dynamic buffer allocation.

Table 31 — Diagnostic message negative acknowledge codes

Value	Description	Support
0x00…0x01	Reserved by this part of ISO 13400	—
0x02	Invalid source address	mandatory
0x03	Unknown target address	mandatory
0x04	Diagnostic message too large	mandatory
0x05	Out of memory	mandatory
0x06	Target unreachable	optional
0x07	Unknown network	optional
0x08	Transport protocol error	optional
0x09…0xFF	Reserved by this part of ISO 13400	—

[DoIP-103] If supported, each DoIP entity shall send the diagnostic message negative acknowledgement with NACK code set to 0x06 (see Table 31) when the target address points to a device that can currently not be reached.

NOTE 3 This can be due to an unavailable destination network (e.g. temporary network reorganization or physical fault).

[DoIP-107] If supported and if an unknown target network or transport protocol error occurs that is not covered by the previous NACK codes, the DoIP entity shall send the diagnostic message negative acknowledgement with NACK code set to 0x07 or 0x08 (see Table 31).

[DoIP-074] Each DoIP entity shall discard the received diagnostic message if any of the aforementioned diagnostic message negative acknowledgement conditions (requirement DoIP-071 to DoIP-073, DoIP-103, DoIP-107) applies.

7.1.7 Alive check request and alive check response

This subclause specifies the message structures of the DoIP messages that are used to determine whether an open TCP_DATA socket is still in use by external test equipment. The alive check messages are utilized by the TCP_DATA socket handler (see 7.2.4). Figure 25 in Clause 11 shows an example sequence of external test equipment triggering alive check messages while trying to establish a new TCP_DATA socket.

[DoIP-075] Each DoIP entity shall support the alive check request as specified in Table 32.

Table 32 — Payload type alive check request structure

Item	Pos.	Len.	Description	Values	Support
Alive check request message					
No additional message element.					

[DoIP-076] Each DoIP entity shall send an alive check request according to the requirements in 7.2.4.

[DoIP-077] Each DoIP entity shall support the alive check response as specified in Table 33.

Table 33 — Payload type alive check response structure

Item	Pos.	Len.	Description	Values	Support
External test equipment logical address information					
Source address (SA)	0	2	Contains the logical address of the external test equipment that is currently active on this TCP_DATA socket.	See Table 39	mandatory

[DoIP-078] Each DoIP entity shall receive and process alive check response messages according to the requirements in 7.2.4.

NOTE The alive check response message can also be used by the external test equipment to keep a currently idle connection alive, i.e. it can be sent by the external test equipment even if it has not previously received an alive check request from a DoIP entity.

7.1.8 Diagnostic power mode information request and response

This payload type serves the purpose of retrieving the diagnostic power mode of a vehicle. This information may be used by external test equipment, for example, to verify whether the vehicle is in diagnostic power mode, which allows reliable diagnostics to be performed on the vehicle's components.

[DoIP-116] Each DoIP entity shall support the diagnostic power mode information request as specified in Table 34.

Table 34 — Diagnostic power mode information request

Item	Pos.	Len.	Description	Values	Support
Diagnostic power mode information request					
No additional message element.					

[DoIP-117] Each DoIP entity shall support the diagnostic power mode information response as specified in Table 35.

[DoIP-118] A DoIP entity shall respond with a diagnostic power mode information response within A_DoIP_Ctrl (see Table 38) after having received a previous diagnostic power mode information request.

Table 35 — Diagnostic power mode information response

Item	Pos.	Len.	Description	Values	Support
Diagnostic Power Mode					
Diagnostic power mode	0	1	Identifies whether or not the vehicle is in diagnostic power mode and ready to perform reliable diagnostics.	0x00: not ready 0x01: ready 0x02: not supported 0x03…0xFF: reserved by this part of ISO 13400	mandatory

7.1.9 DoIP entity status information request and response

This payload type serves the purpose of identifying certain operating conditions of the responding DoIP entity. This allows, for example, external test equipment to detect existing diagnostic communication sessions as well as the capabilities of a DoIP entity.

[DoIP-119] If supported, a DoIP entity shall implement the DoIP entity status request as specified in Table 36.

Table 36 — DoIP entity status request

Item	Pos.	Len.	Description	Values	Support
DoIP Entity Status Request					
No additional message element.					

[DoIP-120] If supported, a DoIP entity shall implement the DoIP entity status response as specified in Table 37.

[DoIP-121] If supported, a DoIP entity shall respond with a DoIP Entity Status Response within A_DoIP_Ctrl (see Table 38) after having received a previous DoIP entity status request.

Table 37 — DoIP entity status response

Item	Pos.	Len.	Description	Values	Support
DoIP Entity Status Response					
Node type (NT)	0	1	Identifies whether the contacted DoIP instance is either a DoIP node or a DoIP gateway.	0x00: DoIP gateway 0x01: DoIP node 0x02…0xFF: reserved by this part of ISO 13400	mandatory
Max. concurrent TCP_DATA sockets (MCTS)	1	1	Represents the maximum number of concurrent TCP_DATA sockets allowed with this DoIP entity, excluding the reserve socket required for socket handling.	1…255	mandatory
Currently open TCP_DATA sockets (NCTS)	2	1	Number of currently established sockets.	0…255	mandatory
Max. data size (MDS)	3	4	Maximum size of one logical request that this DoIP entity can process.	0…4 GB	optional

7.2 Socket handling

7.2.1 Connection states

7.2.1.1 General information

This subclause describes the status information and behavioural requirements of DoIP entities on the vehicle side with respect to connection status information.

7.2.1.2 Connection table

A logical connection between an external device (e.g. external test equipment) and a DoIP entity is uniquely identified by the logical equipment address (SA) and a socket handle. The socket handle is represented by the source and destination IP address and port and the transport layer protocol type (i.e. UDP or TCP).

[DoIP-152] A DoIP entity shall be able to distinguish logical connections based on socket handle and associated SA.

[DoIP-153] A DoIP entity shall be able to support the timers that are connection specific (initial inactivity timer, general inactivity timer) per logical connection.

[DoIP-154] If authentication or confirmation mechanisms are supported by a DoIP entity, the authentication state or the confirmation state shall be supported for each logical connection.

Figure 11 depicts the DoIP connection table.

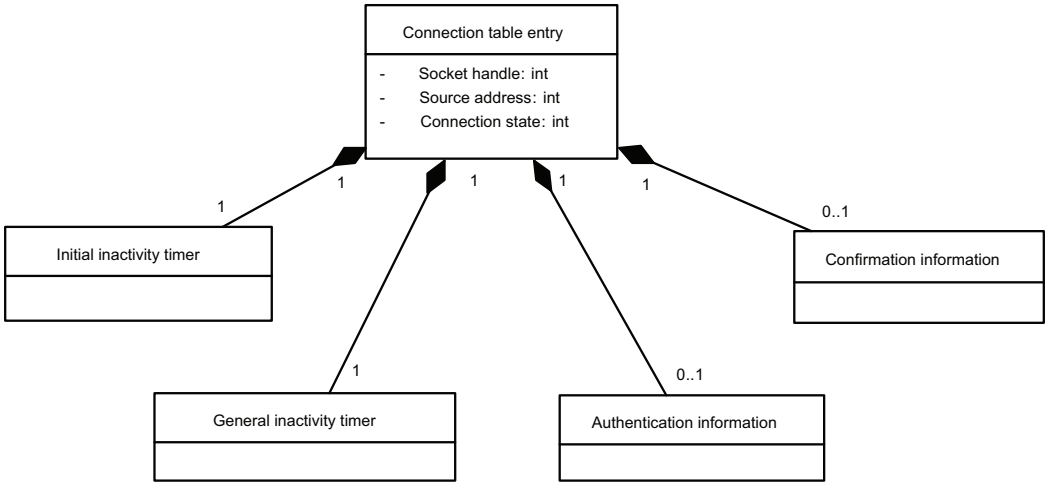


Figure 11 — DoIP connection table

7.2.1.3 Connection states

[DoIP-127] When a new socket is in the state “TCP established”, it shall be added to a connection handling table as “initialized”. An initial inactivity timer shall be started and assigned to the connection entry.

[DoIP-128] After receipt of a DoIP routing activation message and successful completion of the DoIP protocol handler, the initialized socket represents a logical connection and shall be updated to the connection state “Registered [Pending for Authentication]”. The SA of the initializing external test equipment shall be associated to the connection. The initial inactivity timer shall be stopped and a general inactivity timer shall be started and associated with the connection.

[DoIP-129] After successful completion of an authentication mechanism or if authentication is not required, the connection shall be set to the connection state “Registered [Pending for Confirmation]”.

[DoIP-130] After successful completion of a confirmation mechanism or if confirmation is not required, the connection shall be set to the connection state “Registered [Routing Active]”.

[DoIP-131] Incoming DoIP messages, except the DoIP routing activation message or messages required for authentication or confirmation, shall not be processed nor be routed before the connection is in the state “Registered [Routing Active]”.

Figure 12 depicts the DoIP connection states.

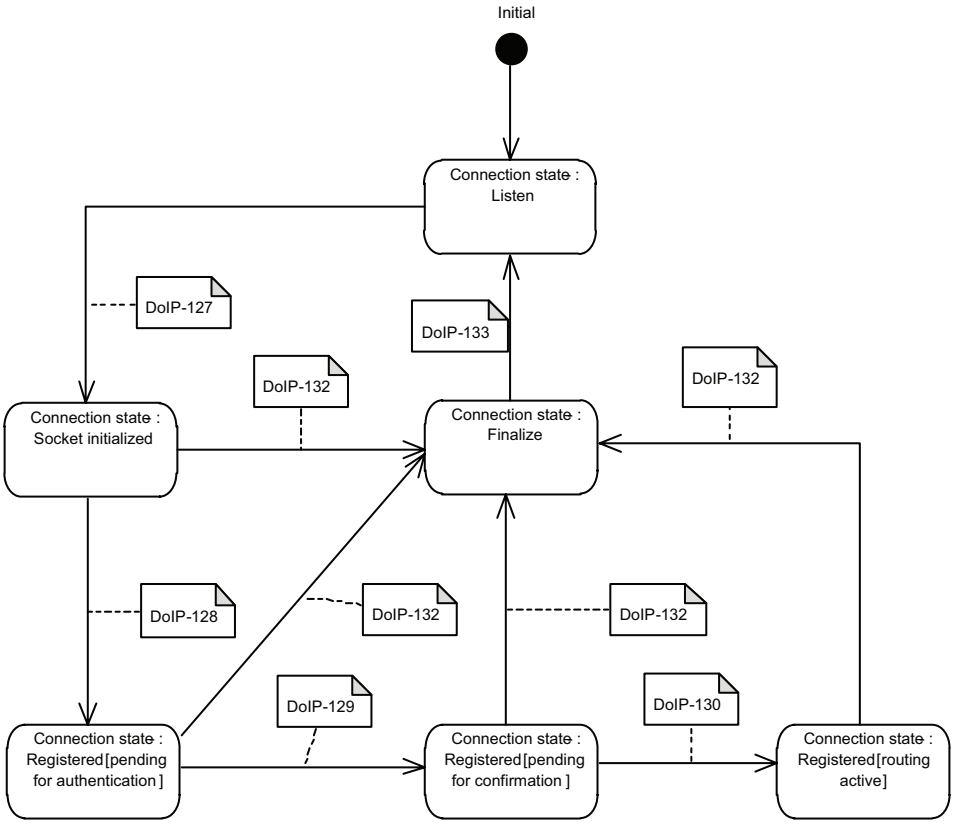


Figure 12 — DoIP connection states

[DoIP-132] If the initial timer or the general inactivity timer elapses or if authentication or confirmation are rejected or the external test equipment does not respond to a DoIP alive check message, the connection shall be set to the connection state “Finalize”.

