MIL-STD-188-220
7 May 1993

MILITARY STANDARD

INTEROPERABILITY STANDARD FOR DIGITAL MESSAGE TRANSFER DEVICE SUBSYSTEMS

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

AMSC N/A

AREA TCSS

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

FOREWORD

Originally, Military Standard -188 (MIL-STD-188) covered technical standards for tactical and long-haul communications. It later evolved through revisions (MIL-STD-188A, MIL-STD-188B) into a document applicable to tactical communications only (MIL-STD-188C).

The Defense Communications Agency (DCA), now the Defense Information Systems Agency (DISA), published DCA circulars (DCACs). These DCACs promulgated standards and engineering criteria that applied to the long-haul Defense Communications System (DCS) and to technical support of the National Military Command System (NMCS).

As a result of a Joint Chiefs of Staff (JCS) action, standards for all military communications are now being published in a MIL-STD-188 series. The MIL-STD-188 series is subdivided into a MIL-STD-188-100 series, which covers common standards for tactical and long-haul communications; a MIL-STD-188-200 series, which covers standards for tactical communications only; and a MIL-STD-188-300 series, which covers standards for long-haul communications only. Ultimately, the -200 and -300 series will be absorbed into the -100 series.

This MIL-STD shall be used for all inter- and intra-Department of Defense (DoD) digital message transfer devices (DMTDs). The MIL-STD contains technical parameters for the data communications protocols that support DMTD interoperability. It provides mandatory system standards for planning, engineering, procuring, and using DMTDs in tactical digital communications systems used in the Fire Support mission function area.

This MIL-STD is approved and shall be used by the Office of the Secretary of Defense, the military departments, the JCS, the unified and specified commands, DoD agencies, and DoD field activities to ensure interoperability and compatibility in accordance with DoD Instruction 5000.2, dated 23 February 1991.

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this MIL-STD should be addressed to:

Director
Joint Interoperability and Engineering Organization
ATTN: TBBC
Fort Monmouth, New Jersey 07703-5613

by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this MIL-STD or by letter.

CONTENTS

PARAGRAPH		PAGE
1.	SCOPE	1
1.1	Purpose	1
1.2	Scope	1
1.3	Application guidance	1
1.4	System standards and design	1
1.5	Tailoring	1
2.	APPLICABLE DOCUMENTS	3
2.1	Government documents	3
2.1.1	Specifications, standards, and handbooks	3
2.1.2	Other Government documents, drawings, and publications	3
2.2	Non-Government documents	4
2.3	Order of precedence	5
3.	DEFINITIONS	7
3.1	Definitions of terms	7
3.2	Abbreviations and acronyms	7
4.	GENERAL REQUIREMENTS	9
4.1	Digital message transfer device	9
4.2	Interoperability	9
4.3	Framework	10
4.4	DMTD capabilities	11
5.	DETAILED REQUIREMENTS	13
5.1	Physical layer	13
5.1.1	Transmission channel interfaces	13
5.1.1.1	Non-return-to-zero interface	13
5.1.1.1.1	Waveform	13
5.1.1.1.2	Transmission rates	13
5.1.1.1.3	Operating mode	13
5.1.1.2	Frequency-shift keying interface for voice frequency channels	13
5.1.1.2.1	Waveform	13
5.1.1.2.2	Transmission rates	14
5.1.1.2.3	Operating mode	14
5.1.1.3	Frequency-shift keying interface for single-channel radio	14
5.1.1.3.1	Waveform	14
5.1.1.3.2	Transmission rates	14
5.1.1.3.3	Operating mode	14
5.1.1.4	Conditioned diphase interface	14
5.1.1.4.1	Waveform	14
5.1.1.4.2	Transmission rates	14
5.1.1.4.3	Operating mode	14

CONTENTS (Continued)

PARAGRAPH		PAGE
5.1.1.5	Differential phase-shift keying interface for voice frequency channels	15
5.1.1.5.1	Waveform	15
5.1.1.5.2	Transmission rates	15
5.1.1.5.3	Operating mode	15
5.2	Physical-layer protocol	15
5.2.1	Physical-layer protocol data unit	15
5.2.1.1	Communications security synchronization and postamble	15
5.2.1.2	Bit synchronization field	17
5.2.1.3	Transmission synchronization field	17
5.2.1.3.1	Frame synchronization subfield	17
5.2.1.3.2	Transmission word-count subfield	18
5.2.1.4	Data field	18
5.2.1.5	COMSEC postamble	18
5.2.2	Keytime delay	18
5.2.3	Net busy indication	18
5.2.4	Physical-layer to upper-layer instructions .	18
5.3	Data-link layer	19
5.3.1	Net access control	19
5.3.2	Types of procedures	19
5.3.2.1	Types of operation	19
5.3.2.1.1	Type 1 operation	20
5.3.2.1.2	Type 2 operation	20
5.3.2.2	Command and response features	20
5.3.3	Data-link frame	20
5.3.3.1	Types of frames	20
5.3.3.1.1	Unnumbered frame	20
5.3.3.1.2	Information frame	20
5.3.3.1.3	Supervisory frame	21
5.3.3.2	Data-link frame structure	21
5.3.3.2.1	Flag sequence	21
5.3.3.2.2	Address fields	22
5.3.3.2.2.1	Address format	22
5.3.3.2.2.2	Addressing convention	22
5.3.3.2.2.2.1	Source and destination	23
5.3.3.2.2.2.1.1	Source address	23
5.3.3.2.2.2.1.2	Destination address(es)	23
5.3.3.2.2.2.2	Types of addresses	23
5.3.3.2.2.2.2.1	Reserved address	23
5.3.3.2.2.2.2.2	Special addresses	23
5.3.3.2.2.2.2.3	Individual addresses	24
5.3.3.2.2.2.2.4	Group multicase address	24
5.3.3.2.2.2.2.5	Unique and group multicase addresses mixed .	24
5.3.3.2.2.2.2.6	Global multicase addressing	24
5.3.3.2.2.3	Mapping	24
5.3.3.2.3	Control field	25

CONTENTS (Continued)

PARAGRAPH PAGE

5.3.3.2.3.1 Type 1 operations 25
5.3.3.2.3.2 Type 2 operations 25
5.3.3.2.3.3 Poll/final bit 25
5.3.3.2.3.4 Sequence numbers 30
5.3.3.2.4 Information field 30
5.3.3.2.5 Frame check sequence 30
5.3.3.3 Data-link PDU construction 31
5.3.3.3.1 Order-of-bit transmission 31
5.3.3.3.2 Zero-bit insertion algorithm 31
5.3.4 Operational parameters 31
5.3.4.1 Type 1 operational parameters 31
5.3.4.2 Type 2 operational parameters 32
5.3.4.2.1 Modulus 32
5.3.4.2.2 PDU-state variables and sequence numbers . . 32
5.3.4.2.2.1 Send-state variable V(S) 32
5.3.4.2.2.2 Send-sequence number N(S) 32
5.3.4.2.2.3 Receive-state variable V(R) 32
5.3.4.2.2.4 Receive sequence number N(R) 32
5.3.4.2.3 Poll/final (P/F) bit 33
5.3.4.2.3.1 Poll-bit functions 33
5.3.4.2.3.2 Final-bit functions 33
5.3.5 Commands and responses 33
5.3.5.1 Type 1 operation commands and responses . . 34
5.3.5.1.1 Unnumbered information command 34
5.3.5.1.2 Unnumbered receive-ready command 34
5.3.5.1.3 Unnumbered receive-no-ready command 34
5.3.5.1.4 Exchange identification command 34
5.3.5.1.5 Test command 35
5.3.5.1.6 Unnumbered receive-ready response 35
5.3.5.1.7 Exchange identification response 35
5.3.5.1.8 Test response 35
5.3.5.1.9 Unnumbered receive-no-ready response 35
5.3.5.2 Type 2 operation commands and responses . . 36
5.3.5.2.1 Information-transfer-format command and response 36
5.3.5.2.2 Supervisory-format commands and responses . 36
5.3.5.2.2.1 Receive-ready (RR) command and response . . 37
5.3.5.2.2.2 Reject (REJ) command and response 37
5.3.5.2.2.3 Receive-not-ready (RNR) command and response 37
5.3.5.2.2.4 Selective-reject (SREJ) command and response 38
5.3.5.2.3 Unnumbered-format command and responses . . 38
5.3.5.2.3.1 Set asynchronous balanced mode extended (SABME) command 38
5.3.5.2.3.2 Disconnect (DISC) command 39
5.3.5.2.3.3 Reset (RSET) command 39

CONTENTS (Continued)

