INTERNATIONAL STANDARD

ISO 11783-5

Second edition
2011-04-01

Corrected version
2011-04-15

Tractors and machinery for agriculture and forestry — Serial control and communications data network —

Part 5: Network management

Tracteurs et matériels agricoles et forestiers — Réseaux de commande et de communication de données en série —

Partie 5: Gestion du réseau

Reference number
ISO 11783-5:2011(E)

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.

ISO 11783-5 was prepared by Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

This second edition cancels and replaces the first edition (ISO 11783-5:2001), which has been technically revised. It also incorporates the Technical Corrigendum ISO 11783-5:2001/Cor.1:2002.

ISO 11783 consists of the following parts, under the general title *Tractors and machinery for agriculture and forestry — Serial control and communications data network*:

— *Part 1: General standard for mobile data communication*

— *Part 2: Physical layer*

— *Part 3: Data link layer*

— *Part 4: Network layer*

— *Part 5: Network management*

— *Part 6: Virtual terminal*

— *Part 7: Implement messages application layer*

— *Part 8: Power train messages*

— *Part 9: Tractor ECU*

— *Part 10: Task controller and management information system data interchange*

— *Part 11: Mobile data element dictionary*

— *Part 12: Diagnostics services*

— *Part 13: File server*

— *Part 14: Sequence control*

In this corrected version, a reference to Subclause 0 at the end of the sixth paragraph in 4.1 has been replaced by a reference to Subclause 4.5.

Introduction

Parts 1 to 14 of ISO 11783 specify a communications system for agricultural equipment based on ISO 11898-1[1] and ISO 11898-2[2]. SAE J1939[3] documents, on which parts of ISO 11783 are based, were developed jointly for use in truck and bus applications and for construction and agriculture applications. Joint documents were completed to allow electronic units that meet the truck and bus SAE J1939 specifications to be used by agricultural and forestry equipment with minimal changes. This part of ISO 11783 is harmonized with SAE J1939/81[4]. General information on ISO 11783 is to be found in ISO 11783-1.

The purpose of ISO 11783 is to provide an open, interconnected system for on-board electronic systems. It is intended to enable electronic control units (ECUs) to communicate with each other, providing a standardized system.

The International Organization for Standardization (ISO) draws attention to the fact that it is claimed that compliance with this part of ISO 11783 may involve the use of a patent concerning the controller area network (CAN) protocol referred to throughout the document.

ISO takes no position concerning the evidence, validity and scope of this patent.

The holder of this patent right has assured ISO that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO. Information may be obtained from:

Robert Bosch GmbH
Wernerstrasse 51
Postfach 30 02 20
D-70442 Stuttgart-Feuerbach
Germany

Attention is drawn to the possibility that some of the elements of this part of ISO 11783 may be the subject of patent rights other than those identified above. ISO shall not be held responsible for identifying any or all such patent rights.

Tractors and machinery for agriculture and forestry — Serial control and communications data network —

Part 5: Network management

1 Scope

ISO 11783 as a whole specifies a serial data network for control and communications on forestry or agricultural tractors and mounted, semi-mounted, towed or self-propelled implements. Its purpose is to standardize the method and format of transfer of data between sensors, actuators, control elements and information storage and display units, whether mounted on, or part of, the tractor or implement. This part of ISO 11783 describes the management of source addresses (SAs) for control functions (CFs) of electronic control units (ECUs), the association of addresses with the functional identification of a device and the detection and reporting of network-related errors. It also specifies procedures, and minimum requirements, for initialization and response to brief power outages of network-connected ECUs.

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 11783-1, *Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 1: General standard for mobile data communication*

ISO 11783-2, *Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 2: Physical layer*

ISO 11783-3, *Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 3: Data link layer*

ISO 11783-4, *Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 4: Network layer*

ISO 11783-7, *Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 7: Implement messages application layer*

ISO 11783-12, *Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 12: Diagnostics services*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 11783-1 and the following apply.

3.1
control function
CF
function that performs operations to complete a specific function on or within devices

NOTE A CF has one unique address on the network.

3.2
current NAME
CF NAME that is transmitted in its address-claimed message

3.3
NAME management
NM
method for changing the NAME of a CF at run time

3.4
pending NAME
NAME temporarily stored by a particular CF as the result of NAME management messages received from a qualified source

3.5
random transmit delay
RT×D
delay period calculated by multiplying a random number in the range 0 to 255 by 0,6 ms

NOTE A seed to the random number generator can use the identity number in the NAME, or other unique information within the CF.

3.6
suspect parameter number
SPN
19-bit number used to identify a particular element, component, or parameter associated with a CF

NOTE Suspect parameter numbers are assigned to each individual parameter in a parameter group and to items that are relevant to diagnostics, but are not a parameter in a parameter group.

4 Technical requirements

4.1 General

Network management for an ISO 11783 network provides the definitions and procedures necessary to uniquely identify CFs on the network, manage the assignment of addresses and manage network errors.

A CF's ability to select an address depends on the CF's address configuration capabilities as described in 4.2.

Each CF shall be capable of providing its unique 64-bit NAME. The rules for creating this NAME, associating it with an address and giving the ability or non-ability to change that address are specified in 4.3.

CFs shall successfully claim an address in accordance with the procedures detailed in 4.4 prior to sending any other messages on the network. Multiple CFs can work together to perform a function, provided each CF claims its own address following the rules in 4.4.2.3.

The inability to successfully claim an address in accordance with the procedure shall be handled and reported to the network following a standard method detailed in 4.4.2.4.

Network initialization sequences associated with the address-claiming process are described in 4.5.

A set of physical requirements which extends the requirements of ISO 11783-2 is listed in 4.6.

Where timeouts are not otherwise specified, the timeout defaults defined in ISO 11783-3 apply.

4.2 Address configuration capabilities

4.2.1 General

Address configuration is the method by which a particular CF determines the SA it will use for an address claim. For the purposes of the address-claiming process, there are two basic address configuration capabilities: non-configurable address and self-configurable address. These are distinguished by the value in the self-configurable address field in the most significant bit position in the CF's NAME.

CFs conforming to ISO 11783 shall be self-configurable-address-capable. Non-configurable-address-capable CFs shall be tolerated on the network to allow compatibility with CFs conforming to the previous edition of this part of ISO 11783 and CFs conforming to SAE J1939.

There are also two extended address configuration capabilities: command-configurable address and service-configurable address. A CF may implement one or more of the extended address configuration capabilities.

4.2.2 Non-configurable address

A non-configurable address CF cannot change its initial address during the address-claiming process. If multiple non-configurable address CFs are claiming the same address, then only the CF with the highest-priority NAME can obtain the address. The others shall announce their inability to claim an address.

The self-configurable address field is the most significant bit in the CF's NAME and therefore a non-configurable address CF always has higher priority than a self-configurable address CF. This implies that a non-configurable address CF forces a self-configurable address CF to claim another address.

4.2.3 Self-configurable address

A self-configurable address CF is one that can select its initial address based on proprietary algorithms and then claim that address. This CF, in cases of address conflict, is also able to re-calculate its address and re-claim (unless all 120 of the addresses between 128 and 247 are used). The value in the self-configurable address field in the NAME (see 4.3.2) indicates whether or not a CF has this capability.

The CF shall only change its initial address when it loses address arbitration, and it shall only use addresses in the range 128 to 247 inclusive. But if the CFs function is one that has an assigned preferred address, then it may also use the preferred address.