[DoIP-133] If a connection is in the state “Finalize” (e.g. after a close request from either side), the TCP socket shall be closed reset to the listen state and resources shall be freed to allow a new connection to be established.

7.2.1.4 Alive check

An alive check request may only be sent on a connection that is in a “Registered” state. On a socket that is initialized and stored in a connection table entry but not yet registered (i.e. waiting for an activate routing request), no alive check requests shall be sent. Such a socket will timeout due to the initial inactivity timer if no routing activation request is sent.

[DoIP-134] The DoIP alive check message shall only be sent on connections that are currently in one of the “Registered” connection states.

7.2.2 General inactivity timer

The general inactivity timer is a measure against situations in which the network connection is broken or the external test equipment does not send any data but does not close the TCP_DATA connection. In this case, the general inactivity timer will close unused TCP_DATA sockets in order to return the DoIP entity into a default state after a specific time of inactivity.

[DoIP-079] Each DoIP entity shall implement an individual general inactivity timer for each supported TCP_DATA socket.

[DoIP-080] The general inactivity timer of a TCP_DATA socket shall be reset to its initial value T_TCP_General_Inactivity (Table 38) when the socket is initially put into the “established” state (open) or whenever data is received or sent over this socket.

[DoIP-124] If the external test equipment needs to keep a currently idle connection alive, the alive check response message shall be used.

NOTE The alive check response message is the smallest valid message that results in no further action than resetting the general inactivity timer for the corresponding connection. An invalid DoIP message would result in the TCP_DATA socket being closed by the DoIP entity.

[DoIP-081] The general inactivity timer of a TCP_DATA socket shall run as long as the TCP_DATA socket is in the established state (open).

[DoIP-082] If the general inactivity timer of a TCP_DATA socket has elapsed, the associated TCP_DATA socket shall be closed and reset to the listen state.

7.2.3 Initial inactivity timer

The initial inactivity timer is a measure against connection attempts on TCP_DATA sockets of a DoIP entity with invalid DoIP messages or without sending any data.

[DoIP-083] Each DoIP entity shall implement an individual initial inactivity timer for each supported TCP_DATA socket.

[DoIP-084] The initial inactivity timer of a TCP_DATA socket shall be reset to its initial value T_TCP_Initial_Inactivity (see Table 38) and shall be started when the socket is initially put into the “established” state (open).

[DoIP-085] The initial inactivity timer of a TCP_DATA socket shall be stopped immediately after receipt of a valid routing activation request (see Table 22) on this TCP_DATA socket.

[DoIP-086] If the initial inactivity timer of a TCP_DATA socket has elapsed, the associated TCP_DATA socket shall be closed and reset to the listen state.

7.2.4 Socket handler and alive check

This subclause specifies the requirements for DoIP entities on how to handle multiple TCP_DATA sockets in order to guarantee that the external test equipment can connect to the DoIP entities and also to make available unused TCP_DATA sockets for communication while ensuring that existing connections are not disturbed by additional connection attempts. Figure 25 in Clause 11 shows an example sequence of external test equipment triggering the TCP_DATA socket handler while trying to activate routing on a newly established TCP_DATA socket.

[DoIP-088] Each DoIP entity shall implement the TCP_DATA socket handling in the order specified in Figure 13.

NOTE 1 For the TCP_DATA socket handler, it is assumed that the underlying TCP stack ensures that multiple TCP sockets listening to the same port are dynamically allocated and used for inbound TCP connect attempts until no further TCP data sockets are available. In this case, it is assumed that the TCP stack will refuse additional connection attempts, using the TCP_RST response.

Figure 13 depicts the TCP_DATA socket handler.

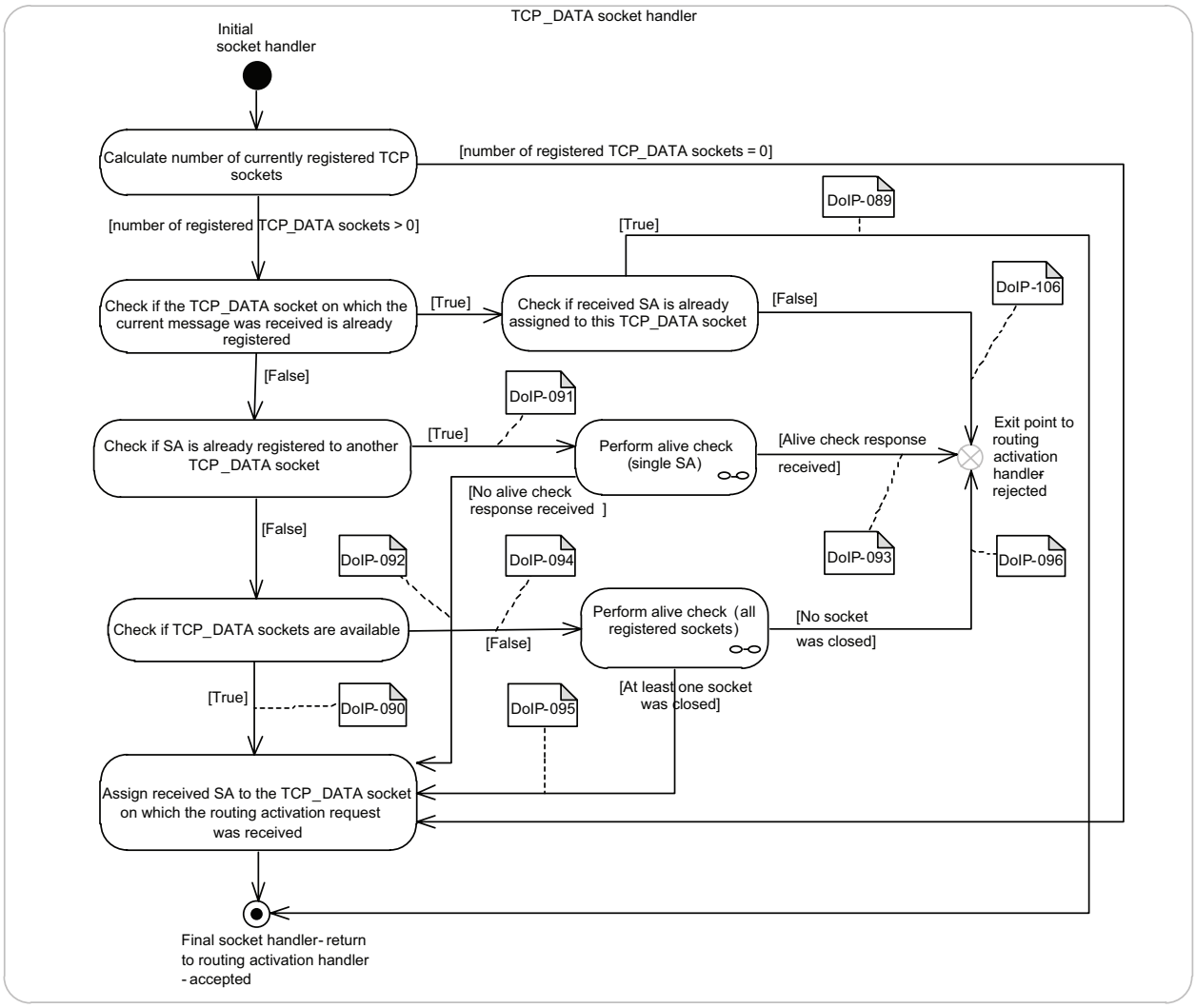


Figure 13 — TCP_DATA socket handler

NOTE 2 To reduce the complexity of the requirements, the description of each requirement focuses on the current specific operation, assuming that all previous checks have already been performed according to the sequence depicted in Figure 13. Examples of the implementation of different alive check methods (single TCP_DATA sockets and all TCP_DATA sockets) are depicted in Figures 14 and 15.

Figure 14 depicts the alive check on single TCP_DATA sockets.

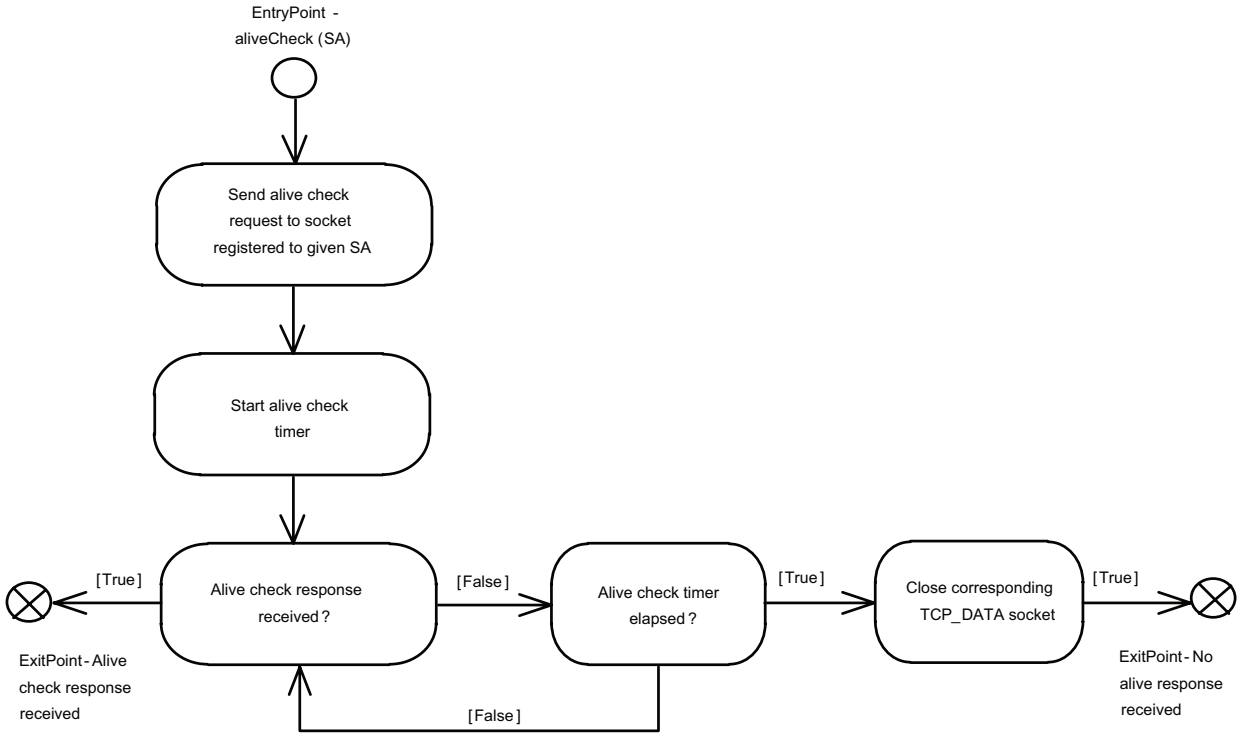


Figure 14 — Alive check on single TCP_DATA sockets

Figure 15 depicts the alive check on all TCP_DATA sockets.