PARAGRAPH PAGE

5.3.5.2.3.4 Unnumbered acknowledgment (UA) response . . 39
5.3.5.2.3.5 Disconnect mode (DM) response 39
5.3.5.2.3.6 Frame reject (FRMR) response 40
5.3.6 Description of procedures by type 42
5.3.6.1 Description of Type 1 procedures 42
5.3.6.1.1 Modes of operation 42
5.3.6.1.2 Procedure for addressing 42
5.3.6.1.3 Procedure for using the P/F bit 42
5.3.6.1.4 Procedures for logical data-link set-up and disconnection 42
5.3.6.1.5 Procedures for information transfer 42
5.3.6.1.5.1 Sending UI command PDUs 42
5.3.6.1.5.2 Receiving UI command PDUs 43
5.3.6.1.5.3 Sending URR response PDUs 43
5.3.6.1.5.4 Sending URNR response PDUs 43
5.3.6.1.5.5 Receiving acknowledgment 43
5.3.6.1.5.6 Sending URNR command PDUs 43
5.3.6.1.5.7 Receiving URNR command PDUs 43
5.3.6.1.5.8 Sending URR command PDUs 43
5.3.6.1.5.9 Receiving URR command PDUs 44
5.3.6.1.5.10 Using XID command and response PDUs 44
5.3.6.1.5.11 Using TEST command and response PDUs 44
5.3.6.2 Description of Type 2 procedures 44
5.3.6.2.1 Modes 44
5.3.6.2.1.1 Operational mode 44
5.3.6.2.1.2 Nonoperational mode 44
5.3.6.2.2 Procedure for addressing 45
5.3.6.2.3 Procedures for using the P/F bit 45
5.3.6.2.4 Procedures for data-link set-up and disconnection 45
5.3.6.2.4.1 Data-link connection phase 45
5.3.6.2.4.1.1 Initiator action 45
5.3.6.2.4.1.2 Respondent action 46
5.3.6.2.4.2 Information transfer phase 46
5.3.6.2.4.3 Data-link disconnection phase 46
5.3.6.2.4.4 Data-link disconnected phase 47
5.3.6.2.4.5 Contention of unnumbered mode-setting command PDUs 47
5.3.6.2.5 Procedures for information transfer 47
5.3.6.2.5.1 Sending I PDUs 47
5.3.6.2.5.2 Receiving an I PDU 48
5.3.6.2.5.3 Receiving incorrect PDUs 48
5.3.6.2.5.4 Receiving out-of-sequence PDUs 48
5.3.6.2.5.4.1 Reject response 49
5.3.6..2.5.4.2 Selective reject response 49
5.3.6.2.5.5 Receiving acknowledgment 49
5.3.6.2.5.6 Receiving and SREJ PDU 50

CONTENTS (Continued)

PARAGRAPH PAGE

5.3.6.2.5.7 Receiving an RSET PDU 50
5.3.6.2.5.8 Receiving an REJ PDU 50
5.3.6.2.5.9 Receiving an RNR PDU 50
5.3.6.2.5.10 Station-busy condition 50
5.3.6.2.5.11 Waiting acknowledgment 51
5.3.6.2.6 Procedures for mode resetting 51
5.3.6.2.6.1 Receiver action 52
5.3.6.2.6.2 Initiator action 52
5.3.6.2.6.3 Resetting with the FRMR PDU 52
5.3.6.2.7 Procedures for sequence number resetting . . 53
5.3.6.2.8 FRMR exception conditions 53
5.3.7 Data-link initialization 53
5.3.7.1 List of data-link parameters 54
5.3.7.1.1 Type 1 logical data-link parameters 54
5.3.7.1.2 Type 2 data-link parameters 55
5.3.8 Frame transfer 56
5.3.8.1 Type 1 PDU transmission 56
5.3.8.1.1 Type 1 data-link concatenation 57
5.3.8.1.2 Type 1 physical-layer concatenation 57
5.3.8.2 Type 2 PDU transmission 57
5.3.8.2.1 Type 2 data-link concatenation 57
5.3.8.2.2 Type 2 physical-layer concatenation 58
5.3.8.3 Type 1 and Type 2 PDU transmission 58
5.3.9 Flow control 58
5.3.9.1 Type 1 flow control 58
5.3.9.2 Type 2 flow control 63
5.3.10 Acknowledgment and response 63
5.3.10.1 Acknowledgment 63
5.3.10.1.1 Type 1 acknowledgment 63
5.3.10.1.2 Type 2 acknowledgment 63
5.3.10.2 Response mode 64
5.3.11 Invalid frame 64
5.3.12 Retransmission 64
5.3.13 Error detection and correction 64
5.3.13.1 Forward-error-correction coding 65
5.3.13.2 Forward-error-correction preprocessing . . . 65
5.3.13.3 Time-dispersive coding 65
5.3.14 Link layer interactions 66
5.4 Network layer 69
5.4.1 Network protocol data unit 69
5.4.2 Network header 69
5.4.2.1 Field 1 - version number 69
5.4.2.2 Field 2 - time-to-live 69
5.4.2.3 Field 3 - message frame number 70
5.4.2.4 Field 4 - station serial number 70
5.4.2.5 Field 5 - tactical system message precedence 71

CONTENTS (Continued)

PARAGRAPH		PAGE
5.4.2.6	Field 6 - security classification	71
5.4.2.7	Field 7 - message type	71
5.4.2.8	Field 8 - originator routing indicator (ORI)	72
5.4.2.9	Field 9 - destination routing indicator (DRI)	73
5.4.2.9.1	Destination list	73
5.4.2.9.1.1	Redundant information indicator	73
5.4.2.9.1.2	Routing indicator type	73
5.4.2.9.2	Source path list	73
5.4.2.10	Field 10 - end of routing	74
5.4.3	Network-layer procedures	74
5.4.3.1	Packet routing	74
5.4.3.1.1	Implementation	74
5.4.3.1.2	Directory routing	74
5.4.3.1.2.1	Transmitting and routing procedures	74
5.4.3.1.2.2	Receiving end routing procedures	75
5.4.3.1.2.3	Routing tables	76
5.4.3.1.2.4	Routing history	76
5.4.3.1.3	Source routing	76
5.4.3.1.4	Packet filter	77
5.4.3.1.5	Data-link acknowledgment	77
5.4.3.2	Packet addressing	77
5.4.3.2.1	Address format	77
5.4.3.2.2	Addressee with no relay	77
5.4.3.2.3	Destinations through relay	77
5.4.3.2.4	Packet precedence	77
5.4.3.3	Network flow and congestion control	78
5.4.3.3.1	Traffic queuing	78
5.4.3.3.2	Discard control	78
5.4.3.4	End-to-end error recovery (message accountability)	78
5.4.3.5	Message segmentation	78
5.4.3.5.1	Segmentation	79
5.4.3.5.2	Reassembly	79
5.4.4	Next-layer interactions	80
5.4.4.1	Data-link layer	80
5.4.4.2	Upper-layer protocol	80
5.5	Presentation layer	82
5.5.1	VMF syntax	82
5.5.1.1	Field presence indicator	82
5.5.1.2	Field recurrence indicator	83
5.5.1.3	Group presence indicator	83
5.5.1.4	Group recurrence indicator	83
5.5.2	VMF syntax indicator implementation rules	83
5.5.3	End-of-literal field marker	84
5.5.4	Data-field construction procedures	84

CONTENTS (Continued)

PARAGRAPH PAGE

5.5.4.1 ASCII data element 85
5.5.4.2 Binary-coded-decimal data element 85
5.5.4.3 Binary data element 85
5.5.5 Next-layer interaction 85
5.6 Application layer 86
5.6.1 Application protocol data unit 86
5.6.1.1 Application header 86
5.6.1.1.1 Field 1 - receipt/compliance 86
5.6.1.1.2 Field 2 - message designator 86
5.6.1.1.3 Field 3 - date and time 87
5.6.1.1.4 Fields 4, 5, 6 - originator, recipient, information addressees 88
5.6.1.1.5 Field 7 - control and release marking . . . 88
5.6.1.1.6 Field 8 - cannot process reason code (CANTPRO) 88
5.6.1.1.7 Message accountability 88
5.6.2 User data field 89
5.6.3 Message acknowledgment 89
5.6.3.1 Receipt/compliance messages 89
5.6.3.2 Message implementation 89
5.6.3.2.1 Perishable messages 89
5.6.3.2.2 Nonperishable messages 89
5.6.3.3 Receipt/compliance message format/content . 90
5.6.3.3.1 Lower-layer parameters 91
5.6.3.3.2 Application header fields 91
5.6.3.3.3 Error fields 91
5.6.3.3.4 Receipt/compliance flag 91
5.6.3.4 Message retransmission timer 92
5.6.4 Lower-layer protocol interaction 92
5.6.4.1 Parameters to the lower-layer protocol . . . 92
5.6.4.1.1 Originator and destination addresses 92
5.6.4.1.2 Originator ID 92
5.6.4.1.3 Quality-of-service parameters 93
5.6.4.1.4 Options 94
5.6.4.1.5 Message type 94
5.6.4.2 Parameters from the lower-layer protocol . . 94
5.7 Application process 94
5.7.1 Message formats 94

