1 Introduction

Sections in this document may be left intentionally blank if no additional commentary is provided.

1.1 Served Use Cases

- Add stronger error detection to DCC packets with lengths greater than 6 bytes (inclusive of X-OR checksum)
- New advanced control commands
- Automatic discovery of decoders
- Bulk transfer of large amounts of data

1.2 Unserved Use Cases

2 Annotations to the Standard

2.1 General

2.1.1 Introduction and Intended Use (Informative)

2.1.2 References

- S-9.7.3 Message Network, which contains harmonized error codes
- S-9.7.4.2, Memory Configuration, which contains harmonized error codes
- S-9.2.1.1 Advanced Extended Packet Formats

2.1.3 Terminology

2.1.4 Requirements

2.2 Packet Framing

2.2.1 Error Detection

The DCC packet length limit of 6 bytes (inclusive of X-OR checksum) is long established in S-9.2.1. This limit exists primarily for two reasons:

1. DCC bandwidth is limited, and ensures that as many diverse packets can be sent in a given time period
2. The probability of the X-OR checksum correctly identifying an error remains reasonably high.

In order to implement the new features in this standard, longer than 6-byte packets are highly desired. Therefore, a CRC-8 checksum has been added for packets resulting in a greater than 6-byte length. The goal is to keep the probability of correctly identifying an error reasonably high despite these longer packet lengths.

For the shortest possible packet requiring the addition of the CRC-8 (8-bytes inclusive of CRC-8 and X-OR checksums), the added bandwidth overhead is approximately 12.5%. The exact percentage overhead will vary depending on the mix of 1's and 0's, and goes down with longer packet lengths.

RCN-218 further requires that both "edges / bit halves" of the DCC signal be evaluated and discarded if either evaluation results in error. The NMRA agrees that this technique may serve to improve message reception integrity. However, the NMRA Standard remains silent on this requirement largely because there is no agreed-upon engineering model available that can be used in NMRA Conformance Warrant evaluation. This technique is recommended to be used, but is not required by the NMRA Standard or evaluated for the purposes of NMRA Conformance.

Should an engineering model that can be used to evaluate Conformance become available, the NMRA may reevaluate whether a requirement should be added to the Standard.

Packet length restrictions are nuanced. Longer packet lengths often improve bandwidth utilization efficiency. However, longer packet lengths increase the amount of time between two back-to-back packets. This can become a concern when there is a necessary sequence of decoder packets addressed to a single decoder. This is often the case in layout automation where the System is ramping the speed of one or more locomotives in a centralized fashion.

In consideration of the goals and concerns, command types that are intended for normal operations should be defined with a maximum packet length of 16 bytes, while commands intended for configuration may be defined with a maximum packet length of 32 bytes, including the 253/254 address and the checksum byte(s).

WriteBlock is an example of a command that is intended for configuration, and has a maximum packet length of 32 bytes. Addressed S-9.2.1 Chained is an example of commands (packet type) that have a maximum packet length of 16 bytes.

2.2.2 Feedback

2.2.2.1 Address Partition 253

2.2.2.2 Address Partition 254

2.2.2.3 Encoding, Padding, and Alignment

2.2.2.4 Variable Length Feedback

2.2.3 Acknowledgement

2.2.4 Frequency

Unless explicitly noted otherwise, messages in this standard are not intended to be refreshed periodically. This is possible because of the requirement that all non-broadcast messages be acknowledged. When an acknowledgement is not received, the standard is intentionally undefined for the number of times or frequency that the System may repeat a packet. However, it is assumed that the System will not retry an unacknowledged packet indefinitely.

Normally S-9.2 allows a decoder to ignore any DCC packets directly following a previously decoded packet addressed to it for which the time between the previously decoded packet end bit and the preamble of the next packet is less than 5 milliseconds. However, this is not the case for the messages defined in this standard.

2.2.5 Sequenced Messages

Sequenced **Get Data** Messages are used to provide one specifically addressed Decoder multiple feedback cutouts in order to transmit a larger amount of data to the System. The **Get Data** message encoding was chosen to be as short as possible in order to maximize the number of feedback cutouts per second. For this reason the Get Data message does not contain any address information. There is still a requirement that only one Decoder may transmit in any one RailCom cutout window, and Decoders implementing this Standard have to operate a simple state machine that defines whether they are selected to transmit in the cutout.

The sequence looks as follows:

1. Command message addressed to one specific decoder to start the sequence
2. **Get Data Start** message
3. **Get Data Continue** message
4. **Get Data Continue** message
5. … as many repetitions as needed.