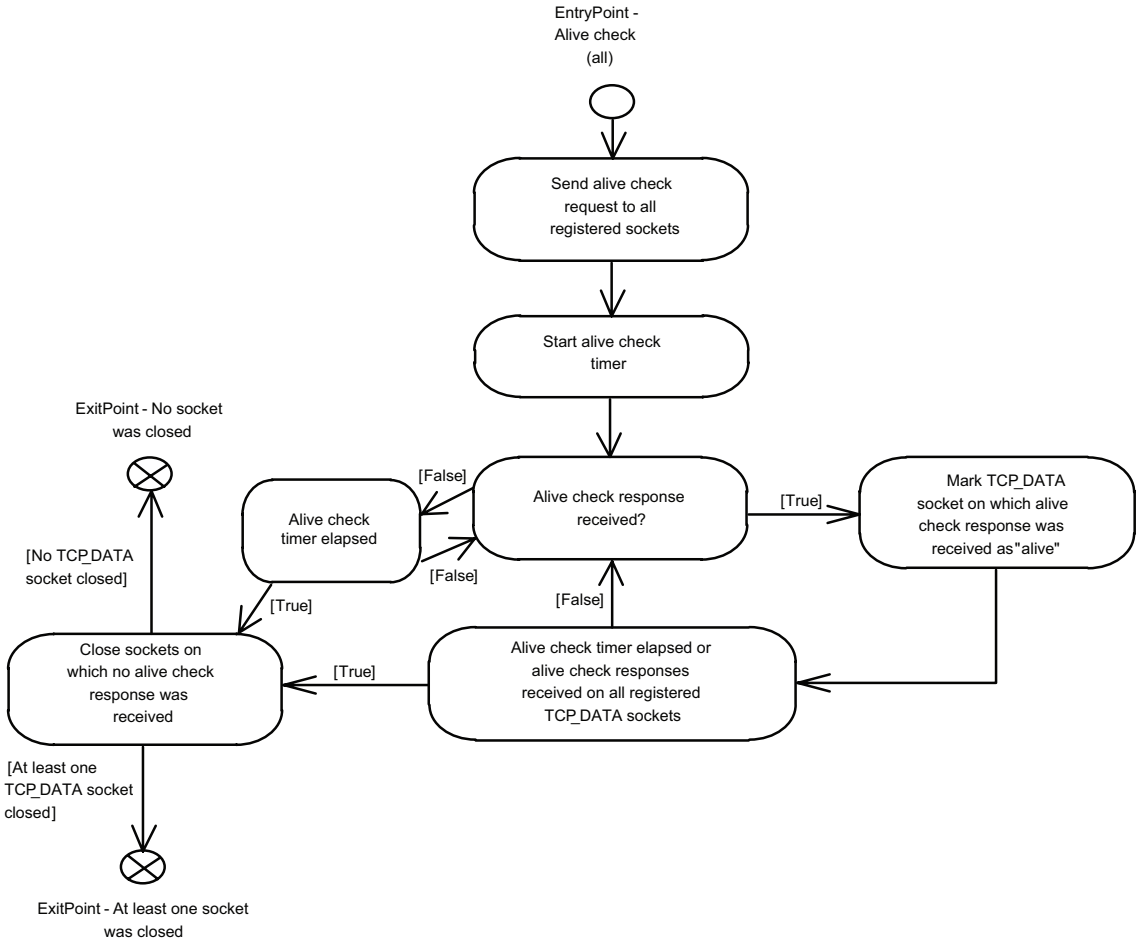


Figure 15 — Alive check on all TCP_DATA sockets

[DoIP-089] The requested DoIP entity shall accept routing activation if the SA in the routing activation request message is already assigned to the TCP_DATA socket on which the request was received.

[DoIP-106] The requested DoIP entity shall reject routing activation if the SA in the routing activation request message is different from the one currently registered for the TCP_DATA socket on which the routing activation request was received.

[DoIP-090] The requested DoIP entity shall accept the routing activation request and assign the SA to the TCP_DATA socket on which the routing activation request was received if the SA in the routing activation request message is not assigned to any of the established TCP_DATA sockets and the maximum number of concurrently supported TCP_DATA sockets is not yet exceeded.

[DoIP-091] The requested DoIP entity shall send an alive check request message via the TCP_DATA socket to which the SA received in the routing activation request message is currently assigned.

[DoIP-092] If no alive check response is received by the DoIP entity within the timeout T_TCP_Alive_Check (see Table 38), it shall close the corresponding TCP_DATA socket and accept the routing activation request on the TCP_DATA socket on which the routing activation request was received.

[DoIP-093] If an alive check response is received by the DoIP entity within the timeout T_TCP_Alive_Check (see Table 38), the DoIP entity shall reject routing activation on the TCP_DATA socket on which the routing activation request was received.

[DoIP-094] The requested DoIP entity shall send an alive check request onto all currently established TCP_DATA sockets if the SA is known but not yet assigned to any of the established TCP_DATA sockets and if the maximum number of concurrently supported TCP_DATA sockets is already registered.

[DoIP-095] The DoIP entity shall close those TCP_DATA sockets on which no alive check response is received when the timeout T_TCP_Alive_Check (see Table 38) elapses, and it shall accept the routing activation request and register the SA with the TCP_DATA socket on which the routing activation request was received.

[DoIP-096] If an alive check response is received on all registered TCP_DATA sockets by the DoIP entity within the timeout T_TCP_Alive_Check (see Table 38), the DoIP entity shall reject routing activation on the TCP_DATA socket on which the routing activation request was received.

7.3 Timing and communication parameters

Table 38 specifies the DoIP-specific communication parameters, including timeout values and payload type-specific performance requirements. In addition, the diagnostic protocol session layer timings are mapped onto the DoIP messages.

Table 38 — DoIP timing and communication parameters

Timing parameter	Description	Parameter value
A_DoIP_Ctrl	This timeout specifies the maximum time that the external test equipment waits for a response to a previously sent UDP message. This includes the maximum time to wait and collect multiple responses to a previous broadcast (UDP only).	Timeout: 2 s
A_DoIP_Announce_Wait	This timing parameter specifies the initial time that a DoIP entity waits until it responds to a vehicle identification request and the time that a DoIP entity waits until it transmits a vehicle announcement message after a valid IP address is configured. The value of this timing parameter shall be determined randomly between the minimum and the maximum value.	Random time: 0…500 ms
A_DoIP_Announce_Interval	This timing parameter specifies the time between the vehicle announcement messages that are sent by the DoIP entities after a valid IP address has been configured.	Delay time: 500 ms
A_DoIP_Announce_Num	This parameter specifies the number of vehicle announcement messages which are sent by the DoIP entity after a valid IP address was configured.	Repetition: 3 times
A_DoIP_Diagnostic_Message	This is the time between receipt of the last byte of a DoIP diagnostic message and the transmission of the confirmation ACK or NACK. After the timeout has elapsed, the request or the response shall be considered lost and the request may be repeated.	Performance time: 50 ms Timeout: 2 s
T_TCP_General_Inactivity	This timeout specifies the maximum time of inactivity on a TCP_DATA socket (no data received or sent) before it is closed by the DoIP entity.	Timeout: 5 min
T_TCP_Initial_Inactivity	This timeout specifies the maximum time of inactivity directly after a TCP_DATA socket is established. After the specified time without routing activation, the TCP_DATA socket is closed by the DoIP entity.	Timeout: 2 s

Table 38 *(continued)*

Timing parameter	Description	Parameter value
T_TCP_Alive_Check	This timeout specifies the maximum time that a DoIP entity waits for an alive check response after having written an alive check request on the TCP_DATA socket. Thus, the timer will also elapse if the underlying TCP stack is unable to deliver the alive check request message.	Timeout: 500 ms
A_Processing_Time	This timeout is defined as the time between transmission from the external test equipment of DoIP messages that require no response message but may need some time to be processed. Thus, the external test equipment must wait for at least A_Processing_Time before sending another request to the same DoIP entity.	Timeout: 2 s
A_Vehicle_Discovery_Timer	This is a per vehicle offboard sided timer. This timer specifies the time a vehicle can take to perform the VIN/GID synchronization between all DoIP entities. The vehicle discovery timer may only be started when a vehicle announcement/vehicle identification response message containing a VIN/GID sync. status code “incomplete” (0x10) and a valid VIN or GID is received by the external test equipment.	Timeout: 5 s

7.4 Logical addressing

This subclause specifies the structure and usage of the logical addresses used, for example, for diagnostic messages. A physical logical address uniquely represents a diagnostic application layer entity within any DoIP entity or on any ECU of the in-vehicle networks connected via DoIP gateways. The vehicle discovery process (see 9.2) allows the external test equipment to map physical logical addresses to IP addresses. Functional logical addresses are used to address messages to groups of, or all of, the diagnostic application layer entities within a vehicle. For functional addressing, the external test equipment may have to send multiple IP packets in order to reach all ECUs addressed by the functional logical address. There is no mechanism to address multiple DoIP entities via a single IP address. For a DoIP Gateway the reception of a functionally addressed diagnostics message implies a multi- or broadcast on the connected in-vehicle sub-networks.

Table 39 defines the addressing scheme for logical addresses.

NOTE The addressing scheme in Table 39 does not standardize individual addresses for individual ECUs. Thus, if external test equipment wants to determine the associated functionality of a responding ECU, this needs to be carried out via other methods, e.g. on the application layer.

Table 39 — Logical address overview

Address	Description
0x0000	ISO/SAE reserved
0x0001…0x0DFF	Vehicle manufacturer specific
0x0E00…0x0FFF	Reserved for addresses of external test equipment
0x0E00…0x0E7F	External legislated diagnostics test equipment (e.g. for emissions test scan-tool use) [a]
0x0E80…0x0EFF	External vehicle-manufacturer-/aftermarket-enhanced diagnostics test equipment [b]
0x0F00…0x0F7F	Internal data collection/on-board diagnostic equipment (for vehicle-manufacturer use only) [c]
0x0F80…0x0FFF	External prolonged data collection equipment (vehicle data recorders and loggers, e.g. used by insurance companies or to collect vehicle fleet data) [d]
0x1000…0x7FFF	Vehicle manufacturer specific
0x8000…0xCFFF	ISO/SAE reserved
0xD000…0xDFFF	Reserved for SAE Truck & Bus Control and Communication Committee
0xE000…0xE3FF	ISO/SAE-reserved functional group addresses
0xE000	ISO 27145 WWH-OBD functional group address
0xE001…0xE3FF	ISO/SAE reserved
0xE400…0xEFFF	Vehicle-manufacturer-defined functional group logical addresses
0xF000…0xFFFF	ISO/SAE reserved

[a] When using these addresses in the routing activation request other ongoing diagnostic communication in the vehicle may be interrupted and other normal functionality may be impaired (e.g. return to a failsafe behavior).