4.2.4 Service-configurable address

A service-configurable address CF is one whose source address can be changed in the field by a service technician. The address can be altered by any one of a number of proprietary techniques or by using the commanded-address message, while in a “service” mode of operation. A service tool may be used for this operation.

4.2.5 Command-configurable address

A command-configurable address CF is one whose source address can be altered using the commanded-address message. The change can take place at any time, without the intervention of a service tool or the requirement of a special service mode of operation. It does require the presence on the network of a CF that can send the appropriate command to cause the address change.

4.3 NAME and address requirements

4.3.1 General

A NAME is a 64-bit entity composed of the fields defined in Table 1. Every CF transmitting messages on an ISO 11783 network shall have a unique NAME. A CF's NAME describes the function that a CF performs, and its numerical value is used in the arbitration for address (see Annex A for examples of NAMEs). NAMEs are normally established during initial network configuration on a machine or when a CF in an ECU is added to an existing network.

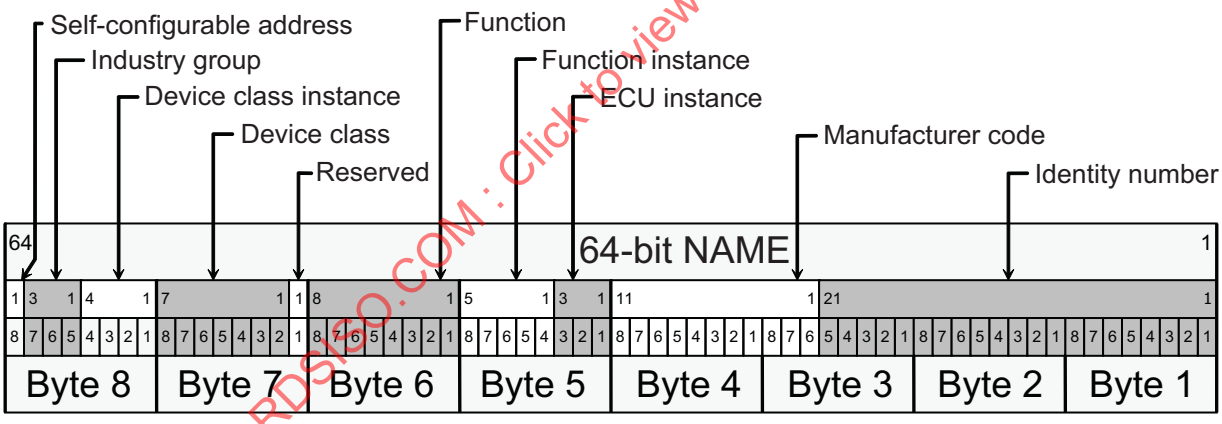
An address is used on an ISO 11783 network to provide a unique message identifier and to determine a message source which is known as a source address (SA). The procedures for address management in the protocol specified in this part of ISO 11783 enable individual SAs to be associated with particular CFs (see 4.4.2). In the case of an ECU that implements several CFs, a different address-configuration capability can exist for each of the CFs and each CF shall claim a unique SA.

An address-claimed message containing both a NAME and an SA is used to associate the two on the network. The association of a unique NAME and address also associates the address with the corresponding function. However, regardless of the SA with which it is associated, a NAME will retain a consistent definition.

4.3.2 NAME

Network integrators and ECU manufacturers shall ensure that each CF on a particular network has a unique NAME not possessed by another CF on that network.

The relationship between the 64-bit value used for arbitration priority (see 4.5.3), the data bytes in the address-claimed message (see 4.4.2.3) and the NAME fields (see Table 1) is shown in Figure 1.



NOTE The 64-bit value is sent with byte 1 first and byte 8 last when transmitted on the network.

Figure 1 — NAME bit fields in controller area network (CAN) message data bytes

Table 1 — NAME fields

Field	SPN	Definition	No. of bits	Byte No.	Byte ordering[a]
Self-configurable address	2844	Indicates whether a CF is self-configurable (1) or not (0); needs always to be known and set to the appropriate value	1	8	Bit 8: Self-configurable address
Industry group[b]	2846	Defined and assigned by ISO, identifies NAMEs associated with industries (e.g. agricultural equipment)	3		Bit 7 to bit 5: Industry group (most significant at bit 7)
Device class instance	2843	Indicates occurrence of a particular device class in a connected network; definition depends on industry group field contents (see Figure 2)	4		Bit 4 to bit 1: Device class instance (most significant at bit 4)[c]
Device class[b]	2842	Defined and assigned by ISO; provides a common NAME for a group of functions within a connected network; when combined with an industry group, can be correlated to a common NAME, e.g. “planter” with “agricultural equipment”	7	7	Bit 8 to bit 2: Device class (most significant at bit 8)
Reserved		Reserved for future definition by ISO	1		Bit 1: Reserved
Function[b]	2841	Defined and assigned by ISO; when value between 0 and 127, independent of any other field for definition; when > 127 but < 254, definition depends on device class; when combined with industry group and device class, can be correlated to a common NAME for specific CF, though not implying any specific capabilities	8	6	Bit 8 to bit 1: Function (most significant at bit 8)
Function instance	2839	Indicates specific occurrence of a function on a particular device system of a network	5	5	Bit 8 to bit 4: Function instance (most significant at bit 8)
ECU instance	2840	Indicates which of a group of ECUs associated with a given function is referenced	3		Bit 3 to bit 1: ECU (most significant at bit 3)
Manufacturer code[b]	2838	Assigned by committee (see ISO 11783-1); indicates manufacturer of ECU for which the NAME is being referenced; independent of any other NAME field	11	4	Bit 8 to bit 1: Most significant eight bits of manufacturer code (most significant at bit 8)
				3	Bit 8 to bit 6: Least significant three bits of manufacturer code (most significant at bit 8)
Identity number	2837	Assigned by the ECU manufacturer	21		Bit 5 to bit 1: Most significant five bits of identity number (most significant at bit 5)
				2	Bit 8 to bit 1: Second byte of identity number code (most significant at bit 8)
				1	Bit 8 to bit 1: Least significant byte of identity number (most significant at bit 8)[d]

[a] The byte ordering of the NAME fields is arranged so that the NAME can be treated as a number, consistent with ISO 11783-7.

[b] See ISO 11783-1 for numerical values of industry groups, device classes, functions and manufacturer codes.

[c] Bit 1 is the last of the data bits sent and closest to the cyclic redundancy code (CRC) in the message.

[d] Bit 8 is the bit closest to the data length code (DLC) in the message.

Table 1 defines and specifies the fields that comprise a NAME, listing them in order of priority, from the self-configurable address bit to the identity number's least significant byte.

The reserved bit shall be set to zero.

Any instance field in the NAME can be changed and reconfigured when an ECU is installed or, where there are multiple instances, on the network by the NAME management message (see 4.5.3).

An agreement can be reached, where appropriate, between the manufacturer and the system integrator on the interpretation and use of function instances. For example, a manufacturer or other parts of ISO 11873 may use the function instance to indicate position or special functionality of a CF.

EXAMPLE In the case of two engines and transmissions, agreement is reached that engine instance 0 be physically connected to transmission instance 0, and engine instance 1 to transmission instance 1.

Where a function is managed by two separate ECUs, each attached to the same ISO 11783 network, the ECU instance field should be set to 0 for the first ECU and to 1 for the second.