The current standard defines **Select (ReadBlock)** and **ReadBlock** as the two commands that may start such a sequence. Further standards or further revisions of this standard may define additional commands.

The System may interleave other DCC messages after the **Get Data Start** and between **Get Data Continue** messages, but no messages of an alternate track protocol. This requirement is necessary so that a Decoder can clearly decide whether it has lost connection to the track. There may be no other message on the track between the Command message 1) and the **Get Data Start** message 2).

The state machine looks as follows, to be evaluated at each packet end:

```
if packet is not DCC or packet timeout:
    state_ = OFF
if packet checksum failed:
    state_ = OFF
if packet is Get Data Start:
    if state_ is STARTING:
        state_ = ENABLED
    else:
        state_ = OFF
else if state_ is STARTING:
    state_ = OFF
if state_ is ENABLED and (packet is Get Data Start or Get
Data Cont):
    transmit in RailCom channel 1 + channel 2
if ((packet is Get Address Info) or (packet is Memory Space
Read Short)) and (packet address is me):
    state_ = STARTING
```

The last condition of this state machine can be evaluated during or after the cutout, so long as the evaluation completes before the subsequent DCC packet end bit arrives (i.e., in ~4 msec).

The goal of this state machine is to shut off using the feedback cutout after a **Get Data** message in all of the following conditions:

when a different Decoder is addressed using a known read command;

when a different Decoder is addressed using a read command unknown to the Decoder (both of these cases are recognized by the **Get Data Start** command arriving in the wrong state);

when the Decoder loses track contact and a packet could have been missed during this time that designates a different Decoder to transmit in cutouts after **Get Data** packets.

2.2.6 Error Codes

The Error Codes described in this section are harmonized with NMRA S-9.7.3 and S-9.7.4.2.

2.3 Extended Address Format

2.4 Command Types in Address Partition 253

RCN-218 had a carefully evaluated mode/address scheme allowing for an easy decision how the decoder should behave in the following cutout. There have been several sessions with decoder vendors until all agreed on this scheme. It is recommended to put all addressed transactions with a channel 2 response only under a different prefix (253). It is still possible to open the sequenced transfer mode (in 254) for transfers initiated by 253 commands.

2.4.1 Addressed and Addressed Continue

2.4.2 Addressed Control

2.4.3 Addressed S-9.2 / S-9.2.1 Chained

S-9.2.1 allows for a single addressed DCC packet to contain multiple commands, which it refers to as instruction-bytes, within a single DCC packet frame so long as the total frame length remains less than 6 bytes inclusive of the X-OR byte. In some instances, this technique can be used to make more efficient use of the DCC bandwidth.

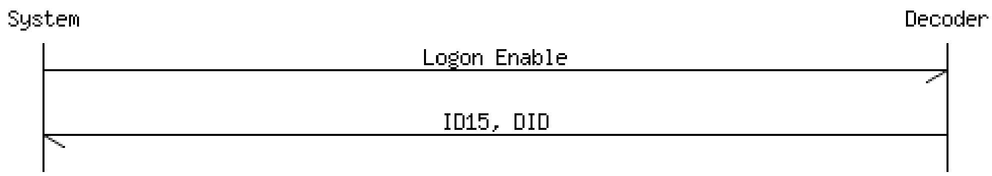
Unfortunately, this feature of the standard has not been well understood by many decoder manufacturers, and therefore most DCC Systems do not take advantage of this technique. Adding support here for Addressed S-9.2 / S-9.2.1 Chained messages provides an opportunity to revive this useful technique by using the **Data Space Info** as a means for the System to discover that it is explicitly supported by the Decoder.