[b] When using these addresses in the routing activation request and diagnostic messages the routing activation may be delayed initially due to other ongoing diagnostic communication, which may then be interrupted and other normal functionality may also be impaired (e.g. return to a failsafe behavior).

[c] These addresses should not be used by external test equipment that is not designed as an integral part of the vehicle. This includes any plug-in equipment that performs diagnostic communication through the diagnostic connector.

[d] These addresses should be used by equipment that is installed in the vehicle and remains in the vehicle for periodic data retrieval by means of diagnostic communication. The DoIP entities may deny/delay accepting a routing activation request from this type of equipment in order to complete ongoing vehicle internal communication to avoid that normal operation of the vehicle may be impaired.

7.5 Communication environments and recommended timings

Depending on the IP network scenario, different timings and influences on communication performance apply. These need to be considered when defining timing parameters for the network scenarios. Since the number of possibilities for network architectures and structures is almost unlimited, this part of ISO 13400 does not specify specific timings and network setups. For some network scenarios refer to ISO 13400-1.

8 Transport layer services

8.1 General information

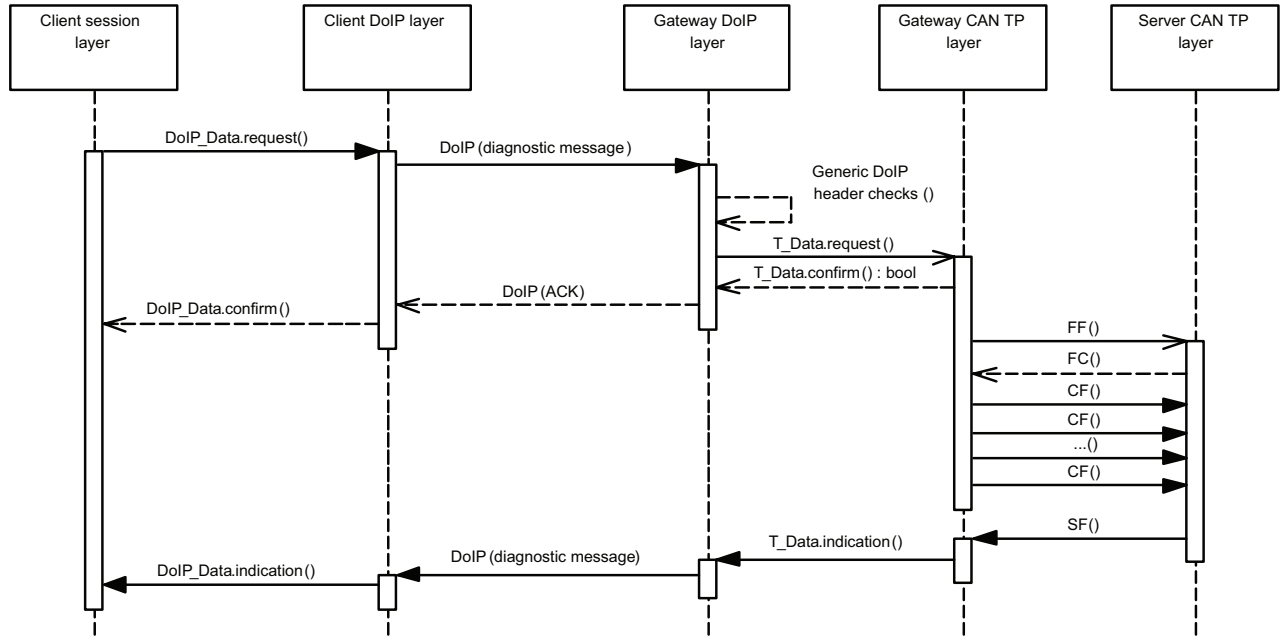
All transport layer services have the same general structure. To define the services, three types of service primitive are specified:

— a *service request primitive*, used by higher communication layers or the application to pass control information and data required to be transmitted to the network layer;

— a *service indication primitive*, used by the DoIP layer to pass status information and received data to upper communication layers or the application;

— a *service confirmation primitive*, used by the DoIP layer to pass status information to higher communication layers or the application.

This service specification does not specify an application programming interface, but only a set of service primitives that are independent of any implementation. An example of their occurrence during diagnostic communication is shown in Figure 16.



Key

CF consecutive frame
FC flow control
FF first frame
SF single frame

Figure 16 — DoIP layer service primitives

All DoIP layer services have the same general format. Service primitives are written in the form:

service_name.type (
parameter A,
parameter B,
[,parameter C, ...]
)

where “service_name” is the name of the service, e.g. _DoIP_Data; “type” indicates the type of the service primitive; and “parameter A, parameter B, [parameter C, ...]” are the DoIP_SDU as a list of values passed by the service primitive. The brackets indicate that this part of the parameter list may be empty.

The service primitives define how a service user (e.g. diagnostic application) cooperates with a service provider (e.g. DoIP layer). The following service primitives are specified in this part of ISO 13400: request, indication and confirm.

— Using the service primitive *request* (service_name.request), a service user requests a service from the service provider.

— Using the service primitive *indication* (service_name.indication), the service provider informs a service user about an internal event of the network layer or the service request of a peer protocol layer entity service user.

— With the service primitive *confirm* (service_name.confirm), the service provider informs the service user about the result of a preceding service request of the service user.

NOTE The order of parameters provided for each service primitive does not represent the order of the representing data elements in the corresponding messages, but only provides a syntactical description.

8.2 Specification of DoIP layer service primitives

8.2.1 DoIP_Data.request

The service primitive requests transmission of <MessageData> with <Length> bytes from the sender to the receiver peer entities identified by the address information in DoIP_SA, DoIP_TA and DoIP_TAtype (see 8.3 for parameter definition).

Each time the DoIP_Data.request service is called, the DoIP layer shall signal the completion (or failure) of the message transmission to the service user by issuing a DoIP_Data.confirm service call:

DoIP_Data.request (
DoIP_SA
DoIP_TA
DoIP_TAtype
<MessageData>
<Length>
)

8.2.2 DoIP_Data.confirm

The DoIP_Data.confirm service is issued by the DoIP layer. The service primitive confirms the completion of a DoIP_Data.request service identified by the address information in DoIP_SA, DoIP_TA and DoIP_TAtype. The parameter <DoIP_Result> provides the status of the service request (see 8.3 for parameter definition).

DoIP_Data.confirm **(**
DoIP_SA
DoIP_TA
DoIP_TAtype
<DoIP_Result>
)

8.2.3 DoIP_Data.indication

The DoIP_Data.indication service is issued by the DoIP layer. The service primitive indicates <DoIP_Result> events and delivers <MessageData> with <Length> bytes received from a peer protocol entity identified by the address information in DoIP_SA, DoIP_TA and DoIP_TAtype to the adjacent upper layer (see 8.3 for parameter definition).

The parameters <MessageData> and <Length> are only valid if <DoIP_Result> equals DoIP_OK.

DoIP_Data.indication **(**
DoIP_SA
DoIP_TA
DoIP_TAtype
<MessageData>
<Length>
<DoIP_Result>
)

The DoIP_Data.indication service call is issued after the reception of a DoIP diagnostic message.

If the DoIP layer detects any type of error in a DoIP diagnostic message, then the message shall be ignored by the DoIP layer and no DoIP_Data.indication shall be issued to the adjacent upper layer.

8.3 Service data unit specification

8.3.1 DoIP_AI, address information

8.3.1.1 DoIP_AI description

These parameters refer to addressing information. As a whole, the DoIP_AI parameters are used to identify the source address (DoIP_SA) and target address (DoIP_TA) of message senders and recipients as well as the communication model for the message (DoIP_TAtype).

8.3.1.2 DoIP_SA, DoIP logical source address

Type: 2 byte unsigned integer value

Range: 0x0000-0xFFFF

Description: The DoIP_SA parameter shall be used to encode the sending DoIP layer protocol entity.

8.3.1.3 DoIP_TA, DoIP logical target address

Type: 2 byte unsigned integer value

Range: 0x0000-0xFFFF

Description: The DoIP_TA parameter shall be used to encode the receiving DoIP layer protocol entity.

8.3.1.4 DoIP_TAtype, DoIP logical target address type

Type: enumeration

Range: physical, functional

Description: The parameter DoIP_TAtype is an extension to the DoIP_TA parameter. It shall be used to encode the communication model used by the communicating peer entities of the DoIP layer. Two communication models are specified: 1 to 1 communication, called physical addressing (unicast), and 1 to n communication, called functional addressing (multicast/broadcast).

NOTE See 7.4 for details on mapping physical and functional logical addresses to IP addresses.

8.3.2 <Length>

Type: 32 bits

Range: 0 GB-4 GB (2^{32} bytes)

Description: This parameter includes the length of data to be transmitted/received.

8.3.3 <MessageData>

Type: array of bytes

Range: 0-255 for each byte

Description: This parameter includes all data that the higher layer entities exchange.

8.3.4 <DoIP_Result>

Type: enumeration

Range: DoIP_OK, DoIP_HDR_ERROR, DoIP_TIMEOUT_A, DoIP_UNKNOWN_SA, DoIP_INVALID_SA, DoIP_UNKNOWN_TA, DoIP_MESSAGE_TOO_LARGE, DoIP_OUT_OF_MEMORY, DoIP_TARGET_UNREACHABLE, DoIP_NO_LINK, DoIP_NO_SOCKET, DoIP_ERROR

Description: This parameter contains the status relating to the outcome of a service execution. If two or more errors are discovered at the same time, then the network layer entity shall use the parameter value first found in this list in the error indication to the higher layers. For details, see Figure 10.

9 DoIP protocol usage

9.1 General information

This subclause gives an example of a standard workflow of a straightforward DoIP session. In order to keep this introduction as helpful as possible for a reader new to DoIP, exceptions and errors that might occur during a DoIP session are not covered here. Two possible network environments – networked and directly connected – are explained. The figures will provide a better understanding of the comprised DoIP components, mechanisms and sequences that allow a proper DoIP session.

As only the connection and the vehicle discovery (see 7.1.4) differ between the direct connection and the networked scenarios, the homogeneous parts of the DoIP session are described in Figure 17 for both scenarios.

9.2 Connection establishment and vehicle discovery

9.2.1 Direct connection scenario

In a direct connection scenario (see ISO 13400-1) with no networking infrastructure, a “crossover” Ethernet cable has to be used or Auto-MDI(X) has to be supported by the Ethernet controller of either the external test equipment or the DoIP entity, in order to directly connect the vehicle to the external test equipment.

It is assumed that, in such a scenario, no DHCP server is present. Thus, although initiated, the DHCP process will not be successful. Rather, a locally valid IP address will be determined by the auto-configuration mechanism and afterwards configured for both interfaces involved.

As soon as the DoIP entity’s interface has been configured with the obtained IP address, the DoIP entity will broadcast its VIN, EID, GID and logical address through a vehicle announcement message (see 7.1.4). The message will be broadcast (UDP) three times with the destination port UDP_DISCOVERY.