6. NOTES 95
6.1 Subject term (key word) listing 95
6.2 Issue of the DoD Index of Specifications and Standards 95
6.3 Interoperability considerations 95
6.3.1 Transmission channel 95
6.3.2 Physical interface 95

CONTENTS (Continued)

PARAGRAPH PAGE

6.3.3 COMSEC interoperability 96
6.3.4 Single-thread data-link diagrams 96

FIGURES

FIGURE PAGE

1 Standard interface for DMTD subsystems 9
2 DMTD functional reference model 10
3 Basic structure of DMTD at the standard interface 10
4 Transmission frame structure 16
5 Transmission synchronization field 17
6 Frame synchronization pattern 17
7 Transmission word-count field 18
8 Data-link frame structure and placement 21
9 Extended address field format 22
10 Address allocation 23
11 Data-link PDU control field formats 30
12 Type 1 operation control-field bit assignments 34
13 Information-transfer-format control field bits 36
14 Supervisory-format control field bits 37
15 Unnumbered-format control field bits 38
16 FRMR information format 41
17 Type 1 data-link concatenation 59
18 Type 1 physical-layer concatenation 60
19 Type 2 data-link concatenation 61
20 Type 2 physical-layer concatenation 62
21 16 x 24 matrix before interleaving 66
22 Transmitter's 24 x 16 matrix after interleaving 66
23 Network protocol data-unit structure 69
24 Routing indication subfields 72
25 Network segmentation example 79
26 Application protocol data unit structure . . . 86
27a Simple R/C message format 91
27b CANTPRO-field content invalid R/C format . . . 91

CONTENTS (Concluded)

TABLES

TABLE		PAGE
I	Characteristic frequencies of frequency-shift keying interface for voice frequency channels	13
II	Characteristic frequencies of frequency-shift keying interface for single-channel radio	14
III	Type 1 PDU formats	26
IV	Type 2 PDU formats	28
V	Network header fields	70
VI	Message precedence	71
VII	Security classifications	71
VIII	Types of messages	72
IX	Application header	85
X	Receipt/compliance codes	87
XI	Functional area designator codewords	87
XII	Data and time group data elements	88
XIII	Values for the routing indicator	92
XIV	Single-thread data links with external COMSEC	97
XV	Single-thread data links with embedded COMSEC	98

APPENDIXES

APPENDIX		PAGE
A	Abbreviations and acronyms	99
B	Layer interactions	105
C	Net access control algorithm	115
D-1	Communications security standards (U)	123
D-2	(Appendix D-2 under separate cover) (C)	
E	Data-link management processes	129
F	Golay coding algorithm	141
G	Variable message format syntax and structure	147
H	DFI/DUI message element definitions	151
I	Routing and relay for multiple destination addressing	175

1. SCOPE

1.1 Purpose. This MIL-STD promulgates the minimum essential technical parameters in the form of mandatory system standards and optional design objectives for interoperability and compatibility among DMTDs, and between DMTDs and applicable command, control, communications, computers, and intelligence (C4I) systems. These technical parameters are based on the data communications protocol standards specified herein to ensure interoperability.

1.2 Scope. This MIL-STD identifies the procedures, protocols, and parameters to be applied in specifications for DMTDs. This MIL-STD addresses the communications protocols and procedures for the exchange of information among DMTDs and between DMTDs and C4I systems participating in inter- and intra-Service tactical networks. The material is presented in the context of the Open Systems Interconnection (OSI), as documented in national and international standards.

1.3 Application guidance. This MIL-STD applies to the design and development of new equipment and systems, and to the retrofit of existing equipment and systems.

1.4 System standards and design. The parameters and other requirements specified in this MIL-STD are mandatory system standards if the word *shall* is used in connection with the parameter value or requirement under consideration. Nonmandatory design objectives are indicated in parentheses after a standardized parameter value or by the word *should* in connection with the parameter value or requirement under consideration.

1.5 Tailoring. This MIL-STD is a compilation of selected options derived from military, commercial, and federal standards.

2. APPLICABLE DOCUMENTS

2.1 Government documents

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this MIL-STD to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the current issue of the DoD Index of Specifications and Standards (DoDISS) and supplements thereto, cited in the solicitation (see 6.2).

STANDARDS

FEDERAL

FIPS-PUB-133	Coding and Modulation Requirements for 2400 bit/second Modems
FED-STD-1037	Glossary of Telecommunication Terms

MILITARY

MIL-STD-188-100 (Series)	Common Long Haul and Tactical Communications System Technical Standards
MIL-STD-188-110	Equipment Technical Design Standards for Common Long Haul/Tactical Data Modems
MIL-STD-188-114	Electrical Characteristics of Digital Interface Circuits
MIL-STD-188-200	System Design and Engineering Standards for Tactical Communications

[Unless otherwise indicated, copies of federal and military standards are available from the Naval Publications and Forms Center, ATTN: NPODS, 5801 Tabor Avenue, Philadelphia, PA, 19120-5099.]

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this MIL-STD to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

Joint Interoperability of Tactical Command and Control Systems, Variable Message Format Technical Interface Design Plan (Test Edition).

VOL I	Overview
VOL II	Data Element Dictionary
VOL III	Message Formats

[This document is available from the Joint Interoperability and Engineering Organization (JIEO), ATTN: TBCA, Suite 210, 11440 Isaac Newton Square North, Reston, Virginia 22090-5006.]

2.2 Non-Government documents. The following documents form a part of this MIL-STD to the extent specified herein. Unless otherwise specified, the issues of the documents that are DoD-adopted are those listed in the issue of the DoDISS cited in the solicitation. Unless otherwise specified, the issues of documents not listed in the DoDISS are the issues of the documents cited in the solicitation (see 6.2).

INTERNATIONAL ORGANIZATION for STANDARDIZATION (ISO)

ISO 3309	Information Processing Systems -- Data Communication -- High-level Data Link Control Procedures -- Frame Structure, 1984-10-01
ISO 6039	Final Text for ISO/IEC 8802-2:1989/DAM 2 -- Information technology -- Local area networks -- Logical link control -- Amendment 2: Acknowledged connectionless-mode service and protocol, Type 3 operation, 1990-06-26
ISO 7498	Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model, 1984.
ISO 7498 AD 1	Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model -- Addendum 1: Connectionless-mode Transmission, 1987.

ISO 8802.2	Information Processing Systems -- Local Area Networks -- Part 2: Logical Link Control, 1987.
ISO 8885	Information Processing Systems -- Data Communications -- High- level Data Link Control Procedures -- General Purpose XID Frame Information Field Content and Format, 1987

[ISO standards are available from the American National Standards Institute, Inc., 1430 Broadway, New York, NY 10018.]

2.3 Order of precedence. In the event of a conflict between the text of this MIL-STD and the references cited herein, the text of this MIL-STD takes precedence. Nothing in this MIL-STD, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

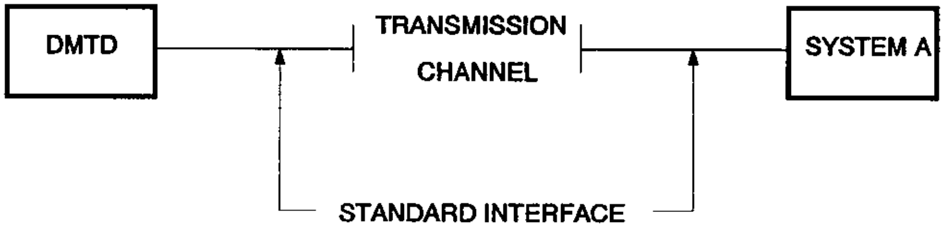
3.1 Definitions of terms. Definitions of terms used in this MIL-STD are specified in FED-STD-1037.

3.2 Abbreviations and acronyms. Abbreviations and acronyms used in this MIL-STD are defined in Appendix A. Those listed in the current edition of FED-STD-1037 have been included for the convenience of the reader.

4. GENERAL REQUIREMENTS

4.1 Digital message transfer device. A DMTD is a portable data terminal device with limited message generation and processing capability. DMTDs are used for remote access to automated C4I systems and to other DMTDs. The environment encompasses point-to-point, point-to-multipoint, and broadcast transfer of information over data communications links.

4.2 Interoperability. Interoperability of DMTDs and associated C4I systems shall be achieved by implementing the standard interface for DMTD subsystems (see Figure 1) specified in this MIL-STD. This standard defines the layered protocols for the transmission of single or multiple segment messages over broadcast radio subnetworks and point-to-point links. It provides the minimum essential data communications parameters and protocol stack required to communicate with other data terminal devices. These communications parameters and protocols will facilitate functional interoperability among DMTDs, and between DMTDs and applicable C4I systems within the layered framework described below. Electrical and mechanical design parameters are design-dependent and are outside the scope of this MIL-STD. Interoperability considerations for terminal designers and systems engineers are addressed in 6.3.