2.5 Command Types in Address Partition 254

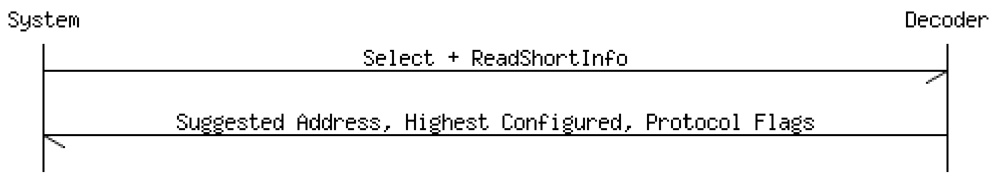
2.6 Logon

2.6.1 Procedure

2.6.1.1 Enumeration

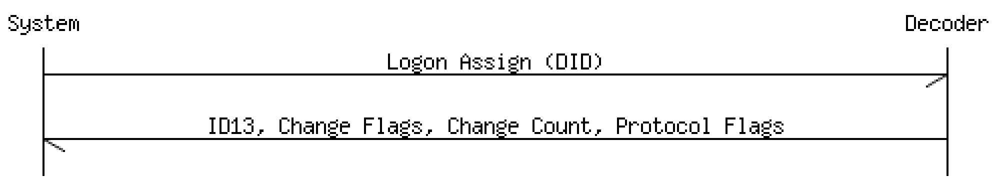


2.6.1.2 Confirmation



2.6.1.3 Assignment

The algorithm by which the System chooses a DCC address to assign is intentionally undefined. However, it is reasonable for a System to take into account the last DCC address that was assigned to the decoder DID either as reported by the decoder itself, or cached within the command station's non-volatile memory.



2.6.1.4 Configuration Discovery

Because the bandwidth required to transfer this information is considerable, it is recommended that Systems keep a cache of previously discovered configuration which is only refreshed when the decoder reports that the configuration is stale (via the feedback to **Logon Assign**).

2.6.1.5 CID

The CID is chosen by the product manufacturer. It should have a reasonably high probability of uniqueness among all Systems produced by a given manufacturer and among all other manufacturers. The Standard intentionally does not prescribe a method to achieve this. One possible way of achieving this is to use the following process:

1. Assign a Unique 44-bit "Decoder" ID (DID) to the System.
2. Generate a CRC-8 using the DID assigned to the System, and use the resulting CRC-8 for the first byte.
3. Generate a CRC-8 using the DID assigned to the System using the result of the first calculator as the CRC-8 seed, and use the resulting CRC-8 for the second byte.

It is recommended that the CID not be chosen sequentially between different System instances manfuactured.

2.6.2 Logon Commands

2.6.2.1 Logon Enable

The frequency of transmission is chosen to balance the need for a decoder to have an opportunity to receive a **Logon Enable** packet relatively quickly without consuming an unreasonable amount of DCC bandwidth. It is recommended to send this command more frequently up on system startup.

2.6.2.2 Select

2.6.2.2.1 ReadShortInfo

2.6.2.2.2 ReadBlock

[Balazs Racz to add commentary about different implementation options for ensuring an adequate number of Get Data packets are sent]

2.6.2.2.3 Set Decoder Internal Status

The primary purpose is to clear the change flags as an indication to a System that discovered information which has been previously cached is still valid upon subsequent Logons.

2.6.2.3 Get Data

2.6.2.3.1 Get Data Start

2.6.2.3.2 Get Data Continue

2.6.2.3.3 Get Data Feedback

2.6.2.4 Set Data

2.6.2.5 Logon Assign

It may be reasonable for a System implementation to provide the user an option to commit the assigned session specific address to a Decoder's non-volatile configuration. In the case of CV17 / CV18 or CV1(513) / CV9(521) pairs, the S-9.2.1 **POM Short Form** instruction should be used in order to ensure the two CV pairs are assigned atomically.

Presently the change flags in the feedback definition are mobile Decoder specific. In the future, it may be necessary to have overlapping flag definitions specific to accessory Decoders.

2.6.3 System Behavior

2.6.3.1 Registration

After sending a few **Logon Enable** messages upon startup and detecting collisions, it may be reasonable for the system to proactively send **Select** messages to Decoders known from a prior operating session before transitioning into the back-off algorithm. This may serve to reduce the total number of collisions at startup and reduce the overall time required for all decoders to logon.

A System may optionally go through the Configuration Discovery process for any decoders that become known to the system. How the System prioritizes the reading of configuration is intentionally undefined. A reasonable methodology would be to start with decoders that are not previously known to the System, then decoders that are previously known but are reporting a configuration change, then decoders that are previously known but do not report a configuration change.

A System may use any read method (**POM**, **XPOM**, **Select + ReadBlock**, **ReadBlock**, or **ReadBackground**) so long as it is reported as supported by the decoder. System designers are encouraged to use a read method that is the most efficient use of bandwidth for transferring data.

2.6.3.2 Configuration Discovery

2.6.4 Decoder Behavior

2.6.4.1 Startup

The waiting period (700 milliseconds) is chosen to balance the need to give a decoder at least two opportunities to receive a **Logon Enable** packet while not having to wait too long to fall back on a previously assigned DCC address.