Depending on whether the external test equipment is configured in time for TCP/IP communication to receive the initial vehicle announcement messages, the external test equipment may have to poll for a vehicle using the vehicle identification request message. The Auto-IP mechanism might be delayed on the external test equipment as some operating systems start the Auto-IP only after DHCP has failed. As the DoIP entity initiates both mechanisms in parallel, it is likely that its IP configuration will be completed quickly and the external test equipment will not receive the initial vehicle announcement.

Figure 17 depicts the connection and vehicle discovery in a direct connection scenario.

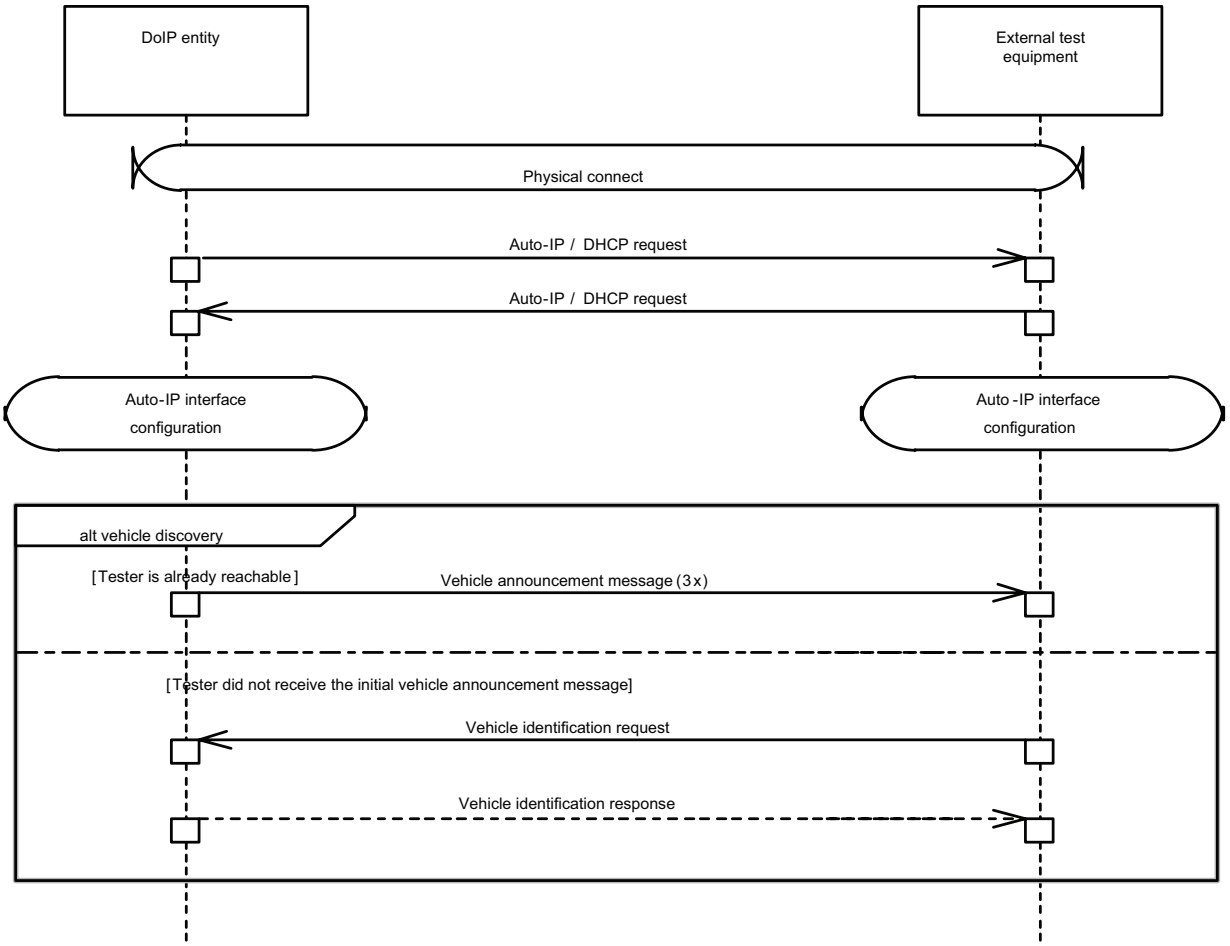


Figure 17 — Connection and vehicle discovery in a direct connection scenario

9.2.2 Networked scenario

The connection and vehicle discovery process is slightly different in a networked scenario (see ISO 13400-1). The physical connections to the network are not necessarily synchronized in time. Accordingly, the points in time when the interfaces are configured and accessible for a TCP/IP connection attempt might differ significantly.

If the external test equipment has not received the vehicle announcement message sent by the desired DoIP entity/vehicle (there might be numerous vehicles sending vehicle announcement messages through the network), it shall poll for it by sending vehicle identification request messages.

Figure 18 depicts the connection and vehicle discovery in a networked scenario.

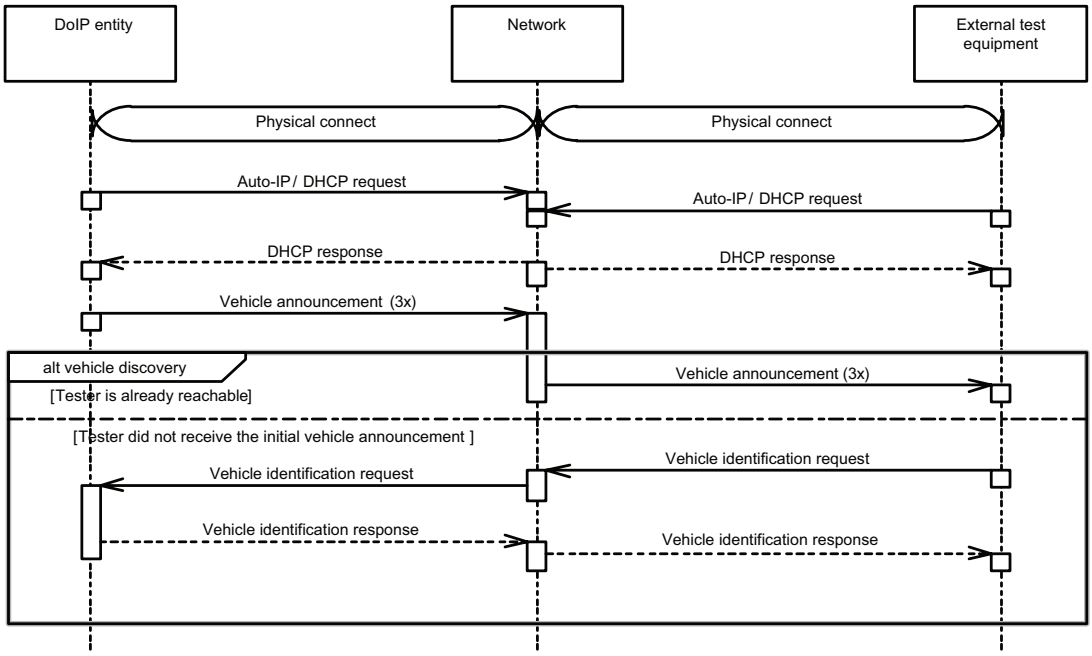


Figure 18 — Connection and vehicle discovery in a networked scenario

9.3 DoIP session

The step “Add vehicle to list” (see Figure 19) is not covered by this part of ISO 13400 and thus it is not mandatory or may not even be necessary. Nevertheless, it is likely that the vehicle announcement message broadcast in the previous step will be processed in some way. For example, the vehicle could be indicated as “ready” to an engineer within a GUI, or an automated process could be initiated based on the information that a vehicle is now available for a DoIP session.

Although in the networked scenario there is still the networking equipment between the external test equipment and the DoIP entity, the communication is now logically directly between the two communication endpoints. Thus, no “network” is shown in Figure 19.

The first step in order to initiate a connection between the external test equipment and the DoIP entity within the vehicle is to open a socket (destination port is TCP_DATA). This has to be done prior to any message exchange. Therefore, a DoIP entity has to provide the resources to handle the incoming communication request (e.g. socket resources). The DoIP entity has to provide sufficient resources to handle the specified number of concurrently supported DoIP sessions (<n>) plus one extra socket (see DoIP-002). If more than <n + 1> connection attempts do arrive at the same time, it is possible that no more resources are free and the <n + 2nd > connection attempt will be refused (because there are no longer any sockets in the listening state rather than because of DoIP protocol handling).

Once a socket has been established, some initializing steps have to be performed. An initial inactivity timer (see 7.2.3) and a general inactivity timer (see 7.2.2) have to be assigned and started. Additionally, it is necessary to ensure that no arriving data, except the routing activation request message, is routed or processed by setting the connection state to “initialize” (see 7.2.1.3). All subsequent messages shall be exchanged through this TCP_DATA socket.

To activate routing on the initialized connection, the external test equipment sends a routing activation request message (see 7.1.5) to the DoIP entity. If the external test equipment is eligible and if there are fewer than <n> active connections registered, the corresponding initial timer is stopped and – assuming that no additional authentication or confirmation is required – the socket state changes to “registered [Routing Active]”. Now valid DoIP messages (e.g. DoIP diagnostic messages) can be routed or processed. This is reported to the external test equipment by a positive routing activation response message. The general inactivity timer is restarted and remains active.

When receiving any kind of data, the DoIP entity first calls the DoIP header handler. If the payload consists of a diagnostic message (identified through the payload type *0x8001* in the generic DoIP header, see 7.1.6), the diagnostic message handler is called to process the payload.

When a diagnostic message arrives, the DoIP confirmation shall be sent to the calling external test equipment immediately after the message has successfully passed the diagnostic message handler (confirmation acknowledgement), i.e. the message has passed through the corresponding internal routing mechanism (assuming here that the DoIP entity is a DoIP gateway) but has not necessarily been sent to the destination ECU yet.

In the case of a UDS conform diagnostic message payload, the destination ECU sends a diagnostic response back to the external test equipment. This behaviour is described by the corresponding diagnostic protocol encapsulated by the DoIP message and thus is not within the scope of this part of ISO 13400.

When a connection is no longer required by the external test equipment, it shall always be closed through TCP/IP protocol mechanisms. The DoIP entity then initiates a finalization process for the connection. That finalization frees the corresponding resources so that the socket is available for a new connection. If the connection is not closed, the resources shall be freed after a timeout based on the general inactivity timer or after the performance of an alive check.

Figure 19 depicts the DoIP session example.