The ECU manufacturer shall ensure that the NAME is unique and non-varying when power is removed. Where all other fields are identical to the NAME of another CF, the NAME shall be made unique by setting the identity number (e.g. a serial number or a data/time code on the product).

Figure 2 shows the relationships between the fields, as well as the dependence of the upper 128 functions on device class and industry group, the dependence of identity number on manufacturer code, and the independence of function 0 to function 127 from either industry group or device class. The number of bits that each field comprises is noted above each field.

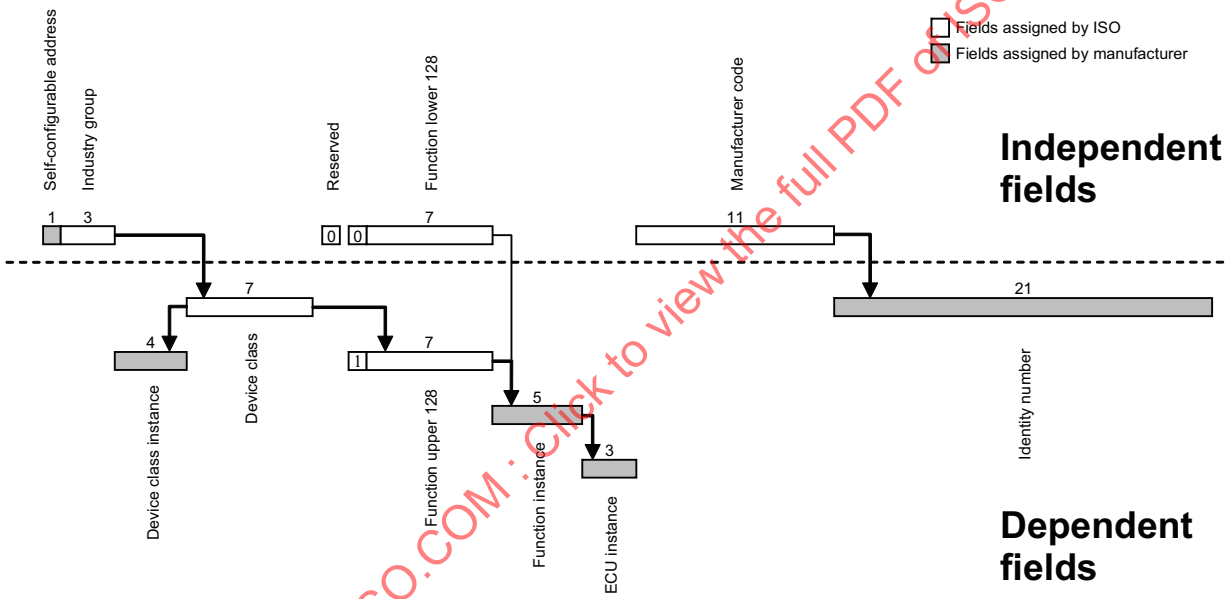


Figure 2 — NAME-field relationships and dependencies

4.3.3 Address

4.3.3.1 General

An address is a one-byte value identifying a particular CF on a network. The address of a CF is incorporated into the controller area network (CAN) identifier of every message sent by that CF and is used to provide uniqueness to messages that are sent by the CF. After initial power-up and when the network is operating, each CF shall have a unique SA. An SA can be associated with a different CF after each power-up of the network and can also vary from one network connection to another network connection. The NAME which is associated with a source address includes the identification of the function the CF performs and retains this consistent definition regardless of the SA that the CF uses.

4.3.3.2 Preferred address

CFs can operate on an ISO 11783 network using an assigned preferred address. If the preferred address has already been claimed, the CF shall either attempt to claim another SA or send a cannot-claim-address message depending on the CF's addressing capability and the availability of an unused address. When the CF claims another address, this new address shall be stored as the initial address to be used at all subsequent power-ups.

See ISO 11783-1 for a list of assigned preferred addresses.

A CF claiming a preferred address in the range 0 to 127 and 248 to 253 shall perform the function defined for that preferred address and shall specify that function within its NAME.

The function performed by a CF shall never be deduced from the SA alone; only the CF's NAME shall be used to establish the function[1)].

4.3.3.3 Self-configurable address

ISO 11783 CFs that do not have an assigned preferred address or cannot claim their preferred address shall claim an address in the range of 128 to 247. Since multiple CFs can be claiming addresses in this range, this type of CF shall be self-configurable-address-capable. This permits the address-claiming process to provide unique addresses for each CF on the network.

4.3.3.4 Initial address

At the time of production, the initial address (the address which the CF attempts to claim on power-up) shall be set to the preferred address. The initial address for a CF may be reprogrammed in order to permit configuration of the system.

Every time a CF with service-configurable, command-configurable or self-configurable address capabilities is required to claim a new address, this new address shall be stored as the initial address to be used at all subsequent power-ups. This also applies to CFs with assigned preferred addresses.

4.3.3.5 NULL address

The NULL address (254) is only permitted in the source address field of the ISO 11783 message identifier and is intended for use only within network management communications.

4.3.3.6 Global address

The global address (255) is only permitted in the destination address field of the ISO 11783 message identifier and never in the source address field.

4.4 Network-management procedure

4.4.1 General

Network management procedures include the messages exchanged and actions taken by CFs to collectively manage the network. Address and network-error management (see 4.4.2 and 4.4.4, respectively) are the network-management protocol's primary roles. With the exception of a limitation on use of the NULL address, network-management messages have the same characteristics, and are subject to the same requirements, as other ISO 11783 messages [for example, the request-for-address-claimed message is the request parameter group number (PGN) message specified in ISO 11783-3].

---

1) The previous edition of ISO 11783-5 did not enforce the address-to-function relationship.

The NULL address (254) is only acceptable in a network-management message's SA field, and only if the message is a request-for-address-claimed or cannot-claim-source-address message.

4.4.2 Address-management messages and procedures

4.4.2.1 Address-management message functions

The set of address-management messages as specified in Table 2 is used by CFs to:

— request a NAME and address used by another CF on the network (request-for-address-claimed message);

— claim an address (address-claimed message);

— respond with the inability to claim an address (cannot-claim-source-address message);

— command another CF to assume a new address (commanded-address message).

Table 2 — Address-management messages

Message	PGN	PF	PS	SA	Data length	Data
Request-for-address-claimed (request PGN)	59904[a]	234	DA	SA[b]	3	PGN 60928
Address-claimed	60928	238	255	SA	8	NAME
Cannot-claim-source-address	60928	238	255	254	8	NAME
Commanded-address	65240	254	216	SA	9[c]	NAME, new SA

[a] See ISO 11783-3.

[b] The SA is set to 254 if an address has not yet been claimed.

[c] The commanded-address message is sent using the broadcast announce message (BAM) transport protocol.

4.4.2.2 Request-for-address-claimed message

The request-for-address-claimed message can be transmitted by any CF to request the NAME and address of any other CF operating on the network. Upon its receipt, the receiving CF shall respond with an address-claimed message containing its address and its NAME, while a CF that is not able to claim an address shall respond with a cannot-claim-source-address message (see 4.4.2.3 for the procedure in both cases). The exception to this requirement is a CF that has not yet attempted to claim an address, which shall not send a cannot-claim-source-address message, nor, in fact, participate in any network communications (except request-for-address-claimed), before attempting to claim an address.