The way in which an error condition is displayed is intentionally undefined. It is up to the manufacturer to define the method of indication. One possible implementation could be to Flash one or more function outputs (lights).

2.6.4.2 Back-off

The primary reason that a decoder will not receive a **Select** confirmation after an attempted registration is a collision between two or more decoders responding in the feedback channel. The back-off algorithm is designed so that some decoders can begin responding without collision.

2.6.4.3 CV19 Consisting Behavior

If a decoder uses its CV19 consist address upon **Logon Assign**, it could result in undesirable and confusing behavior. This is because the user may not know or expect that the locomotive is consisted. It is also possible that the programmed consist address is in conflict with an assigned address or a known permanent address. It is for these reasons that the CV19 consist address is ignored before, during, and after **Logon Assign**. The System will know if the Decoder is in a CV19 consist from the **Logon Assign** feedback. It is up to the System implementation to decide what to do with this information, including reading the assigned CV19 consist address as a clue on what to do next.

If the System wants to Decoder to use CV19 consisting, it must reaffirm its CV19 address. It is intentionally unspecified what address the System should program into CV19. It may program the existing CV19 consist address, or it may choose another consist address to program.

There is a pending proposal for a way of assigning a session based consist address with Logon which may be considered for future revisions of this Standard. The CV19 behavior currently described within the Standard is designed to be forward compatible with the proposal as of this writing.

2.7 Data Spaces

2.7.1 WriteBlock

When compared to **POM**, a significant difference is that a **POM** write requires two identical packets to be received by the decoder before a write is allowed to be executed. There is intentionally no such requirement here. The CRC-8 checksum on the Write provides the necessary protection against erroneous writes.

2.7.1.1 WriteBlock Feedback

2.7.1.2 WriteBlock Continue

2.7.2 ReadBackground

For decoders that are not on a handheld right now background read is a better option as it takes no dedicated bandwidth. The System can optionally handle multiple **ReadBackground** operations simultaneously.

2.7.3 ReadBlock

For a currently controlled decoder, it is desirable to use the "short read" commands because they are faster. However, only one **ReadBlock** can be active at a time.

2.7.3.1 ReadBlock Errors

The Get Data commands from the 254 address space are required to complete the ReadBlock transaction. Therefore address space 254 must be enabled (CV28, bit 7) in order for the ReadBlcok transaction to complete.

2.7.4 Data Space Definitions

Suggestions for future data spaces include:

Name	Size (bytes)	Description
Product Name	16	Manufacturer defined product designation (UTF-8 format, 0x00 padded)
Long Name	31	User defined [long] name (UTF-8 format, 0x00 padded)
Display Text	31	User defined message (UTF-8 format, 0x00 padded)

2.7.4.1 Extended Capabilities

2.7.4.2 Data Space Info

2.7.4.3 Short GUI

2.7.4.4 Configuration Variables (CV's)

2.7.4.5 [Indexed] CV Space Overlay Mapping

Supporting the **ReadBlock** or **ReadBackground** sequence requires additional state machine complexity both in the System and the Decoder. For this reason, the Data Spaces are also mapped to CV address space. This provides a System or Decoder manufacturer the option to read this information without the additional state machine complexity of **ReadBlock** or **ReadBackground**.

Supporting **ReadBlock** or **ReadBackground** in the System and Decoder provides for much faster transfer of read data compared to **POM** or **XPOM**.

Prepending a length byte to the Data Space data allows for the System to avoid unnecessarily reading superfluous information.

The table mapping is intended to be in harmony with S-9.2.2.

2.8 Manufacturer Specific Command Space

Ordinarily, the DCC address/command space is very limited. There is not enough space for every manufacturer to define their own commands without coordinating with the wider DCC community or running into future conflict.

With the addition of the 253 address space, there is now the possibility of much larger addressed DCC packet lengths. Longer packet lengths provide adequate space for the 12-bit manufacturer ID preceding the "interesting" command payload. Prefixing a 12-bit manufacturer ID to a manufacturer defined command prevents any possibility of conflict between manufacturers.

As explained in Section 2.2.1 above, it is normally preferred to keep packet lengths to a maximum of 16 bytes, including the 253 address and the checksum byte(s).

The Standard intentionally does not require manufacturers to share information about commands they define in this manufacturer specific space. Manufacturers are still highly encouraged to share their command definitions publicly. The NMRA DCC WG may decide to adopt concepts developed in a manufacturer specific address/command space into a standardized address/command space. It is recommended that manufacturers create their implementations with this in mind.