NOTES:

1. DMTD and System A (where system A can be another DMTD or a C4I system) may include modems, line drivers, error control algorithms, encryption devices, control units, and other devices as required to comply with this MIL-STD.
2. The transmission channel may include single and multichannel transmission equipment.
3. The baseband signal waveform and handshaking protocols at the standard interface are specified in Section 5.

FIGURE 1. Standard interface for DMTD subsystems.

4.3 Framework. The communications and procedural protocols used in DMTD equipment shall support the layers of the functional reference model depicted in Figure 2. The DMTD functional reference model in Figure 2 is based on the ISO 7498 OSI seven-layer model and is for reference only. Figure 2 contains the framework that is used in this MIL-STD for defining the protocols required to exchange information among DMTD subsystems, and between DMTD subsystems and applicable C4I systems. Figure 3 illustrates a representative time epoch of the basic frame structure supported by the DMTD subsystem.

Application Layer
Presentation Layer
Session Layer *
Transport Layer *
Network Layer
Link Layer
Physical Layer

* NOTE: These layers are null and provide a pass-through service.

Figure 2. DMTD functional reference model.

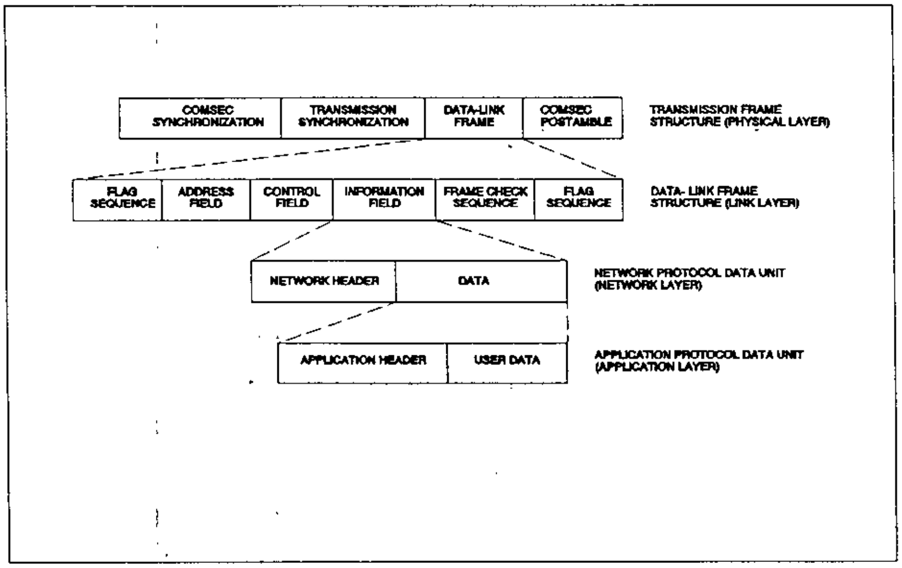


FIGURE 3. Basic structure of DMTD at the standard interface.

4.4 DMTD capabilities. The waveform and the protocols necessary to ensure end-to-end interoperability at the interface shall support the following capabilities:

a. Transmission in a half-duplex mode over radio, wireline, and cable links;

b. Link encryption;

c. Point-to-point, multipoint, or broadcast connectivity between stations;

d. Asynchronous balanced mode of operation between two or more stations;

e. Network access control for network access management and collision avoidance;

f. Transport of bit-oriented or free-text (character-oriented) messages for information exchange in a variable message format over the link;

g. User data exchange using single or multiple frame packets;

h. Addressing conventions that support single, multiple, and global station addressing, as well as routing and relay;

i. Error control, for maintaining data integrity over the link, including frame check sequence (FCS), forward error correction (FEC), and time-dispersive coding (TDC); and

j. Data-link frame acknowledgment and message accountability through application layer receipt/compliance capabilities.

5. DETAILED REQUIREMENTS

5.1 Physical layer. The physical layer shall provide the control functions required to activate, maintain, and deactivate the connections between communications systems.

5.1.1 Transmission channel interfaces. The transmission channel interfaces specified below define the transmission envelope characteristics (signal waveform, transmission rates, and operating mode) authorized at the standard interface between a DMTD and the transmission channel. The transmission channel may consist of wireline, cable, or radio links.

5.1.1.1 Non-return-to-zero interface. This interface shall be used primarily with digital transmission equipment. A non-return-to zero (NRZ) signal waveform shall be used for this interface.

5.1.1.1.1 Waveform. The NRZ unbalanced and balanced waveforms shall conform to paragraphs 5.1.1.7 and 5.2.1.7, respectively, of MIL-STD-188-114.

5.1.1.1.2 Transmission rates. The output transmission rates of the NRZ interface shall be the following bit rates: 75, 150, 300, 600, 1200, 2400, 4800, 8000, 9600, and 16000 bits per second (bps).

5.1.1.1.3 Operating mode. The NRZ interface shall support half-duplex transmission.

5.1.1.2 Frequency-shift keying interface for voice frequency channels. This interface shall be used primarily with analog single-channel [3-kilohertz (kHz)] radio equipment. The frequency-shift keying (FSK) data modem characteristics shall conform to paragraph 5.2.2 of MIL-STD-188-110.

5.1.1.2.1 Waveform. The FSK modulation waveform shall conform to paragraph 5.2.2.1 of MIL-STD-188-110. The characteristic frequencies, in hertz (Hz), for transmission rates of 600 bps or less, and 1200 bps, shall be as shown in Table I.

Table I. Characteristic frequencies of frequency-shift keying interface for voice frequency channels.

PARAMETER	CHARACTERISTIC FREQUENCY (Hz)	
	600 bps or less	1200 bps
Mark Frequency	1300	1300
Space Frequency	1700	2100

5.1.1.2.2 Transmission rates. Output transmission rates of the FSK interface shall be the following bit rates: 75, 150, 300, 600, and 1200 bps.

5.1.1.2.3 Operating mode. The FSK interface shall support half-duplex transmission.

5.1.1.3 Frequency-shift keying interface for single-channel radio. This interface, used within DoD, may also be used for North Atlantic Treaty Organization (NATO) single-channel radio applications. The FSK interface data modem characteristics shall conform to paragraph 5.1 of MIL-STD-188-110.

5.1.1.3.1 Waveform. The FSK modulation waveform shall conform to paragraphs 5.1.1 and 5.1.2 of MIL-STD-188-110. The characteristic frequencies are specified in Table II.

Table II. Characteristic frequencies of frequency-shift keying interface for single-channel radio.

PARAMETER	CHARACTERISTIC FREQUENCY (Hz)
Mark Frequency	1575
Space Frequency	2425

5.1.1.3.2 Transmission rates. Output transmission rates of the single-channel FSK interface shall be the following bit rates: 75, 150, 300, 600, and 1200 bps.

5.1.1.3.3 Operating mode. The single-channel FSK interface shall support half-duplex transmission.

5.1.1.4 Conditioned diphase interface. This interface shall be used primarily with wideband wireline equipment and digital single-channel radio equipment. A conditioned diphase (CDP) modulation data modem shall be used for this interface.

5.1.1.4.1 Waveform. The CDP modulation waveform shall conform to paragraph 5.4.1.4 of MIL-STD-188-200. The unbalanced and balanced signal waveform shall conform to paragraphs 5.1.1.7 and 5.2.1.7, respectively, of MIL-STD-188-114.

5.1.1.4.2 Transmission rates. The output transmission rate of the CDP interface shall be 16 kilobits per second (kbps).

5.1.1.4.3 Operating mode. The CDP interface shall support half-duplex transmission.

5.1.1.5 Differential phase-shift keying interface for voice frequency channels. This interface shall be used primarily with analog (nominal 4-kHz voice frequency) wireline and radio equipment. Differential phase-shift keying (DPSK) modulation data modem (2400 bps) and phase-shift keying (PSK) modulation data modem (1200 bps) characteristics shall conform to the applicable requirements of FIPS-PUB-133.

5.1.1.5.1 Waveform. The DPSK modulation waveform shall conform to paragraph 2.2 of FIPS-PUB-133. The PSK modulation waveform shall conform to paragraph 2.3 of FIPS-PUB-133.

5.1.1.5.2 Transmission rates. The output transmission rate of the DPSK and PSK interfaces shall be 2400 and 1200 bps, respectively.