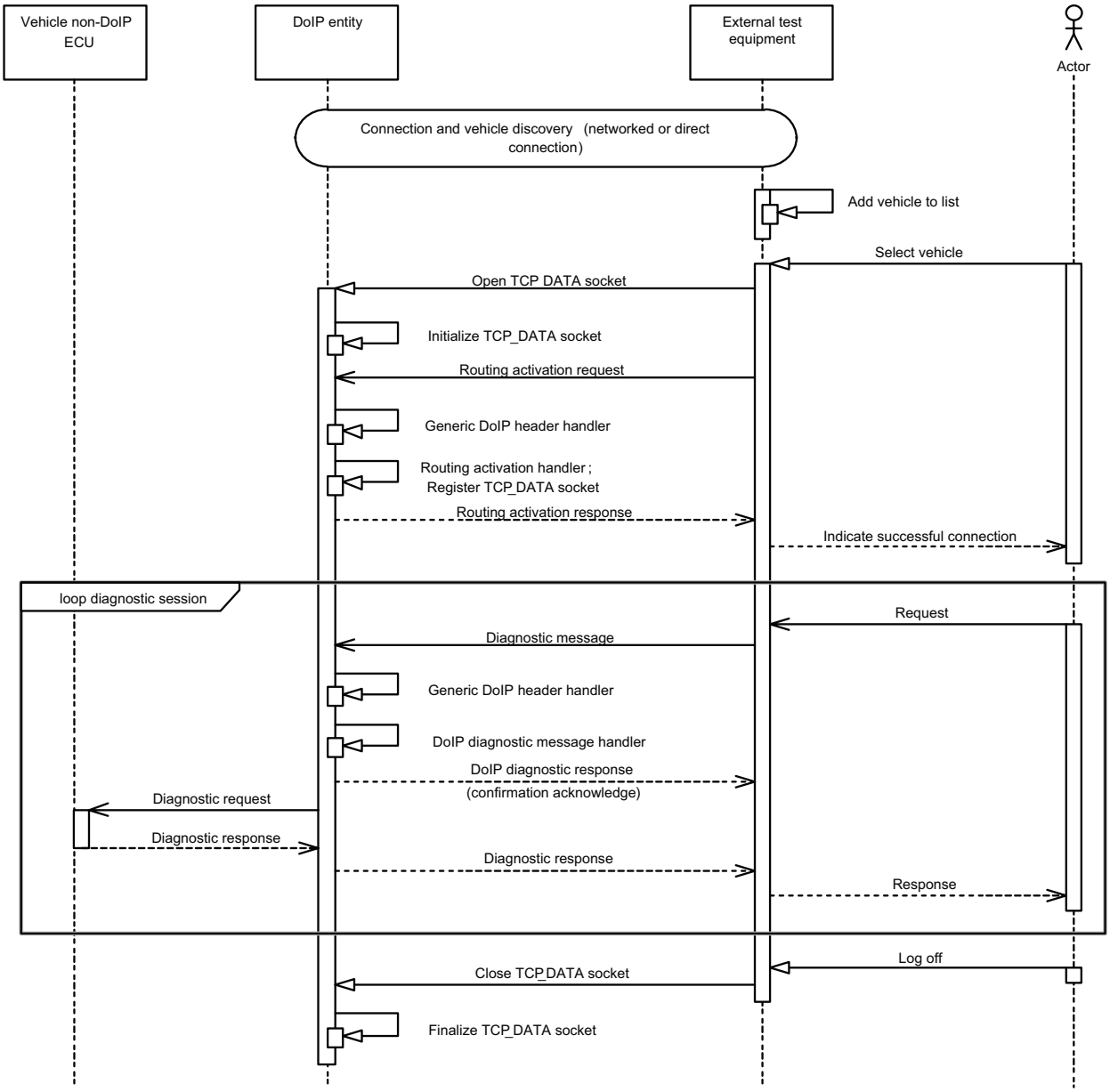


Figure 19 — DoIP session example

9.4 Vehicle network integration

9.4.1 Vehicle identification

This subclause specifies how a vehicle and its DoIP entities can be discovered and associated with their IP addresses on the network.

A vehicle will usually be identified by its VIN. In manufacturing or in after-sales environments, several DoIP entities may be installed on the same vehicle, but the vehicle-specific VIN is not yet configured at this point in time. In order to associate newly installed and un-configured DoIP entities with a certain vehicle, the group ID (GID) may be used instead of the VIN. A decentralized approach for identifying multiple DoIP entities within one vehicle is specified.

This implies that there will be a VIN/GID master (e.g. the DoIP edge node) from which all other DoIP entities receive the VIN/GID during a synchronization process. As this synchronization process usually requires some time (e.g. after a new DoIP entity is added to the vehicle) invalidity values are defined (see Table 40) for use by the DoIP entities until the VIN/GID synchronization is finished.

A detailed specification of VIN/GID synchronization between DoIP entities is outside the scope of this part of ISO 13400 and is left to the vehicle manufacturer's discretion.

[DoIP-143] Each DoIP entity shall support the synchronization of a vehicle's GID if more than one DoIP entity is present within the vehicle and if the availability of a valid VIN cannot always be guaranteed to be configured for every DoIP entity.

NOTE One possible way to ensure a globally unique GID is to use the GID masters MAC address.

Figure 20 describes schematically the VIN/GID synchronization and identification of two separate DoIP entities within the same vehicle.

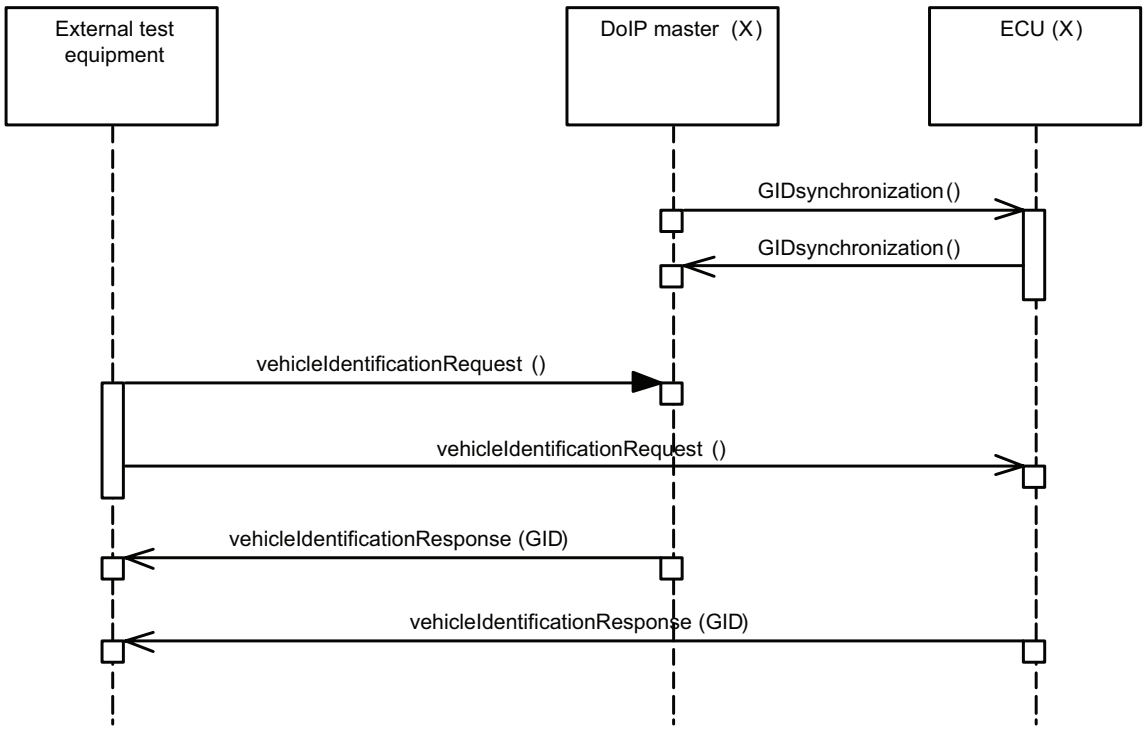


Figure 20 — Example of vehicle identification with VIN/GID synchronization

Table 40 — Invalidity values

Item	Len.	Values
VIN	17	0x00...00 or 0xFF…FF
Logical address	2	0x00 00 or 0xFF FF
Entity ID (EID)	6	0x00…00 or 0xFF…FF
Group ID (GID)	6	0x00…00 or 0xFF…FF

Figure 21 shows the sequence for connecting external test equipment to the vehicle and the IP address allocation process.

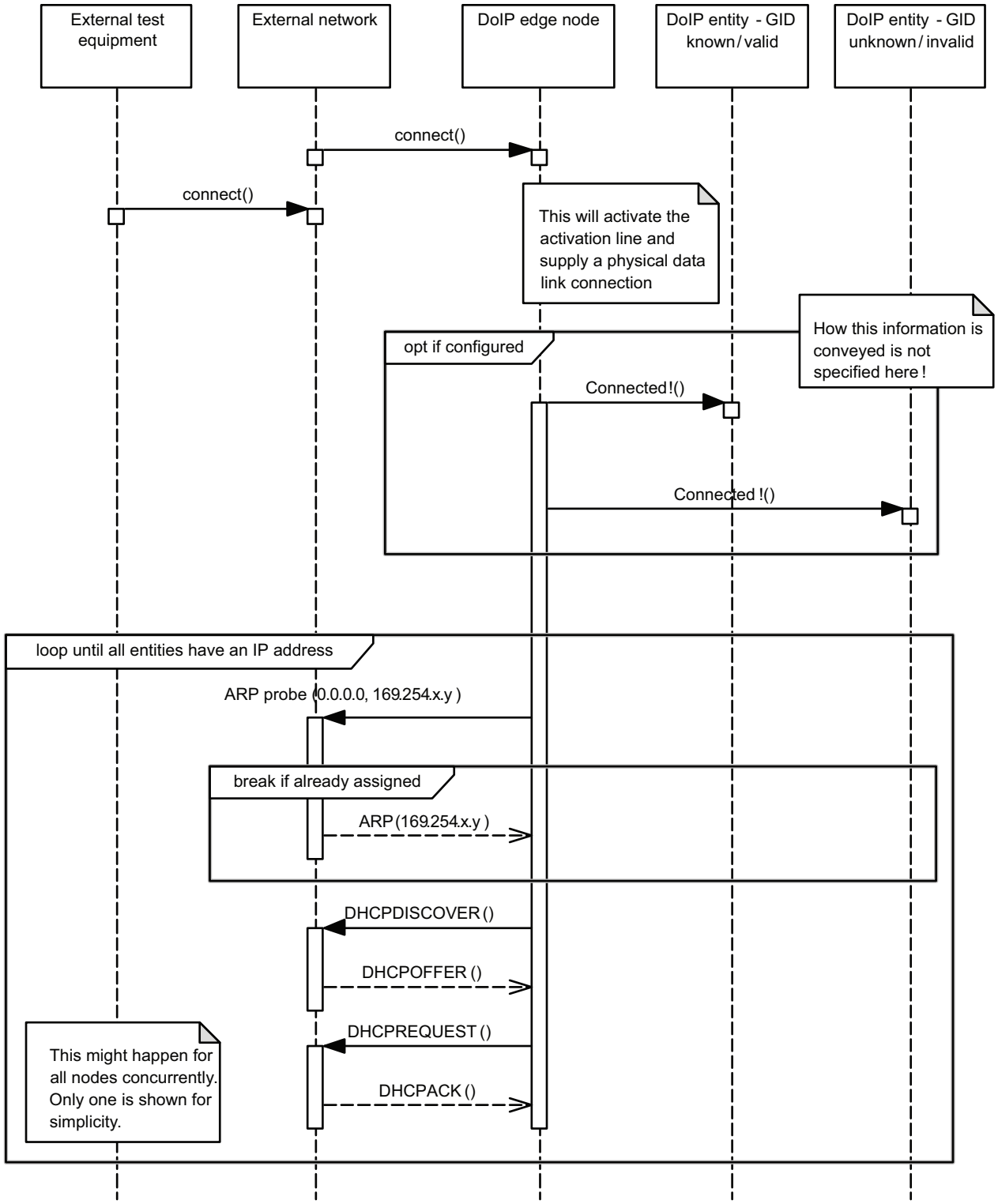


Figure 21 — Detailed vehicle identification

Figure 22 describes in more detail the complete decentralized approach to identifying multiple DoIP entities.