The Standard allows manufacturers to use this command space in any way that they choose. This could include, but is not limited to:

1. Manufacturing test
2. Proprietary System/Decoder capabilities
3. Experimental System/Decoder capabilities
4. Encapsulation of another protocol

3 Document History

Date	Description
	First Revision

4 Table of Contents

1 Introduction 1
1.1 Served Use Cases 1
1.2 Unserved Use Cases 1
2 Annotations to the Standard 1
2.1 General 1
2.1.1 Introduction and Intended Use (Informative) 1
2.1.2 References 1
2.1.3 Terminology 1
2.1.4 Requirements 1
2.2 Packet Framing 1
2.2.1 Error Detection 1

2.2.2 Feedback 2
2.2.3 Acknowledgement 2
2.2.4 Frequency 2
2.2.5 Sequenced Messages 3
2.2.6 Error Codes 4
2.3 Extended Address Format 4
2.4 Command Types in Address Partition 253 4
2.4.1 Addressed and Addressed Continue 4
2.4.2 Addressed Control 4
2.4.3 Addressed S-9.2 / S-9.2.1 Chained 4
2.5 Command Types in Address Partition 254 5
2.6 Logon 5
2.6.1 Procedure 5
2.6.2 Logon Commands 6
2.6.3 System Behavior 6
2.6.4 Decoder Behavior 7
2.7 Data Spaces 7
2.7.1 WriteBlock 7
2.7.2 ReadBackground 8
2.7.3 ReadBlock 8
2.7.4 Data Space Definitions 8
2.8 Manufacturer Specific Command Space 9
3 Document History 9
4 Table of Contents 9

Important Notices and Disclaimers Concerning NMRA Standards Documents

The Standards (S), Recommended Practices (RP), Technical Note (TN), and Technical Information (TI) documents of the National Model Railroad Association ("NMRA Standards documents") are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning NMRA Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of NMRA Standards Documents

NMRA Standards documents are developed within the Standards and Conformance Department of the NMRA in association with certain Working Groups, members, and representatives of manufacturers and sellers. NMRA develops its standards through a consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. NMRA Standards documents are developed by volunteers with modeling, railroading, engineering, and industry-based expertise. Volunteers are not necessarily members of NMRA, and participate without compensation from NMRA.

NMRA does not warrant or represent the accuracy or completeness of the material contained in NMRA Standards documents, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard or recommended practice, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, NMRA disclaims any and all conditions relating to results and workmanlike effort. In addition, NMRA does not warrant or represent that the use of the material contained in NMRA Standards documents is free from patent infringement. NMRA Standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of NMRA Standards documents is wholly voluntary. The existence of an NMRA Standard or Recommended Practice does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the NMRA Standards documents. Furthermore, the viewpoint expressed at the time that NMRA approves or issues a Standard or Recommended Practice is subject to change brought about through developments in the state of the art and comments received from users of NMRA Standards documents.

In publishing and making its standards available, NMRA is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is NMRA undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any NMRA Standards document, should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given NMRA Standards document.

IN NO EVENT SHALL NMRA BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD OR RECOMMENDED PRACTICE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

NMRA's development of NMRA Standards documents involves the review of documents in English only. In the event that an NMRA Standards document is translated, only the English version published by NMRA is the approved NMRA Standards document.

Official Statements

A statement, written or oral, that is not processed in accordance with NMRA policies for distribution of NMRA communications, or approved by the Board of Directors, an officer or committee chairperson, shall not be considered or inferred to be the official position of NMRA or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of NMRA.

Comments on Standards

Comments for revision of NMRA Standards documents are welcome from any interested party, regardless of membership. However, **NMRA does not provide interpretations, consulting information, or advice pertaining to NMRA Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since NMRA standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, NMRA, its departments, Working Groups or committees cannot provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, NMRA does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to NMRA Standards documents may request participation in the relevant NMRA working group.

Laws & Regulations

Users of NMRA Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any NMRA Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. NMRA does not, by the publication of NMRA Standards documents, intend to urge action that is not in compliance with applicable laws, and NMRA Standards documents may not be construed as doing so.

Copyrights

NMRA Standards documents are copyrighted by NMRA under US and international copyright laws. They are made available by NMRA and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of modeling, structural and engineering practices and methods. By making NMRA Standards documents available for use and adoption by public authorities and private users, NMRA does not waive any rights in copyright to the NMRA Standards documents.

IMPORTANT NOTICE

NMRA Standards documents do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other systems, devices or networks. NMRA Standards documents development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of NMRA Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.