The SA for a request-for-address-claimed message shall be the NULL address if the message is sent from a CF that has not yet claimed an address.

A CF can transmit a request-for-address-claimed message either to the global destination address (255) or to a particular address. In the first case, the CF can then determine the existence on the network of another CF with a particular NAME by examining the responses to its message to the global destination address, while, in the second case, the initiating CF can interrogate the other to determine if the address has already been claimed. The CF shall respond to its own request-for-address-claimed message if it is sent to the global address.

4.4.2.3 Address-claimed message

The address-claimed message shall be used by a CF to respond to a request-for-address-claimed message and to claim an address on the network. If a CF receives an address-claimed message claiming its own

source address, it shall compare its own NAME with the one received and determine which NAME has the higher priority, i.e. the lower numerical value. If it determines that it has the higher priority, the CF shall transmit an address-claimed message containing its NAME and address. If, however, it has the lower priority, it shall either claim a new address or transmit a cannot-claim-source-address message (see 4.4.2.4). A single parameter group number (PGN) is used for both the address-claimed and cannot-claim-source-address messages.

Transmission repetition rate:	As required
Data length:	8 bytes
Data page field:	0
Protocol data unit (PDU) format field:	238
PDU-specific field:	255 (global address)
Default priority:	6
Parameter group number:	60928 ($00EE00_{16}$)
Source address	0 to 253
Bytes 1 to 8	NAME

In order to successfully claim an address, the CF sending an address-claimed message shall not receive a contending claim from another CF for at least 250 ms. A network interconnection unit shall not use its own address in communications on the network until it has already successfully claimed an address (forwarding messages between other ECUs is a special task of the network interconnection unit) (see ISO 11783-4). However, a network interconnection unit may forward messages before claiming its own address.

4.4.2.4 Cannot-claim-source-address message

A cannot-claim-source-address message is transmitted (in response to a request-for-address-claimed or address-claimed message) by any CF that cannot claim its initial address and does not have a self-configurable address capability, or that has a self-configurable address capability but cannot claim an address because none is available for use. Although the cannot-claim-source-address message has the same PGN as the address-claimed message, its SA shall be the NULL address (254).

Transmission repetition rate:	As response only
Data length:	8 bytes
Data page field:	0
Protocol data unit (PDU) format field:	238
PDU-specific field:	255 (global address)
Default priority:	6
Parameter group number:	60928 ($00EE00_{16}$)
Source address	254 (NULL address)
Bytes 1 to 8	NAME

An RT×D shall be inserted between the reception of a message triggering the cannot-claim-source-address response and the sending of the response in order to minimize the possibility of two such responses causing bus errors.

A CF that cannot claim an address shall send no message other than a cannot-claim-source-address or request-for-address-claimed message.

A CF that cannot claim an address may continue to receive and process global messages (e.g. the commanded-address message).

4.4.2.5 Commanded-address message

Support of the commanded-address message is optional. If the CF does not support the commanded-address message, the remainder of this subclause shall be ignored.

This message can be used by one CF (for example a network interconnection unit, such as a bridge or a service tool) to command another CF (hereafter known as the commanded CF) to use a particular SA. If a CF receives a commanded-address message but is unable to change to the commanded SA, the CF shall respond with an address claim claiming the CF's current SA. An operator or technician could then modify the commanded CF's SA by other means. The ECU manufacturer could prevent its product from accepting commanded-address messages from any CF other than, for example, a bridge or service tool, or demand a security verification for its CF to accept such a message.

Transmission repetition rate:	As required
Data length:	9 bytes
Data page field:	0
Protocol data unit (PDU) format field:	254
PDU-specific field:	216
Default priority:	6
Parameter group number:	65240 ($00FED8_{16}$)
Bytes 1 to 8	NAME
Byte 9	Address assignment field (new SA)

When it accepts a commanded-address message, the commanded CF shall issue an address-claimed message using the address specified in the commanded-address message as its new SA. The requirements of 4.5.2 shall apply.

The commanded-address message shall contain 9 bytes of data and shall be sent to the global address (255) using the broadcast announce message (BAM) of the transport protocol (see ISO 11783-3). Therefore, CFs designed to support the commanded-address message shall also support BAM.

4.4.3 NAME management message and procedures

4.4.3.1 General

A message to change fields of the NAME of a CF can be used when configuring a network containing CFs with multiple instances of functions, ECUs or device classes. Changing the function of a generic ECU is another possible use of this message. It can also be used when other methods of uniquely identifying CFs are not available. This message can be used in conjunction with manual setup steps and/or with the commanded-address method to accomplish the configuration of the network.

NOTE This is a new message in this second edition of this part of ISO 11783.

One CF (the commanding CF) can command another CF (the target CF) to use a given NAME by using the NAME management message. This message can be used to instruct the target CF with a specific source address to replace some fields of its NAME with newly specified values.

The primary use of this message is to set the instance fields in the NAME, but all of the NAME fields can be modified by using this message, except for the identity number field which shall remain unchanged after initial manufacture.

It is optional for a CF to support the NAME management message. If the message is supported, the ECU manufacturer may limit the use of the message by not accepting it from CFs other than e.g. service tools or network interconnection units. ECU manufacturers might also require additional proprietary security verification processes before accepting a NAME management message. The ECU manufacturer may further limit the use of the message by only accepting changes to a subset of the fields of the NAME, e.g. the instance fields.

The CF commanding the changes to NAME fields shall correctly identify the source addresses of CFs being changed prior to using this command. Commands are directed to source addresses.

4.4.3.2 NAME management (NM) message

The NM message is used to manage the assignment of fields of the NAME of a CF during configuration of the network. The NM message contains 8 bytes of data and is sent as a PDU1 message. Depending on the NM control mode, the message is sent either to the global address or to a destination-specific source address of the CF to be modified.

As specified below, there are two main users and several uses of the message.

a) A commanding CF can

1) command a target CF to set a new pending NAME;

2) request the pending or current NAME from a target CF;

3) announce to one or more target CFs that they shall adopt their pending NAME;

4) request that a CF with a specified NAME transmit the address-claimed message with its current NAME.

b) A target CF shall

1) respond to requests for its pending or current NAME;

2) acknowledge (ACK) or negatively acknowledge (NACK) a command to change its pending NAME;

3) adopt its pending NAME as the current NAME and claim its current NAME on the network;

4) send an address-claimed message in response to a request for a matching NAME.

The NM control mode indicator is always sent in the least-significant four bits of byte 3 and indicates how the NM message is being used. The other parameter fields are used for some modes, but not all. When not used for a specific mode, the unused fields should be set to all 1's. Fields used for each mode are specified in Table 3 and in 4.4.3.3.