NOTE The scenario in Figure 22 does not cover the case in which vehicles are connected to the DoIP network once the vehicle discovery timer has already started.

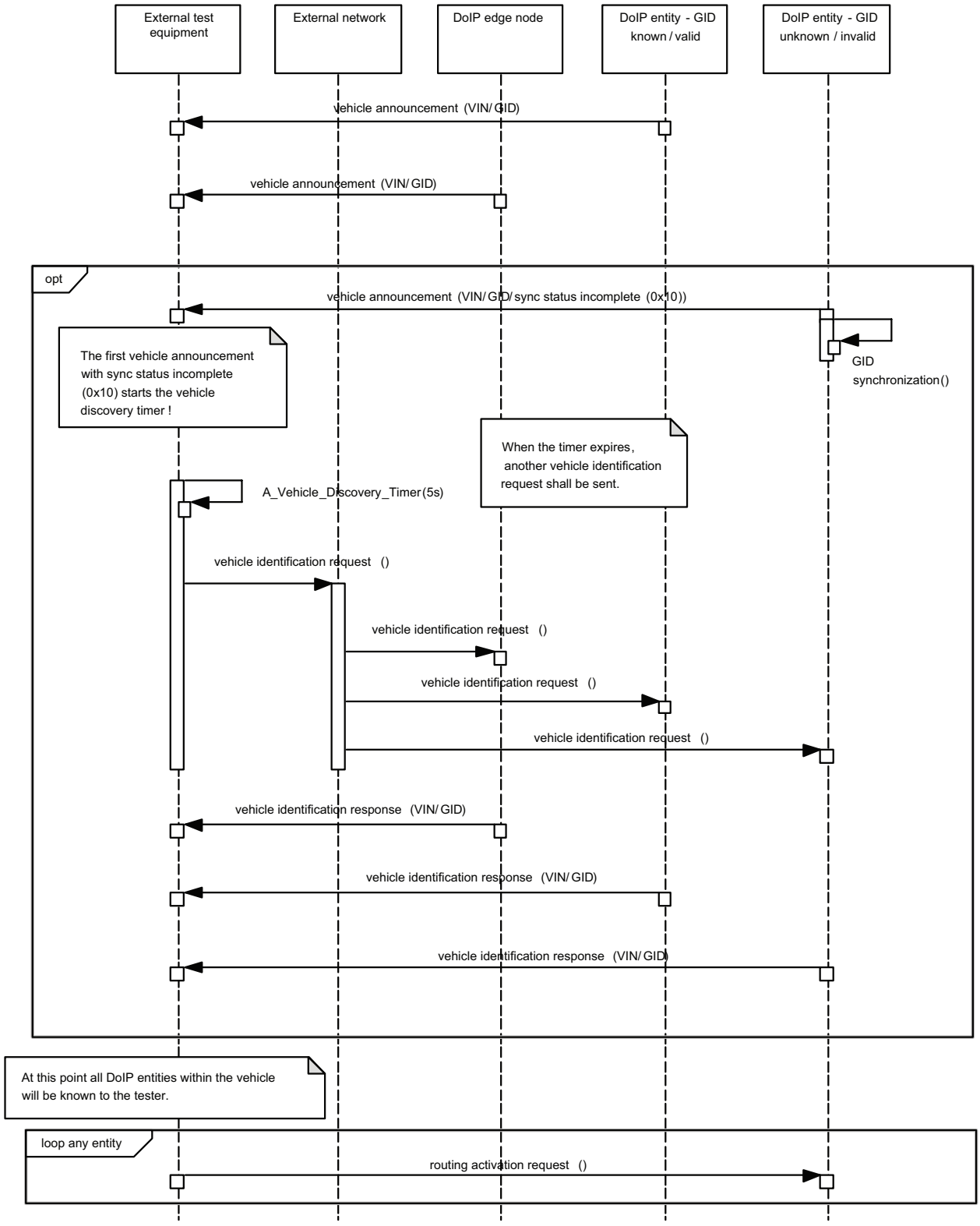


Figure 22 — Detailed vehicle identification with VIN/GID synchronisation

9.4.2 Vehicle identification — Off-board view

This subclause gives an example of a sequence by which external test equipment may be able to identify and group DoIP entities of all connected vehicles within the DoIP network.

Figure 23 shows an example of a simplified identification sequence performed by external test equipment. When a vehicle has been connected to the DoIP network and the IP address allocation has been completed (see Figure 21), the DoIP entities send out vehicle announcements after waiting for A_DoIP_Announce_Wait.

If the external test equipment is connected to the DoIP network at a later time, it should trigger vehicle announcement/identification responses by sending a broadcast vehicle identification request.

The DoIP entities in all vehicles respond to a vehicle identification request within A_DoIP_Ctrl.

If a vehicle announcement/vehicle identification received by the external test equipment contains a VIN/GID sync. status incomplete message (0x10), meaning that the VIN or GID is *not* synchronized with all DoIP entities in the vehicle, the external test equipment will start a vehicle discovery timer for this vehicle (identified by the VIN/GID given by the VIN/GID master in its vehicle announcement/vehicle identification response).

This mechanism allows the VIN/GID master to notify the external test equipment when some entities need more time for VIN/GID synchronization. When the vehicle discovery timer expires, another vehicle identification request shall be sent to all those DoIP entities, who reported VIN/GID invalid in their initial vehicle announcement/identification responses.

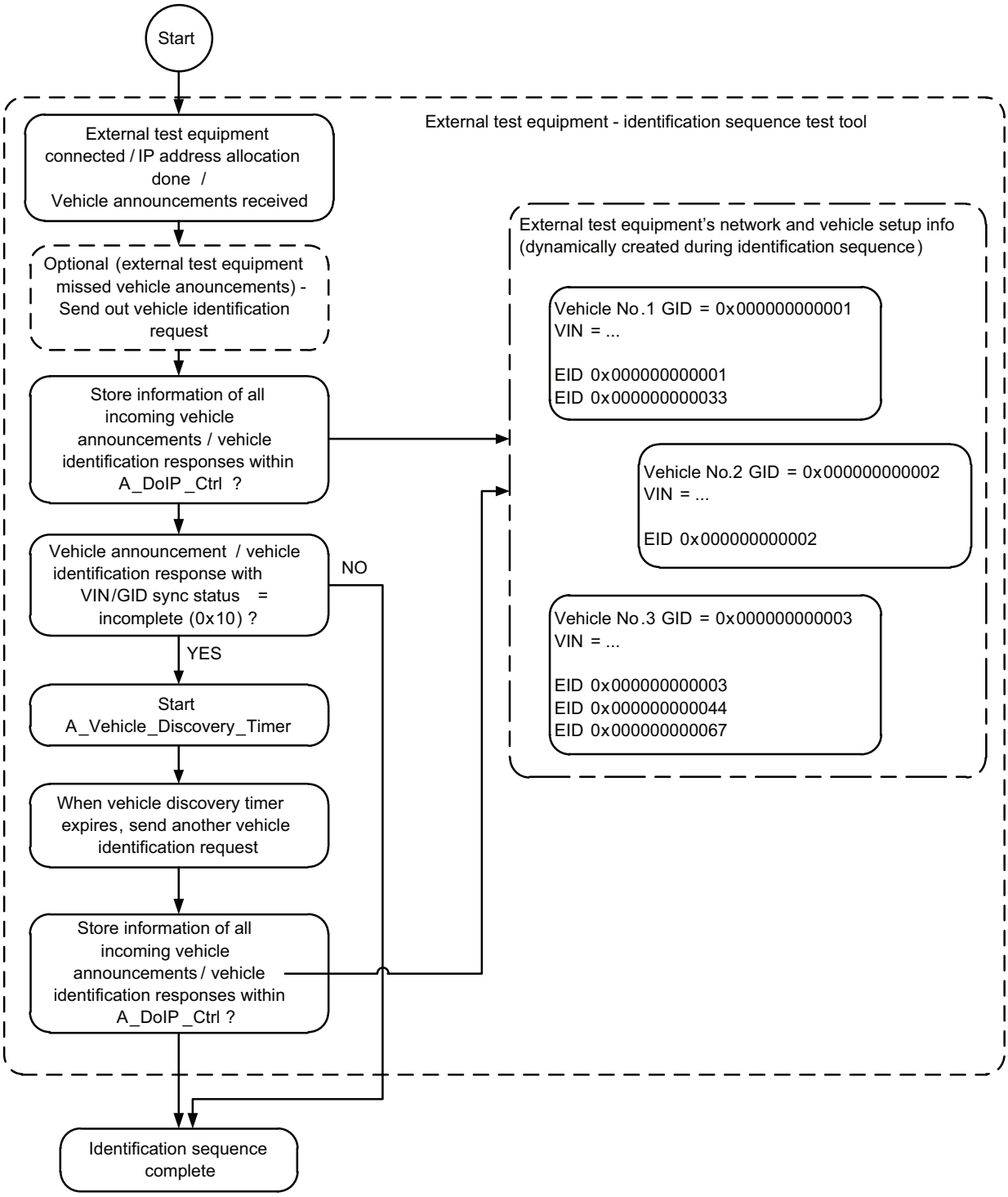


Figure 23 — Example of a simplified identification sequence of external test equipment

10 DoIP entity functional requirements

[DoIP-097] Each DoIP gateway shall route user data from diagnostic messages (see Table 26) received through the TCP_DATA socket to the corresponding ECU on the vehicle network according to the address information contained in the diagnostic message, using the ECU-specific vehicle network transport protocol.

[DoIP-098] Each DoIP gateway shall route the user data from the transport protocol transfer from ECUs on the vehicle network to the TCP_DATA socket using diagnostic messages (see Table 26) and the ECU-associated address information (source and target addresses).

NOTE This implies that a DoIP gateway needs to ensure that the correct address information is used for diagnostic messages to be sent on the corresponding TCP_DATA sockets.

Diagnostic messages that are addressed to the DoIP gateway itself may be routed to a “virtual” internal network for consistency reasons.

11 Communication example message sequence charts

This clause contains a number of message sequence charts (MSCs) showing the most common communication scenarios of external test equipment communication with the DoIP entities of a vehicle.

Figure 24 depicts the common vehicle announcement and identification sequence between a DoIP gateway or DoIP node and the external test equipment.