5.1.1.5.3 Operating mode. The DPSK and PSK interfaces shall support half-duplex transmission.

5.2 Physical-layer protocol

5.2.1 Physical-layer protocol data unit. The transmission frame shall be the basic protocol data unit (PDU) of the physical layer and shall be composed of the following components, as shown in Figure 4.

a. Communications security (COMSEC) synchronization
b. Bit synchronization
c. Frame synchronization
d. Transmission word count (TWC)
e. Data field
f. COMSEC postamble

5.2.1.1 Communications security synchronization and postamble. These fields are present when link encryption is used. The COMSEC synchronization field shall be used to achieve cryptographic synchronization over the link. The COMSEC postamble field shall be used to provide an end-of-transmission flag to the COMSEC equipment at the receiving station. These fields and the COMSEC synchronization process are described in Appendix D. Figure 4a presents the transmission frame structure for traditional COMSEC (backward-compatible mode). Traditional COMSEC is used in this MIL-STD to denote systems with the COMSEC equipment placed external to the DMTD. Figure 4b presents the transmission frame structure with COMSEC embedded in the DMTD (embedded mode). Figure 4c presents the transmission frame structure without COMSEC.

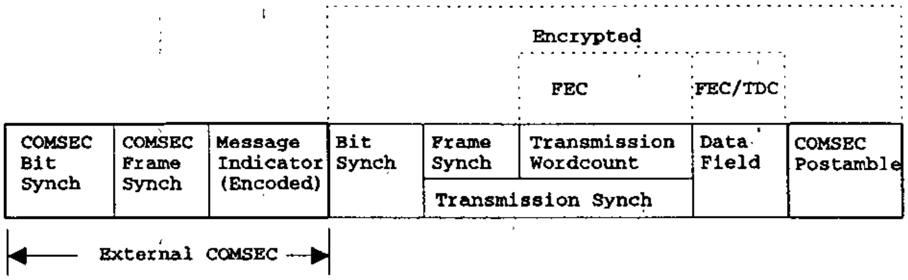


FIGURE 4A. Transmission frame structure with traditional COMSEC.

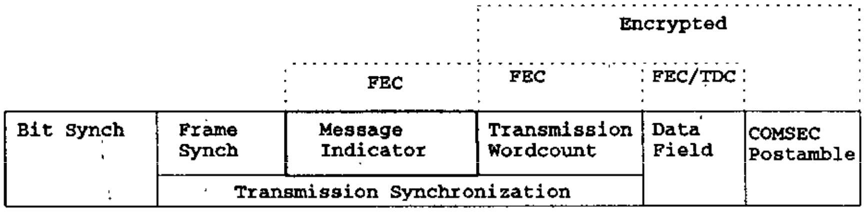


FIGURE 4B. Transmission frame structure with embedded COMSEC.

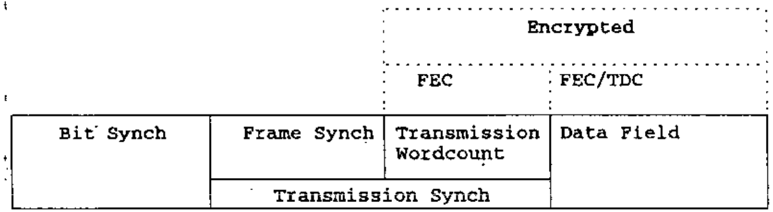


FIGURE 4C. Transmission frame structure without COMSEC.

FIGURE 4. Transmission frame structure.

5.2.1.2 Bit synchronization field. This field shall be used to provide to the receiver a signal for achieving bit synchronization. The duration of the bit synchronization field shall be the time interval required to transmit at least a 32-bit pattern that consists of alternating ones and zeros, beginning with a one. The bit synchronization field is required with embedded COMSEC (Figure 4b) and without COMSEC (Figure 4c). When external COMSEC is used (Figure 4a), the COMSEC bit synchronization field of the external device may be used instead of the internal field.

5.2.1.3 Transmission synchronization field. This field shall be used (a) to provide a framing signal, indicating the start of the data-link frame to the receiving station, and (b) to indicate the number of words in the frame. This field shall be composed of two subfields, frame synchronization and TWC, as shown in Figure 5. For equipment with embedded COMSEC, the COMSEC Message Indicator (MI) is placed between the two subfields, as shown in Figure 4b. The embedded COMSEC application is described in Appendix D.

Frame Synchronization	Transmission Word Count
31 bits	24 bits

Figure 5. Transmission synchronization field.

5.2.1.3.1 Frame synchronization subfield. This subfield shall consist of the fixed 31-bit synchronization pattern shown in Figure 6.

LSB																														MSB
1	1	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0

Figure 6. Frame synchronization pattern.

The receiver, upon detecting the synchronization pattern (with 4 or less bits in error), shall place the incoming data block, starting with the TWC, in the correct octet boundaries for further processing. Failure to detect the synchronization pattern (more than 4 bits in error) shall cause the receiver to stop the frame synchronization function and resume monitoring the channel for bit synchronization of another frame.

5.2.1.3.2 Transmission word-count subfield. The TWC is a value calculated by the transmitting station to inform the receiving station of the number of 16-bit words that form the data field of the transmission frame. The maximum TWC is 4095 (2^{12}-1). The 24-bit TWC subfield shall be 1 half-rate Golay FEC codeword that consists of 12 information bits, indicating the number of 16-bit words in the transmission; 11 checksum bits for error correction; and a "don't care" (d/c) bit (this bit has the value 0 or 1). Golay encoding is described in Appendix F. This subfield shall be structured as shown in Figure 7. The value provided by the 12 information bits is binary-encoded. The maximum number of words is dependent on the maximum number of bits allowed in the data field of a transmission frame. It is possible that the number of bits in the data field will not be evenly divisible by 16. In that case, the word count shall be rounded to the next higher integer.

LSB		MSB
WORD COUNT 12 BITS	CHECKSUM 11 BITS	d/c BIT

Figure 7. Transmission word-count field.

5.2.1.4 Data field. The data field shall contain the string of bits created by the data-link layer following the procedures for framing, bit stuffing, FEC, and TDC.

5.2.1.5 COMSEC postamble field. This field shall be used to provide an end-of-transmission flag to the COMSEC at the receiving station. The field shall be as described in Appendix D, Communications Security Standards.

5.2.2 Keytime delay. Keytime delay (KT) is an element of the transmission equipment and one of the many variables that must be considered for net access control. KT is defined in Appendix C.

5.2.3 Net busy indication. The net busy information is conveyed to the upper layer protocol (data link) through a status indication. Upon detection of a net busy, the data net busy indicator shall be set. The data net busy sensing indicator shall be reset when the digital data is no longer detected by the net busy sensing function. Appendix C describes the net busy sensing function.

5.2.4 Physical-layer to upper-layer interactions. Three primitives are used to pass information for the sending and receiving of data across the upper layer boundary.

a. Requests for transmission of data are sent by the upper layer, using the physical layer (PL) Unitdata Request primitive with the following parameter:

PL-Unitdata Request	Data/Data length

b. Indication of data received is provided to the upper layer through the Unitdata Indication primitive with the following parameter:

PL-Unitdata Indication	Data/Data length

c. Net activity status information is provided to the upper layer through a Status Indication with the following parameters:

PL-Status Indication	Net activity 0 = net clear 1 = net busy

5.3 Data-link layer. The data-link layer shall provide the control functions to ensure the transfer of information over established physical paths, to provide framing requirements for data, and to provide for error control.

5.3.1 Net access control. The presence of multiple subscribers on a single communications net requires a method of controlling the transmission opportunities for each subscriber. To minimize conflicts, the net busy sensing function and net access control (NAC) procedures regulate transmission opportunities for all participants on the net. Random - Net Access Delay (R-NAD), Hybrid - Net Access Delay (H-NAD), and Prioritized - Net Access Delay (P-NAD) shall be implemented as the authorized NAC procedures at this interface. Appendix C defines the NAC parameters for R-NAD, H-NAD, and P-NAD.

5.3.2 Types of procedures. Three types of operation for data communication between systems are defined to provide basic connectionless and connection mode operations. These types and services are based on ISO 8802-2:1989, IEEE Std 802.2-1989, ISO/IEC 8802-2:1989/AME(E), and ISO/IEC JTC 1/SC 6 N 6039:1990. The connectionless operations are mandatory for implementation in all systems. The connection mode is optional for this interface.

5.3.2.1 Types of operation. Three types of operation are provided by ISO 8802-2:

Type 1 - Unacknowledged Connectionless Operation
Type 2 - Connection-mode Operation
Type 3 - Acknowledged Connectionless Operation

5.3.2.1.1 Type 1 operation. For the purpose of this protocol, Type 1 service will designate both of the ISO 8802.2 connectionless operations (acknowledged and unacknowledged).

5.3.2.1.2 Type 2 operation. With the optional Type 2 operation, a data-link connection shall be established between two systems prior to any exchange of information bearing PDUs. The normal communications cycle between Type 2 systems shall consist of transferring PDUs from the source to the destination, and acknowledging receipt of these PDUs in the opposite direction.