Transmission repetition rate:	As required
Data length:	8 bytes
Data page field:	0
Protocol data unit (PDU) format field:	147
PDU-specific field:	Depending on NM control mode: — Mode 0: SA of target CF — Modes 1-4: SA of commanding CF — Modes 5-7: SA of target CF, or the global address (FF_{16}) — Mode 8: The global address (FF_{16})
Default priority:	6
Parameter group number:	37632 (009300_{16})
Bytes 1 to 8	See Table 3 and Figure 3 Reserved and unused bit fields shall be set to all 1's

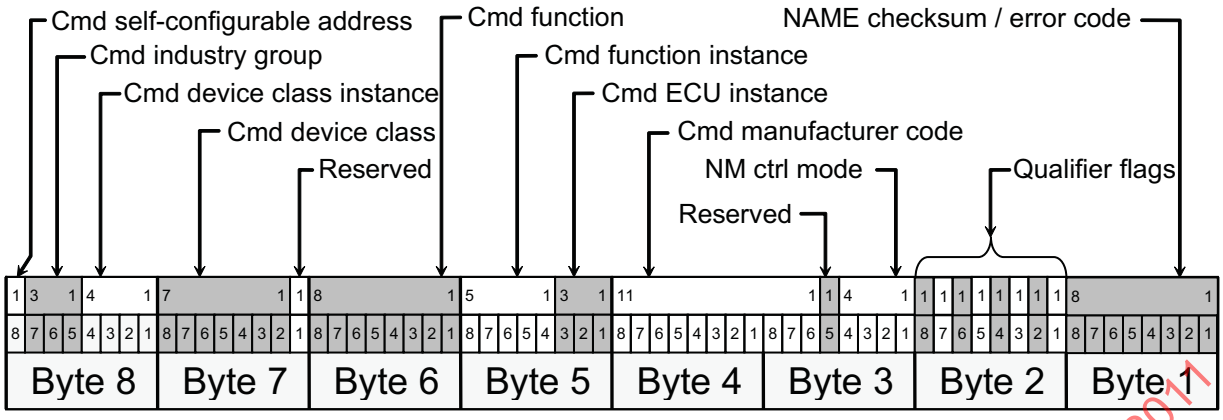


Figure 3 — NAME management message data bytes

Table 3 — NAME management message parameters

Parameter	SPN	Parameter used in modes	No. of bits	Byte No.	Byte ordering
Commanded self-configurable address[a]	5674	0, 1, 2, 3, 8	1	8	Bit 8
Commanded industry group[a,b]	5673		3		Bit 7 to bit 5
Commanded device class instance[a]	5672		4		Bit 4 to bit 1
Commanded device class[a,b]	5671		7	7	Bit 8 to bit 2
Reserved			1		Bit 1
Commanded function[a,b]	5670	0, 1, 2, 3, 8	8	6	Bit 8 to bit 1
Commanded function instance[a]	5669		5	5	Bit 8 to bit 4
Commanded ECU instance[a]	5668		3		Bit 3 to bit 1
Commanded manufacturer code[a,b]	5667		11	4	Bit 8 to bit 1 Most significant eight bits
				3	Bit 8 to bit 6 Least significant three bits
Reserved			1		Bit 5
NM control mode indicator	5666	All modes	4		Bit 4 to bit 1
Self-configurable-address-capable qualifier flag	5665	0, 4, 8	1	2	Bit 8
Industry group qualifier flag	5664		1		Bit 7
Device class instance qualifier flag	5663		1		Bit 6
Device class qualifier flag	5662		1		Bit 5
Function qualifier flag	5661		1		Bit 4
Function instance qualifier flag	5660		1		Bit 3
ECU instance qualifier flag	5659		1		Bit 2
Manufacturer code qualifier flag	5658		1		Bit 1
NAME checksum/error code	5657	0, 4	8	1	Bit 8 to bit 1

[a] These fields are populated if their corresponding qualifier flag is set to 0. If their qualifier flag is set to 1, the field is set to all 1's.

[b] See ISO 11783-1 for numerical values of industry groups, device classes, functions and manufacturer codes.

4.4.3.3 NAME management (NM) message parameters

4.4.3.3.1 NAME checksum/error code

When the NM control mode indicator is set to Mode 0 “set pending NAME”, NAME checksum is used as a check to ensure the NM message has been sent to the correct CF. It is a guard against the possibility that the SA of the target CF has been claimed by another CF through the address arbitration process since the commanding CF started the NAME change process. The NAME checksum byte shall contain the arithmetic sum of the 8 bytes of the target CF's original NAME truncated to the eight least significant bits.

Data length:	8 bits
Resolution:	1 bit
Data range:	0 to 255
Type:	Command
Suspect parameter number:	5657

When the NM control mode indicator is set to Mode 4 “NAME NACK”, it represents an error code sent by the target CF. The code values are as follows:

0	Security not satisfied. Different SA for adopt pending than for set pending.
1	Item(s) not allowed to change. Set qualifier flag to 1 for disallowed items.
2	Item conflict. Cannot perform function assigned, cannot perform as self-configurable-address-capable, etc. Set qualifier flag to 1 for disallowed items.
3	Checksum does not match.
4	Pending NAME not set.
5	Other.
6-254	Reserved.
255	Not available.

4.4.3.3.2 Qualifier flags

If the NM control mode indicator is set to Mode 0 “set pending NAME”, the qualifier flags are used to indicate whether the corresponding fields in the pending NAME of the target CF shall be changed. If a qualifier flag is set to 0, the corresponding field in the pending NAME shall be set to the value in the corresponding commanded parameter in the NAME management message. If a qualifier flag is set to 1, the corresponding field shall not be changed.

If the NM control mode indicator is set to Mode 4 “NAME NACK” and the error code is 1 or 2, then the qualifier flags are used to indicate disallowed items. The target CF shall set the qualifier flag to 1 if the corresponding parameter caused the error and to 0 if it did not cause the error. For error codes other than 1 and 2, this qualifier flag shall be set to 1.

If the NM control mode indicator is set to Mode 8 “request NAME address claim”, the qualifier flags are used to indicate whether the corresponding commanded parameter shall be used by the target CF to match the current NAME. If a flag is set to 0, the corresponding commanded parameter shall be used in the NAME match. If a qualifier flag is set to 1, the corresponding commanded parameter shall not be used in the NAME match.

For all other NM control modes, the qualifier flags are not applicable and shall all be set to 1.

Data length:	1 bit
Resolution:	1 bit
Data range:	0 to 1
Type:	Command
Suspect parameter number:	See Table 3

4.4.3.3.3 NM control mode indicator

4.4.3.3.3.1 General

This four-bit parameter is used to define the purpose of the NM message, as described in Subclauses 4.4.3.3.3.2 to 4.4.3.3.3.11.

Data length:	4 bits
Resolution:	1 bit
Data range:	0 to 15
Type:	Command
Suspect parameter number:	5666

4.4.3.3.3.2 Mode 0 — Set pending NAME

This form of the message is the command to the target CF at the destination address in the CAN identifier to change its pending NAME to the one contained in the message. All data fields of the message are required.

The “commanded” parameter fields are the new (i.e. commanded) NAME field values. These shall be qualified with the qualifier flags. A value of 0 in the qualifier flags indicates that the associated field shall be changed to the value in the corresponding parameter field in the message. A value of 1 indicates that the associated field shall remain unchanged.

The NAME checksum byte contains the arithmetic sum of the 8 bytes of the target CF's original NAME truncated to the eight least significant bits. This is used as a check to make sure the command message has been received by the correct CF. This check protects against the possibility of the SA having changed through the address arbitration process.

4.4.3.3.3.3 Mode 1 — Pending NAME

This form of the message is sent by the target CF and is a response to a “request for pending NAME”. The CF's pending NAME is contained in the “commanded” parameter fields. All “commanded” parameter fields of the NAME are required. The qualifier flags and NAME checksum are not used, so the qualifier flags shall be set to 1 and the checksum shall be set to all 1's. If the pending NAME has not been set or is not valid, the NACK message (Mode 4) shall be sent instead of this form of the message.