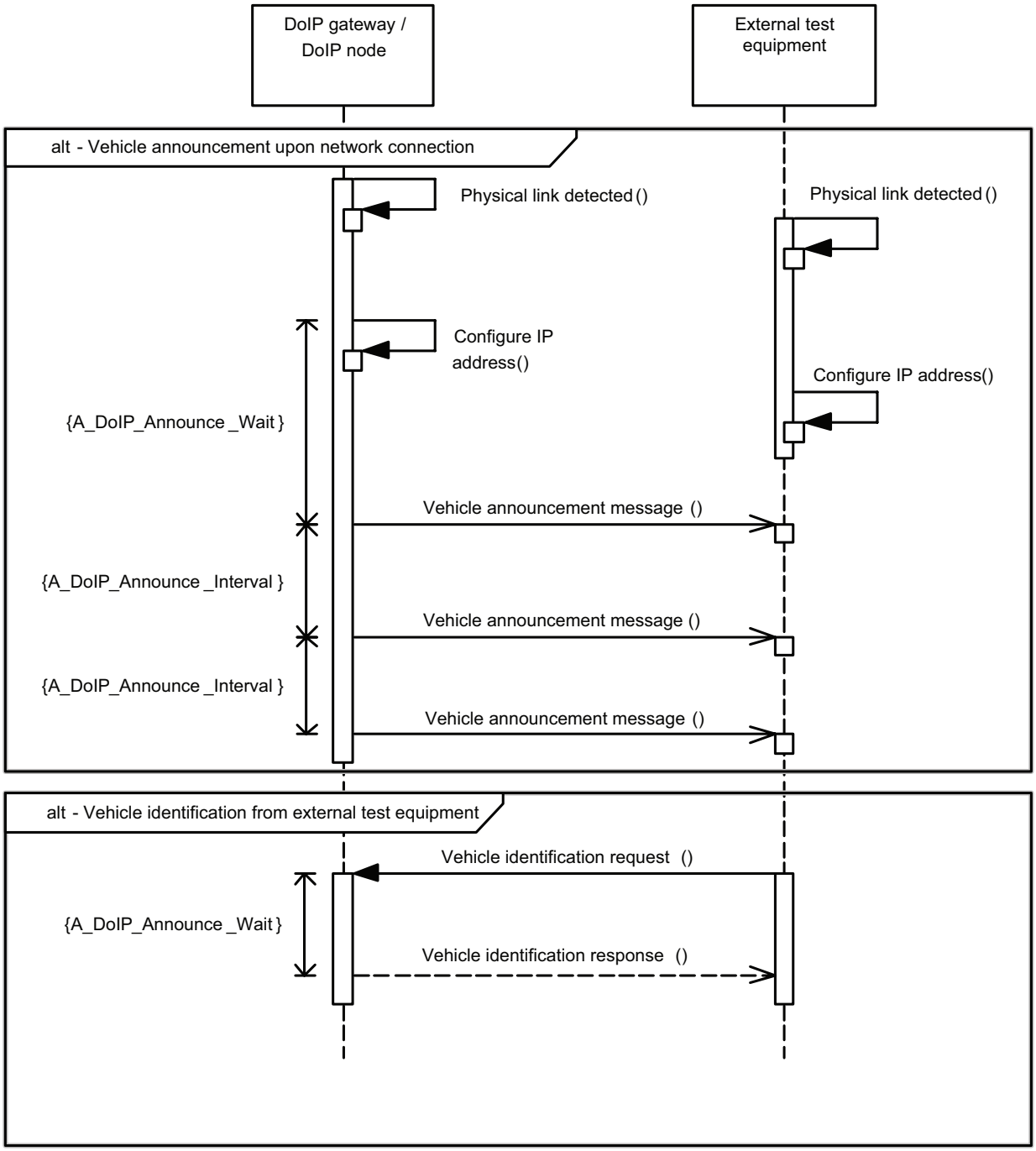


Figure 24 — Vehicle announcement and vehicle identification sequence

Figure 25 shows a sequence followed by the TCP_DATA socket handler, which is handling two concurrent sockets when a third connection is requested with a new routing activation request.

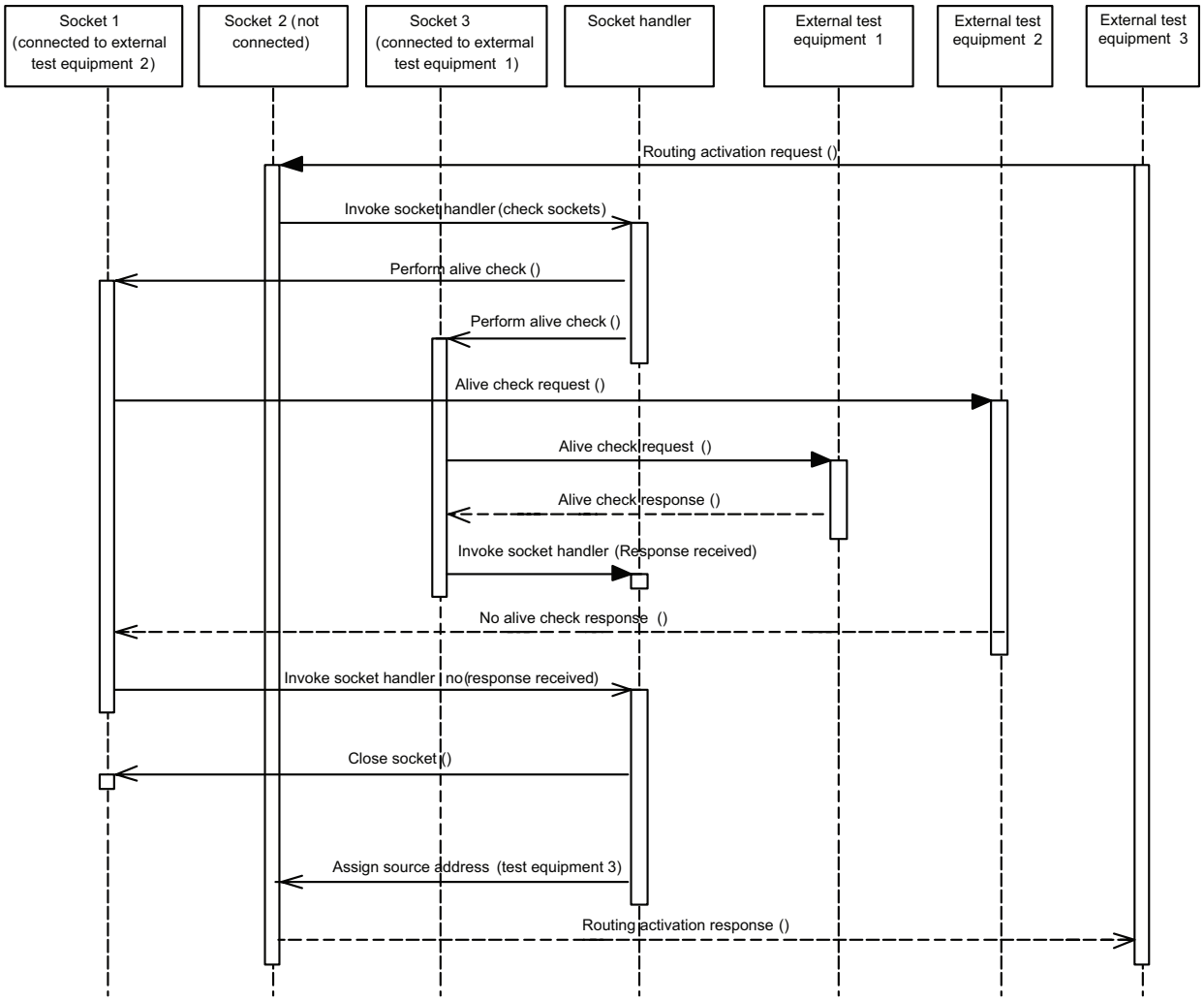


Figure 25 — Socket handler with two concurrent sockets and a third connection attempt

Bibliography

[1] ISO/IEC 7498-1, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

[2] ISO/IEC 10731, *Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services*

[3] ISO 13400-5[1)], *Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 5: Conformance test specification*

[4] ISO 14229-1, *Road vehicles — Unified diagnostic services (UDS) — Part 1: Specification and requirements*

[5] ISO 14229-2[2)], *Road vehicles — Unified diagnostic services (UDS) — Part 2: Session layer services*

[6] ISO 14229-5[3)], *Road vehicles — Unified diagnostic services (UDS) — Part 5: UDS on internet protocol implementation (UDSonIP)*

[7] ISO 15765-2, *Road vehicles — Diagnostic communication over Controller Area Networks (DoCAN) — Part 2: Transport protocol and network layer services*

[8] ISO 22900-2, *Road vehicles — Modular vehicle communication interface (MVCI) — Part 2: Diagnostic protocol data unit application programming interface (D-PDU API)*

[9] ISO 27145-1[4)], *Road vehicles — Implementation of WWH-OBD communication requirements — Part 1: General information and use case definition*

[10] ISO 27145-2[5)], *Road vehicles — Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication requirements — Part 2: Common data dictionary*

[11] ISO 27145-3[6)], *Road vehicles — Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication requirements — Part 3: Common message dictionary*

[12] ISO 27145-4[7)], *Road vehicles — Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication requirements — Part 4: Connection between vehicle and test equipment*

[13] IANA Ports, *Port Numbers*, IANA. Available at: http://www.iana.org/assignments/port-numbers (last updated 29 November 2011)

[14] IANA Protocols, *Protocol Numbers*, IANA. Available at: http://www.iana.org/assignments/protocol-numbers (last updated 1 November 2011)

[15] IEEE EUI-48 Guidelines, *Guidelines for use of a 48-bit Extended Unique Identifier (EUI-48™)*. Available at: http://standards.ieee.org/develop/regauth/tut/eui48.pdf

[16] IETF RFC 3942, *Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options*

[17] IETF RFC 4213, *Basic Transition Mechanisms for IPv6 Hosts and Routers*

---

1) Under preparation.

2) To be published.

3) Under preparation.

4) To be published. (Revision of ISO/PAS 27145-1:2006)

5) To be published. (Revision of ISO/PAS 27145-2:2006)

6) To be published. (Revision of ISO/PAS 27145-3:2006)

7) To be published. (Revision of ISO/PAS 27145-4:2006)

[18] IETF RFC 5220, *Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules*

[19] IETF RFC 5735, *Special Use IPv4 Addresses*

[20] IETF RFC 6298, *Computing TCP's Retransmission Timer*

[21] SAE J1930-DA, *Electrical/Electronic Systems Diagnostic Terms, Definitions, Abbreviations, and Acronyms Web Tool Spreadsheet*

[22] SAE J1939:2011, *Serial Control and Communications Heavy Duty Vehicle Network — Top Level Document*

[23] SAE J1939-73:2010, *Application Layer — Diagnostics*

[24] SAE J1962, *Diagnostic Connector*

[25] SAE J1979-DA, *Digital Annex of E/E Diagnostic Test Modes*

[26] SAE J2012-DA, *Digital Annex of Diagnostic Trouble Code Definitions and Failure Type Byte Definitions*

ICS 43.040.10; 43.180

Price based on 68 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™