5.3.2.2 Command and response features. Below is the full set of command and response PDUs supported for Types 1 and 2:

	Commands	**Responses**
Type 1:	UI XID URR URNR TEST	UI XID URR URNR TEST
Type 2:	I RR RNR REJ SABME DISC SREJ RSET	I RR RNR REJ UA DM SREJ FRMR

5.3.3 Data-link frame. The data-link frame shall be the basic protocol data unit of the link layer.

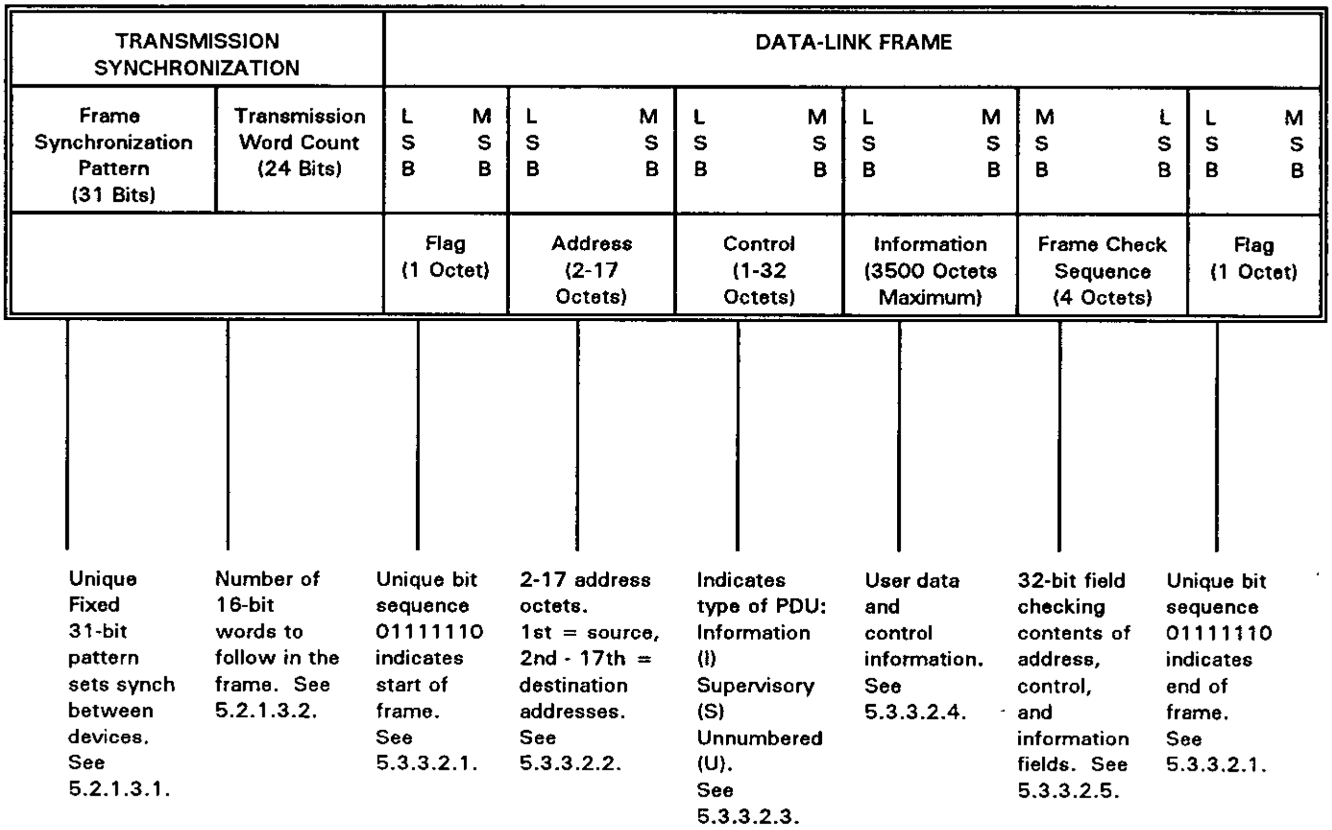
5.3.3.1 Types of frames. Three types of frames are defined for this interface to convey data over the data-link: an unnumbered frame (U PDUs), an information frame (I PDUs) and a supervisory frame (S PDUs).

5.3.3.1.1 Unnumbered frame. The U PDUs shall be used for Type 1 and Type 2 operations. They provide connectionless information transfer, acknowledgment, and station identification/status information for Type 1 operations. They also provide data-link control functions for Type 2 operations.

5.3.3.1.2 Information frame. The I PDUs are optional and are used for information transfer in Type 2 operations. They convey user data or message traffic across a link. The I PDUs are not used in Type 1 operations.

5.3.3.1.3 <u>Supervisory frame</u>. The S PDUs are optional and are used for data-link supervisory control functions and to acknowledge received I PDUs in Type 2 operations. The S PDUs are not used in Type 1 operations.

5.3.3.2 <u>Data-link frame structure</u>. The basic elements of the data-link frame shall be the opening flag sequence, the address field, the control field, the information field, the FCS, and the closing flag sequence. Each data-link frame shall be structured as shown in Figure 8.



TRANSMISSION SYNCHRONIZATION		DATA-LINK FRAME					
Frame Synchronization Pattern (31 Bits)	Transmission Word Count (24 Bits)	LSB MSB	LSB MSB	LSB MSB	LSB MSB	MSB LSB	LSB MSB
		Flag (1 Octet)	Address (2-17 Octets)	Control (1-32 Octets)	Information (3500 Octets Maximum)	Frame Check Sequence (4 Octets)	Flag (1 Octet)
Unique Fixed 31-bit pattern sets synch between devices. See 5.2.1.3.1.	Number of 16-bit words to follow in the frame. See 5.2.1.3.2.	Unique bit sequence 01111110 indicates start of frame. See 5.3.3.2.1.	2-17 address octets. 1st = source, 2nd - 17th = destination addresses. See 5.3.3.2.2.	Indicates type of PDU: Information (I) Supervisory (S) Unnumbered (U). See 5.3.3.2.3.	User data and control information. See 5.3.3.2.4.	32-bit field checking contents of address, control, and information fields. See 5.3.3.2.5.	Unique bit sequence 01111110 indicates end of frame. See 5.3.3.2.1.

Figure 8. <u>Data-link frame structure and placement</u>.

5.3.3.2.1 <u>Flag sequence</u>. All frames shall start and end with the 8-bit flag sequence of one 0 bit, six 1 bits, and one 0 bit (01111110). The flag shall be used for data-link frame synchronization. The closing flag sequence of a frame may be used as the opening flag sequence for the following frame.

5.3.3.2.2 Address fields. These fields shall identify the link addresses of the source and destinations.

5.3.3.2.2.1 Address format. Each address in the address fields shall consist of a single octet. The source address octet shall consist of a command/response (C/R) designation bit [the least significant bit (LSB)] followed by a 7-bit address representing the source. Each destination octet shall consist of an extension bit (the LSB) followed by the 7-bit destination address. The destination address uses a modification of the High-Level Data-link Control (HDLC) extended addressing format. The destination address shall be extended by setting the extension bit of a destination address octet to 0, indicating that the following octet is another destination address. The destination address field shall be terminated by an octet that has the extension bit set to 1. The destination address field shall be extendible from 1 address octet to 16 address octets. The format of the address fields shall be as shown in Figure 9.

1	2	3	4	5	6	7	8	Bit Position
0/1	X	X	X	X	X	X	X	SOURCE Octet (0 = response; 1 = command)
0	X	X	X	X	X	X	X	DESTINATION 1 Octet
.				.				.
.				.				.
.				.				.
1	X	X	X	X	X	X	X	DESTINATION M Octet where M ≤ 16

Figure 9. Extended address field format.

5.3.3.2.2.2 Addressing convention. The following addressing conventions shall be implemented in the 7 address bits of each address octet. Address allocations, as shown in Figure 10, are divided among five address types: individual, group, global, special, and reserved.

NOTE: Source and destination addresses are assigned by an administrative authority.

LSB							MSB		
1	1	1	1	1	1	1	1	127	Global Multicast Address
X	X	X	X	X	X	1	1	96-126	Group Multicast Addresses
X	X	X	X	X	X	X	X	3-95	Individual Addresses
X	0	1	0	0	0	0	0	2	Special (Net Control) Address
X	1	0	0	0	0	0	0	1	Special (Net Entry) Address
X	0	0	0	0	0	0	0	0	Reserved Address

Figure 10. Address allocation.

5.3.3.2.2.2.1 Source and destination

5.3.3.2.2.2.1.1 Source address. The source address is either an individual or special net entry address and is always the first address. Its legal values range from 3 to 95 (1 for special net entry). The source address has two parts: the C/R designation bit (bit 1, LSB) and the actual 7-bit address value. The C/R designation bit shall be set to 1 for commands and 0 for responses.

5.3.3.2.2.2.1.2 Destination address(es). The second through seventeenth address bytes are labeled destination addresses, which may be global, group, individual, or special addresses. Each destination address is contained in an 8-bit field, which has two parts: the extension bit (bit 1, LSB) and the actual 7-bit address value. An extension bit set to 0 indicates that 1 or more addresses follow. An extension bit set to 1 indicates the last address of the address string has been reached. Figure 10 illustrates the allocation of addresses in the address field.