4.4.3.3.3.4 Mode 2 — Current NAME

This form of the message is sent by the target CF and is a response to a “request for current NAME”. The CF's current NAME is contained in the “commanded” parameter fields. All fields of the NAME are required. The qualifier flags and NAME checksum are not used and shall be set to all 1's.

4.4.3.3.3.5 Mode 3 — NAME ACK

This form of the message is sent by the target CF to indicate that the most recently received “set pending NAME” command has been successfully fulfilled. The CF's pending NAME is contained in the “commanded” parameter fields. All “commanded” parameter fields of the NAME are required. The qualifier flags and the NAME checksum are not used and shall be set to all 1's.

4.4.3.3.3.6 Mode 4 — NAME NACK

This form of the message is sent by the target CF to indicate that the most recently received “set pending NAME” command or “request pending NAME” command was not successful. The NM control mode indicator, error code and qualifier flags are the only valid fields in this form of the message. All other fields shall be set to all 1's.

4.4.3.3.3.7 Mode 5 — Request pending NAME

This form of the message is sent by the commanding CF and is a request for the target CF to respond with its "pending" NAME. The control mode parameter is the only valid field in this form of the message. All other fields shall be set to all 1's.

4.4.3.3.3.8 Mode 6 — Request current NAME

This form of the message is sent by the commanding CF and is a request for the target CF to respond with its "current" NAME. The control mode parameter is the only valid field in this form of the message. All other fields shall be set to all 1's.

4.4.3.3.3.9 Mode 7 — Adopt pending NAME

This form of the message is sent by the commanding CF and is a "trigger" command to the target CF (or all CFs with pending NAMEs if sent to the global address) to adopt their pending NAME as their current NAME and to initiate the address claim procedure with this new NAME. The control mode parameter is the only valid field in this form of the message. All other fields are set to all 1's. This form of the message may be sent to a specific SA or to the global address.

4.4.3.3.3.10 Mode 8 — Request NAME address claim

This form of the message is used to request that a CF, whose SA is unknown to the requester, send the address-claimed message, thus allowing the requester to determine the CF's SA. All or portions of the NAME can be specified in the request using the qualifier flags. This form of the message shall be sent to the global address.

If a CF receives this request and the indicated qualifier fields match its current NAME, it shall send its address claim using its current NAME. If a CF receives this request but it does not match the indicated fields of the its current NAME, it shall not send an address claim and shall not send the NACK form of the NAME management message.

4.4.3.3.3.11 Modes 9-15 — Reserved for future use

These modes are reserved by ISO for future use.

4.4.3.3.4 Commanded parameters

4.4.3.3.4.1 General

The use of the commanded parameters (SPN 5667 to 5674) (see Table 3) depends on the NM control mode indicator.

If the NM control mode indicator is set to Mode 0 "set pending NAME" and the qualifier flag corresponding to the commanded parameter is set to 0, then the commanding CF shall set the commanded parameter to the desired value. The target CF shall then use the commanded value for the corresponding field in its pending NAME. If a commanding CF sets a qualifier flag to 1, it shall set the corresponding commanded parameter to all 1's and the target CF shall not change the corresponding field in its pending NAME.

If a qualifier flag is set to 1 by the commanding CF, then the target CF shall not change the corresponding field in its pending NAME.

If the NM control mode indicator is set to Mode 1 "pending NAME", the target CF shall populate the commanded parameters with the corresponding fields of its pending NAME.

If the NM control mode indicator is set to Mode 2 "current NAME", the target CF shall populate the commanded parameters with the corresponding fields of its current NAME.

If the NM control mode indicator is set to Mode 3 “NAME ACK”, the target CF shall populate the commanded parameters with the corresponding fields of its pending NAME.

If the NM control mode indicator is set to Mode 8 “request NAME address claim” and the corresponding qualifier flag is set to 0, the commanding CF sets the commanded parameter to the value that it wishes to match in the target CF's current NAME. The target CF then uses this value in the match test against its current NAME. If a commanding CF sets a qualifier flag to 1, it shall set the corresponding commanded parameter to all 1's and the target CF shall ignore the commanded parameter when matching the NAME.

For all other modes, the commanded parameters shall be set to all 1's by the commanding CF and target CF.

4.4.3.3.4.2 Commanded manufacturer code

See Table 1 for the definition of manufacturer code.

Data length:	11 bits
Resolution:	1 bit
Data range:	0 to 2 047
Type:	Command
Suspect parameter number:	5667

4.4.3.3.4.3 Commanded function instance

See Table 1 for the definition of function instance.

Data length:	5 bits
Resolution:	1 bit
Data range:	0 to 31
Type:	Command
Suspect parameter number:	5669

4.4.3.3.4.4 Commanded ECU instance

See Table 1 for the definition of ECU instance.

Data length:	3 bits
Resolution:	1 bit
Data range:	0 to 7
Type:	Command
Suspect parameter number:	5668

4.4.3.3.4.5 Commanded function

See Table 1 for the definition of function.

Data length:	8 bits
Resolution:	1 bit
Data range:	0 to 254
Type:	Command
Suspect parameter number:	5670

4.4.3.3.4.6 Commanded device class

See Table 1 for the definition of device class.

Data length:	7 bits
Resolution:	1 bit
Data range:	0 to 126
Type:	Command
Suspect parameter number:	5671

4.4.3.3.4.7 Commanded self-configurable-address-capable

See Table 1 for the definition of self-configurable-address-capable.

Data length:	1 bit
Resolution:	1 bit
Data range:	0 to 1
Type:	Command
Suspect parameter number:	5674

4.4.3.3.4.8 Commanded industry group

See Table 1 for the definition of industry group.

Data length:	3 bits
Resolution:	1 bit
Data range:	0 to 7
Type:	Command
Suspect parameter number:	5673

4.4.3.3.4.9 Commanded device class instance

See Table 1 for the definition of device class instance.

Data length:	4 bits
Resolution:	1 bit
Data range:	0 to 15
Type:	Command
Suspect parameter number:	5672

4.4.3.4 NAME management procedures

4.4.3.4.1 NAME management message support

To determine if a CF supports the NM message, a commanding CF may send a request (PGN 59904) for the NM message. As specified in ISO 11783-3, CFs that do not support the requested message shall respond with the acknowledgement message PGN 59392 with the appropriate NACK control byte.

If the target CF supports the NM message, it shall send the NM message when requested. If it has a valid pending NAME, it shall set the mode indicator to “pending NAME” and shall set bytes 3 to 8 to those of the pending NAME. If it does not have a valid pending NAME, it shall set the mode indicator to “current NAME” and bytes 3 to 8 to those of the current NAME. This allows a method of querying for the support of the NM message and for a currently existing or pending NAME. This can be useful for a service tool or other ECUs trying to configure multiple devices.

If the NAME is successfully modified, the target CF has a “pending” NAME. While in this pending state, the target CF can still be transmitting messages using its current NAME. The pending NAME does not take effect until the unit responsible for configuring the network sends an NM message with the mode indicator set to

"adopt pending NAME". When this message is received, the target CF shall re-issue an address claim with its new NAME and successfully claim an address with that NAME before originating or resuming transmissions on the network.

The NAME management message has multiple uses. These uses are identified by a mode indicator parameter in the message (see 4.4.3.3.3).

4.4.3.4.2 Set pending NAME

A target CF, upon receiving a NAME management message with the "set pending NAME" mode and its own source address as the destination address, shall respond in one of two ways:

— The target CF may accept the commanded changes to fields of the NAME. These changes to the NAME, together with the unchanged portions of the NAME, become the pending NAME. The target CF shall respond by sending the NM message with the appropriate ACK mode indicator (see mode definitions in 4.4.3.3.3). The response shall include the pending NAME in bytes 3 to 8 and is sent to the SA of the commanding CF. The target CF shall use its current SA (the last address successfully claimed) when sending this message.

— The target CF may reject the commanded changes to the NAME by sending the NM message with the mode indicator for NACK and the error code field set to the most appropriate value (see 4.4.3.3.1 for error values). If the error value is "item not allowed" or "item conflict", the qualifier flags in byte 2 shall be set to 1 for fields that cannot change and 0 for fields that can change. The other data bytes of the message shall be set to all 1's.

4.4.3.4.3 Adopt pending NAME

The commanded NAME changes shall be stored temporarily by the target CF until the commanding CF completes all such commands and then sends the NM message with the mode indicator for "adopt pending NAME". The target CF with temporarily stored (pending) NAME shall adopt the pending NAME and perform the necessary "reset" of the CF, including the sending of the address-claimed message with the new NAME. Note that the NM message with the "adopt pending NAME" mode indicator may be sent to the global address. This enables the commanding CF to configure multiple CFs and then simultaneously activate all NAME changes.

4.4.3.4.4 Verifying NAME source address

The identity of the CF to be changed and its source address shall be verified prior to sending the NM message. A target CF can acquire a new SA through the address-claiming process at any time. Since the timing of this event relative to the commanding CF sending the NM message with the "set pending NAME" mode indicator is not synchronized, a method is required to prevent a CF with a newly acquired SA from being incorrectly commanded to a new NAME. To guard against this possible mismatch between SA and NAME, the "set pending NAME" mode of the NM message includes a checksum of all eight bytes of the original NAME of the intended recipient of the new NAME (see 4.4.3.3.1).

4.4.3.4.5 Rules for use of the NM message

The target CF shall check each field marked for change and ensure it can provide the indicated behaviour before accepting the change.

If this message is supported, it shall, as a minimum, allow the changing of the ECU instance and function instance.

Target CFs may accept "set pending" commands from any CF.

A target CF shall verify that the CF which sent the "adopt NAME" command is the same CF as the one which sent the most recent "set pending NAME" command that the target CF accepted.

4.4.4 Network-error management

4.4.4.1 General

Network-error management refers to the detection of certain addressing errors, for example the failure of a CF to secure an address. Other addressing errors, such as duplicate address claims or NAMEs, can be detected by a diagnostic tool using a request-for-address-claimed message.

4.4.4.2 Unable to claim address

If a CF attempting to claim an SA is unsuccessful, it shall send the cannot-claim-source-address message as described in 4.4.2.4 and continue to operate in accordance with 4.5.5.

4.4.4.3 Address violation

Address violation occurs when two CFs are using the same SA.

If a CF receives a message, other than the address-claimed message, which uses the CF's own SA, then the CF

— shall send the address-claimed message to the global address;

— shall also activate a diagnostic trouble code with SPN = 2000 + SA and FMI = 31 (see ISO 11783-12 regarding diagnostic trouble codes).

NOTE These are new requirements in this second edition of this part of ISO 11783.

4.5 Network initialization

4.5.1 Acquisition of a unique address

Following power-up and before originating any other communication, the CF shall acquire a unique address on the network.

CFs with self-configurable addresses shall use one of the following sequences to obtain an address.

a) Build an address table, as follows:

   1) Send a request-for-address-claimed message to the global address.

   2) Wait at least 250 ms + RT×D.

   3) The SA of all address-claimed messages received during the waiting period is stored.

   4) Send an address-claimed message claiming an unused address.

      The CF shall claim its initial address if this is not already claimed by another CF. If the initial address is already claimed, the CF shall try to claim another unused address.

b) Interrogate a single address, as follows:

   1) Send a request-for-address-claimed destination-specific message to the CF's initial address.

   2) Wait at least 250 ms + RT×D.

      If an address-claimed message, claiming the initial address, is received before the end of the waiting period, then the CF shall select a new initial address and repeat step 1).

3) Send an address-claimed message claiming the initial address.

NOTE 1 These are additional requirements in this second edition of this part of ISO 11783 for acquiring an address.

NOTE 2 While the sequences above minimize the risk of two CFs claiming the same address, they do not completely eliminate the risk. The requirements specified in 4.5.2 and 4.5.3 ensure that only valid addresses are used.

NOTE 3 The previous edition of this part of ISO 11783 specified 1,25 s instead of the 250 ms waiting period. When boot time is not critical, it is considered good practice to implement a waiting period longer than 250 ms.

The algorithm for selecting another initial address is proprietary to the CF, but the new address shall either be the CF's preferred address or an address in the range 128 to 247

CFs without self-configurable addresses may omit, from the sequences given above, the request for the address claimed, but shall nevertheless send the address-claimed message before originating any other communication.

It is recommended that CFs always send the request for the address claimed before claiming an address.

4.5.2 Address claim requirements

The following list comprises the main requirements for avoiding contention and for detecting and eliminating duplicate addresses during initialization:

a) The CF shall claim its own address when initializing and when responding to a command to change its NAME or address (in the latter instance, in confirmation of its acceptance of a commanded-address message). This ensures that each CF takes responsibility for obtaining a valid address and correctly arbitrates for an address if its claim has not yet been received by another CF.

b) The destination address for an address-claimed message shall be the global address (255), in order that the transmitting CF's claim is announced to all other CFs on the network. (It should be noted that this is an exception to the requirements of ISO 11783-3.)

c) A CF shall be able to differentiate between address-claimed messages it receives from other CFs and those which it itself sent.

d) No CF shall begin, or resume, transmission on the network until 250 ms after it has successfully claimed an address (see Figure 4). This does not apply when responding to a request for an address claimed.

4.5.3 Other basic requirements for initialization

A CF shall respond to a request-for-address-claimed message directed to the global address with either an address-claimed message or, if the claim is unsuccessful, a cannot-claim-source-address message.

The CF shall not respond to a request-for-address-claimed message (as required above) if an address claim has not been attempted.

A CF shall respond to a request-for-address-claimed message when the destination address is the same as the CF's address and shall transmit its response to the global address (255).

A CF shall transmit an address claim if it receives an address-claimed message with an SA matching its own and if its own NAME has a priority higher (lower value) than the claim received.

If a CF NAME has a lower priority (higher value) than the NAME in a received address-claimed message, it shall discontinue using the address. It shall then transmit a cannot-claim-source-address message or attempt to claim another address (see 4.5.1).

A non-configurable, service-configurable or command-configurable address CF that is unable to use a particular address shall transmit a cannot-claim-source-address message.

A self-configurable address CF that cannot use the particular address it is attempting to claim shall select another address and attempt to claim it (see 4.5.1).

A CF that has previously communicated with another CF unable to claim a particular address shall be capable of detecting when that other CF has been "disabled" by monitoring its cannot-claim-source-address message as well as the address-claimed message of the higher-priority CF that impeded the claim.

Service tools and, in certain systems, bridges are expected to detect and resolve address-claim failures. Such tools shall be able to monitor the cannot-claim-source-address message and report the problem to its operator.