5.3.3.2.2.2.2 Types of addresses. The following paragraphs describe the five types of addresses and how they shall be used.

5.3.3.2.2.2.2.1 Reserved address. Address 0 is labeled a reserved address. The sending of the reserved address is prohibited. A station receiving a value of 0 in the destination address field shall ignore the address and continue processing any remaining addresses.

5.3.3.2.2.2.2.2 Special addresses. Addresses 1 and 2 are labeled special addresses. These addresses are provided as secondary net control and unit entry addresses for units entering a new net without knowledge of actual addresses being used. Special addresses are used as described in Appendix E.

5.3.3.2.2.2.2.3 Individual addresses. Individual addresses uniquely identify a single station on a broadcast subnetwork. Individual addresses shall be assigned within the address range 3 to 95. Stations shall be capable of sending and receiving 1 to 16 individual destination addresses in a single data-link frame. When only individual addresses are present, a receiving station shall receive all addresses, search for its unique individual address, and follow the media access procedures described in Appendix C.

5.3.3.2.2.2.2.4 Group multicast addresses. Group multicast addressing, used when broadcasting messages to multiple (but not all) stations on a broadcast subnetwork, may be implemented. The valid address range shall be 96 to 126. Membership to (or deletion from) a group is outside the scope of this protocol. While the use of link group multicast addresses is optional, all stations shall be capable of recognizing received group addresses. If a receiving station does not implement group addressing procedures, it shall still process all received addresses, but ignore the group addresses (that is, recognize range 96 to 126 as group addresses). When group addressing is implemented, a station shall be capable of sending and receiving 1 to 16 destination group addresses. In this case, data-link acknowledgment shall not be allowed [Poll/Final (P/F) bit set to 1 shall be prohibited].

5.3.3.2.2.2.2.5 Unique and group multicast addresses mixed. A station that optionally implements group addressing shall also be capable of sending and receiving both group and unique addresses "mixed" in a destination address subfield. All stations shall be capable of receiving mixed addresses. The total number of destination addresses shall not exceed 16. The presence of one or more group addresses shall prohibit the use of data-link acknowledgment (P/F bit set to 1 shall be prohibited). The reception and acknowledgment procedures stated in this paragraph shall be valid even for stations that do not implement group addressing procedures.

5.3.3.2.2.2.2.6 Global multicast addressing. Global multicast addressing, used when broadcasting messages to all systems on a broadcast subnetwork, shall be implemented through the unique bit pattern 1111111 (127). If the global address is used, it shall be the only destination address. All broadcast stations shall be capable of receiving and sending this address, and all stations will process the information contained within the frame. Data-link acknowledgment shall not be allowed with this address (P/F bit set to 1 shall be prohibited).

5.3.3.2.2.3 Mapping. A link address is a point of attachment to a broadcast network. The upper-layer protocol is responsible for mapping one or more upper-layer addresses to a data-link address. Multiple upper-layer addresses may map to one or more group or individual addresses (for example, multiple routing indicators can be located through a single group-link address).

5.3.3.2.3 Control field. The control field indicates the type of PDU and the response requirements and connection information about the PDU being transmitted over the data link. Figure 11 illustrates the data-link PDU control field formats. A summary of the formats and bit patterns for Types 1 and 2 is shown in Tables III and IV, respectively.

5.3.3.2.3.1 Type 1 operations. For Type 1 operations, the control field is an 8-bit pattern designating 1 of 5 types of U PDUs.

5.3.3.2.3.2 Type 2 operations. The Type 2 control field is a 16-bit pattern for I PDUs and S PDUs and includes sequence numbers. The Type 2 U PDUs have an 8-bit pattern. The Type 2 control field may be repeated if more than one destination address is present. Each destination address field shall have a corresponding control field for I PDUs and S PDUs, which contain sequence numbers. A Type 2 U PDU control field is not repeated if there is more than one destination.

5.3.3.2.3.3 Poll/final bit. The fifth LSB of the control field is called the P/F bit. The P/F bit serves a function in both command and response PDUs. In command PDUs, the P/F bit is referred to as the P-bit. In response PDUs, it is referred to as the F-bit. The P-bit set to 1 shall be used to solicit a response PDU, with the F-bit set to 1. On a data link, only 1 PDU with a P-bit set to 1 shall be outstanding in a given direction at a given time. Before a station issues another PDU with the P-bit set to 1 to a particular destination, it shall have received a response PDU from that remote station with the F-bit set to 1.

Table III. Type 1 PDU formats.

COMMANDS/ RESPONSES	ADDRESS FIELD	CONTROL FIELD	INFORMATION FIELD
XID PDU EXCHANGE IDENTIFICATION (XID) COMMAND MESSAGE	Contains source address and up to 16 link addresses of systems required to respond to this command, or the special net controller address, or the global address.	Variable bit pattern = 1111X101 (X represents the P/F bit settings)	This field follows the ISO 8885 format for XID commands and responses. It is used to supply or request link management information. Appendix E details the information field structure.
EXCHANGE IDENTIFICATION (XID) RESPONSE MESSAGE	Contains source address and address of the sender of the command message.	Unique bit pattern = 11111101	
UI PDU ACKNOWLEDGMENT REQUIRED	Contains the source address and up to 16 individual link addresses of agencies for which the message is intended.	Unique bit pattern = 11001000 identifies this frame as a UI PDU requiring acknowledgment.	Contains data from the upper protocol layer.
ACKNOWLEDGMENT NOT REQUIRED	Contains the source address and up to 16 group (or group and individual mixed) addresses of agencies for which the message is intended; or the source address and the global address.	Unique bit pattern = 11000000 identifies this frame as a UI PDU not requiring acknowledgment.	Contains data from the upper protocol layer.

Table III. Type 1 PDU formats (Concluded).

COMMANDS/ RESPONSES	ADDRESS FIELD	CONTROL FIELD	INFORMATION FIELD
Status PDU			
UNNUMBERED RECEIVE READY (URR) COMMAND	Contains source address, and individual, group, or global addresses.	Unique bit pattern = 11000110 indicating receive ready command.	No information field allowed.
UNNUMBERED RECEIVE READY (URR) RESPONSE	Contains source address and the address contained in the source subfield of a received UI PDU, which this frame acknowledges.	Unique bit pattern = 11001110 indicating last UI PDU is acknowledged.	No information field allowed.
UNNUMBERED RECEIVE NOT READY (URNR) COMMAND	Contains source address and individual, group, or global addresses of agencies that are to stop transmitting UI PDUs to the agency generating this frame.	Unique bit pattern = 11010000 indicating receive not ready command.	No information field allowed.
UNNUMBERED RECEIVE NOT READY (URNR) RESPONSE	Contains source address and destination to which this response is being sent.	Unique bit pattern = 11011000 indicating receive not ready response.	No information field allowed.
TEST COMMAND	Contains source address to the individual, group, or global address of agencies that are to respond.	Unique bit pattern = 11001111	Information field optimal.
TEST RESPONSE	Contains source address and destination to which this response is being sent.	Unique bit pattern = 11001111	Information field optional.

Table IV. Type 2 PDU formats.

COMMANDS/ RESPONSES	ADDRESS FIELD	CONTROL FIELD	INFORMATION FIELD
U PDUs			
UNNUMBERED ACKNOWLEDGMENT (UA) RESPONSE	Contains source address and destination to which this response is being sent.	Variable bit pattern = 1100X110	No information field allowed.
SET ASYNCHRONOUS BALANCED MODE EXTENDED (SABME) COMMAND	Contains source address and a single individual link address of station required to respond to this command.	Unique bit pattern = 11111100	No information field allowed.
RESET (RSET) COMMAND	Contains source address and a single individual link address of station required to respond.	Unique bit pattern = 11111001	No information field allowed.
FRAME REJECT (FRMR) RESPONSE	Contains source address and individual destination link address.	Variable bit pattern = 1110X001	See Figure 16.
DISCONNECT MODE (DM) RESPONSE	Contains source address and appropriate individual destination address.	Variable bit pattern = 1111X000	No information field allowed.
DISCONNECT (DISC) COMMAND	Contains source address and a single individual destination address.	Variable bit pattern = 1100X010	No information field allowed.
I PDU			
ACKNOWLEDGMENT OR OTHER APPROPRIATE RESPONSE REQUIRED	Contains source address and up to 16 individual addresses of agencies for which the message is intended.	Variable bit pattern = 0SSSSSSSXRRRRRRR. Identifies this frame as an I PDU.	Contains data from the upper layer protocol.

TABLE IV. Type 2 PDU formats (Concluded).