4.5.4 Message sequences

4.5.4.1 Initialization without contention

The initialization sequence of a CF claiming an address which no other CF is claiming is shown in Figure 4.

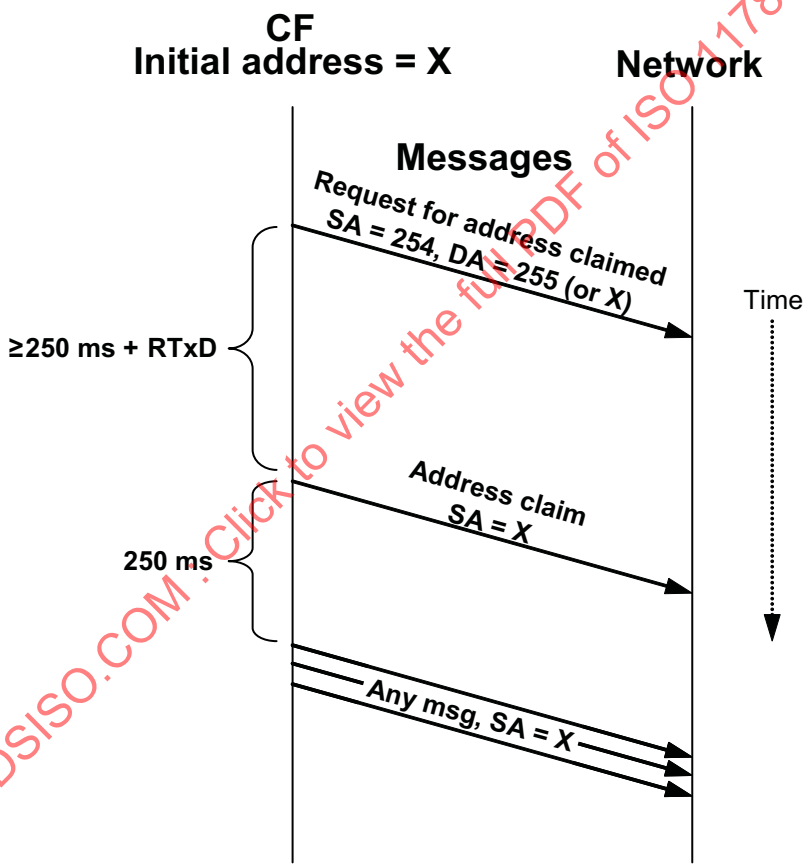


Figure 4 — Initialization of a CF claiming an SA without contention

If two self-configurable CFs have the same initial address, one of the following three scenarios will occur during initialization:

1) one CF will complete the 250 ms + RT×D before the other;
2) both CFs will complete the 250 ms + RT×D at the same time but one will send the address claim slightly earlier than the other;
3) both CFs will complete the 250 ms + RT×D at the same time and send the address claim at the same time.

In case 1, the address will be resolved without contention, as shown in Figure 5.

In case 2, address claim prioritization will resolve the addresses (see 4.5.4.2).

In case 3, a CAN error is generated. This is resolved as described in 4.5.4.3.

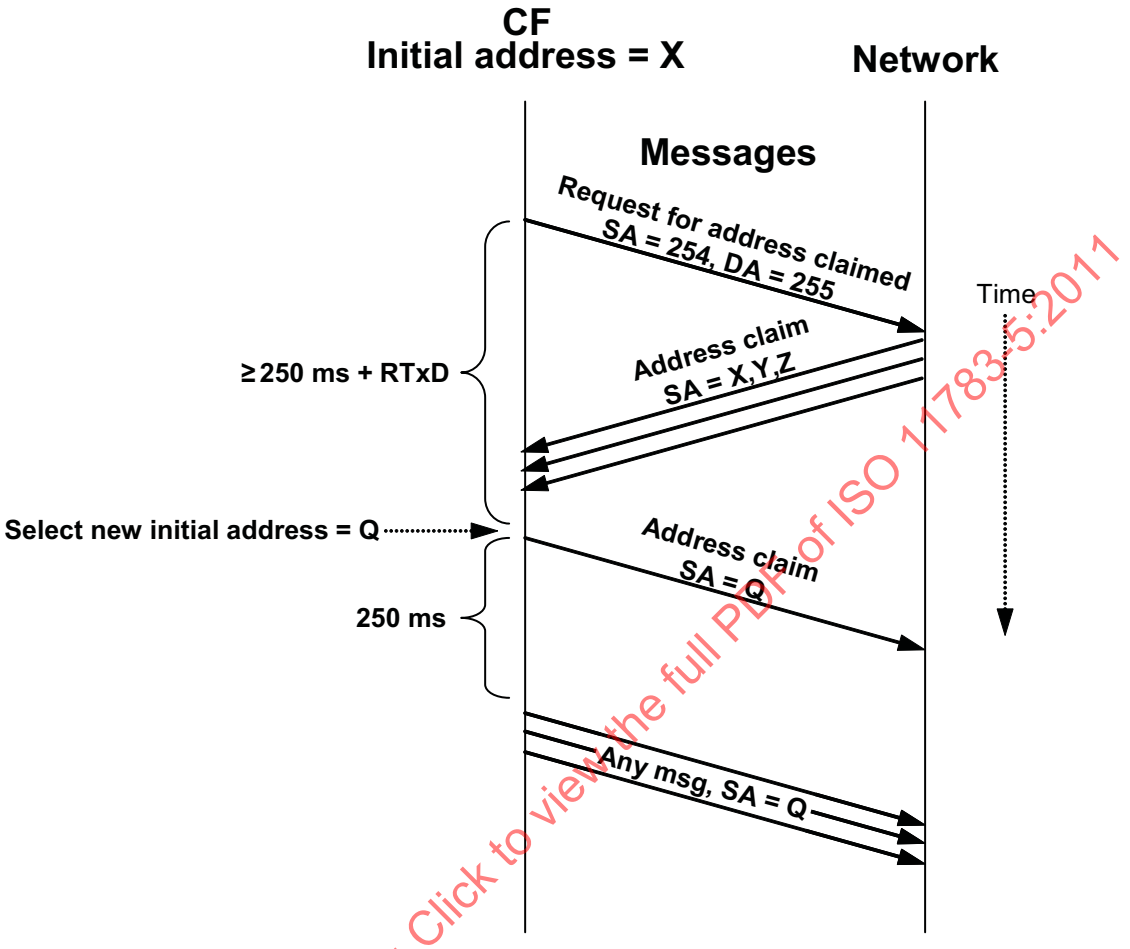


Figure 5 — Resolving initial addresses without contention

4.5.4.2 Address claim prioritization

Where a single address is contested by two CFs, priority shall be given to the CF with the NAME of lower numerical value and thus higher priority. This NAME shall be treated as an 8-byte value, with the most significant bit, i.e. the self-configurable address bit, determining the numerical value. Although necessitating comparison of the 8-byte NAMEs in the respective address-claimed-message data fields of the contending CFs, this eliminates ambiguity from the address-claiming process.

EXAMPLE Two CFs (CF A and CF B) with the same function both request the same address. CF A is function instance 0 and therefore it has a lower absolute value NAME and obtains the address.

The message sequence which will solve the address contention depends on the address configuration capability of the CFs involved. The figures below show the sequences for solving address contention between two self-configurable address CFs (see Figure 6), a non-configurable and a self-configurable address CF (see Figure 7) and two non-configurable address CFs (see Figure 8).