COMMANDS/ RESPONSES	ADDRESS FIELD	CONTROL FIELD	INFORMATION FIELD
S PDUs			
RECEIVE READY (RR) COMMAND	Contains source address and the global address or appropriate individual addresses.	Variable bit pattern = 10000000XRRRRRRR, indicating receive ready command.	No information field allowed.
RECEIVE READY (RR) RESPONSE	Contains source address and the address contained in the source subfield of a received I PDU, which this PDU acknowledges.	Variable bit pattern = 10000000XRRRRRRR, indicating last I PDU is acknowledged.	No information field allowed.
RECEIVE NOT READY (RNR) COMMAND	Contains source address and the individual, group, or global address of agencies that are to stop transmitting I PDUs to the agency generating this frame.	Variable bit pattern = 10100000XRRRRRRR, indicating receive not ready command.	No information field allowed.
RECEIVE NOT READY (RNR) RESPONSE	Contains source address and the address contained in the source subfield of a received I command, which this frame acknowledges.	Variable bit pattern = 10100000XRRRRRRR, indicating receive not ready.	No information field allowed.
SELECTIVE REJECT (SREJ) COMMAND AND RESPONSE	Contains source address and appropriate individual destination address.	Variable bit pattern = 10110000XRRRRRRR.	No information field allowed.
REJECT (REJ) COMMAND AND RESPONSE	Contains source address and appropriate individual destination address.	Variable bit pattern = 10010000XRRRRRRR. (X represents the P/F bit setting, S represents send sequence number, and R represents receive sequence number.)	No information field allowed.

<table>
<tr><th></th><th colspan="10">Data-link PDU control field bits</th></tr>
<tr><th></th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10 - 16</th></tr>
<tr><td>INFORMATION TRANSFER COMMAND RESPONSE (I PDU)</td><td>0</td><td colspan="7">N(S)</td><td>P/F</td><td>N(R)</td></tr>
<tr><td>SUPERVISORY COMMANDS/RESPONSES (S PDUs)</td><td>1</td><td>0</td><td>S</td><td>S</td><td>X</td><td>X</td><td>X</td><td>X</td><td>P/F</td><td>N(R)</td></tr>
<tr><td>UNNUMBERED COMMANDS/RESPONSES (U PDUs)</td><td>1</td><td>1</td><td>M</td><td>M</td><td>P/F</td><td>M</td><td>M</td><td>M</td><td></td><td></td></tr>
</table>

N(S) = Transmitter send sequence number (Bit 2 = low-order bit)
N(R) = Transmitter receive sequence number (Bit 10 = low-order bit)
S = Supervisory Function bit
M = Modifier function bit
X = Reserved and set to zero
P/F = Poll bit - command PDU transmissions
Final bit - response PDU transmissions
(1 = Poll/Final)

Figure 11. Data-link PDU control field formats.

5.3.3.2.3.4 Sequence numbers. The Type 2 I and S PDUs shall contain sequence numbers. The sequence numbers shall be in the range of 0-127.

5.3.3.2.4 Information field. The information field may be present in either the I, UI, FRMR, TEST, or XID PDU. The length of the information field shall be a multiple of 8 bits, not to exceed 3500 octets. If the data is not a multiple of 8 bits, 1 to 7 fill bits (0) shall be added to meet this requirement. The maximum information field size defaults to 3500 octets. This size is also called the maximum transmission unit (MTU) by the network layer. A smaller MTU size may be established at initialization through local system information or using the XID PDUs. Contents of the information fields of the FRMR, TEST, and XID PDUs are described in 5.3.5.2.3.6 and 5.3.5.1.5, and in Appendix E, respectively.

5.3.3.2.5 Frame check sequence. For error detection, all frames shall include a 32-bit FCS prior to the closing flag sequence. The contents of the address, control, and information fields are included in the FCS calculation. Excluded from the FCS calculation are the 0's inserted by the 0-bit insertion algorithm. The formula for calculating the FCS, which is the 1's complement (inversion) of the remainder of a modulo-2 division process, employs the generator polynomial, *P(X)*, having the form

$$P(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

FCS generation shall be in accordance with the paragraph entitled "32-bit Frame Checking Sequence" in ISO 3309, and implemented in a manner that provides a unique remainder when a frame is received without bit errors incurred during transmission. If the FCS of a received frame proves the frame to be invalid, the frame shall be discarded.

5.3.3.3 Data-link PDU construction. The data-link procedures that affect data-link PDU construction include (a) order-of-bit transmission and 0-bit insertion, discussed below; and (b) FEC and TDC, discussed in 5.3.13.

5.3.3.3.1 Order-of-bit transmission. The bit order of the frame components are specified in Figure 8. The order-of-bit transmission function specifies the sequence in which bits are ordered by the data-link layer for transmission by the physical layer. The flag and control fields shall be transmitted LSB first. For the FCS, the most significant bit (MSB) shall be transmitted first. For the address field, the source address octet is transmitted first and the destination address octet(s) are transmitted in order. The LSB of each address octet is transmitted first. The information field octets shall be transmitted in the same order as received from the upper layers, LSB first.

5.3.3.3.2 Zero-bit insertion algorithm. The occurrence of a spurious flag sequence within a frame shall be prevented by employing a 0-bit insertion algorithm. After the entire frame has been constructed, the transmitter shall always insert a 0 bit after the appearance of five 1's in the frame (with the exception of the flag fields). After detection of an opening flag sequence, the receiver shall search for a pattern of five 1's. When the pattern of five 1's appears, the sixth bit shall be examined. If the sixth bit is a 0, the 5 bits shall be passed as data, and the 0 shall be deleted. If the sixth bit is a 1, the receiver shall inspect the seventh bit. If the seventh bit is a 0, a flag sequence has been received. If the seventh bit is a 1, an invalid message has been received and should be discarded.

5.3.4 Operational parameters. The various parameters associated with the control field formats are described in the following sections.

5.3.4.1 Type 1 operational parameters. The only parameter that exists in Type 1 operation is the P/F bit. The P/F bit set to 1 shall be used only in Type 1 operation with the UI, XID, TEST, URR, and URNR command/response PDU functions. The Poll (P) bit set to 1 shall be used to solicit (poll) an immediate correspondent response PDU with the Final (F) bit set to 1 from the addressed station. The response with F-bit set to 1 shall be transmitted in accordance with the response hold delay (RHD) procedures defined in Appendix C.

5.3.4.2 Type 2 operational parameters. The various parameters associated with the control field formats in Type 2 operation are described in 5.3.4.2.1 to 5.3.4.2.3.2.

5.3.4.2.1 Modulus. Each I PDU shall be sequentially numbered with a numeric value between 0 and MODULUS minus ONE (where MODULUS is the modulus of the sequence numbers). MODULUS shall equal 128 for the Type 2 control field format. The sequence numbers shall cycle through the entire range. The maximum number of sequentially numbered I PDUs that may be outstanding (that is, unacknowledged) in a given direction of a data-link connection at any given time shall never exceed one less than the modulus of the sequence numbers. This restriction shall prevent any ambiguity in the association of sent I PDUs with sequence numbers during normal operation and error recovery action.

5.3.4.2.2 PDU-state variables and sequence numbers. A station shall maintain a send-state variable, V(S), for the I PDUs it sends and a receive-state variable, V(R), for the I PDUs it receives on each data-link connection. The operation of V(S) shall be independent of the operation of V(R).

5.3.4.2.2.1 Send-state variable V(S). The V(S) shall denote the sequence number of the next in-sequence I PDU to be sent on a specific data-link connection. The V(S) shall take on a value between 0 and MODULUS minus ONE. The value of V(S) shall be incremented by one with each successive I PDU transmission on the associated data-link connection, but shall not exceed receive sequence number N(R) of the last received PDU by more than MODULUS minus ONE.

5.3.4.2.2.2 Send-sequence number N(S). Only I PDUs shall contain N(S), the send sequence number of the sent PDU. Prior to sending an I PDU, the value of N(S) shall be set equal to the value of the V(S) for that data-link connection.

5.3.4.2.2.3 Receive-state variable V(R). The V(R) shall denote the sequence number of the next in-sequence I PDU to be received on a specific data-link connection. The V(R) shall take on a value between 0 and MODULUS minus ONE. The value of the V(R) associated with a specific data-link connection shall be incremented by one whenever an error-free I PDU is received whose N(S) equals the value of the V(R) for the data-link connection.

5.3.4.2.2.4 Receive sequence number N(R). All I and S PDUs shall contain N(R), the expected sequence number of the next received I PDU on the specified data-link connection. Prior to sending an I or S PDU, the value of N(R) shall be set equal to the current value of the associated V(R) for that data-link connection. N(R) shall indicate that the station sending the N(R) has received correctly all I PDUs numbered up through N(R)-1 on the specified data-link connection.

5.3.4.2.3 Poll/final (P/F) bit. The P/F bit shall serve a function in Type 2 operation in both command and response PDUs. In command PDUs the P/F bit shall be referred to as the P-bit. In response PDUs it shall be referred to as the F-bit. P/F bit exchange provides a distinct C/R linkage that is useful during both normal operation and recovery situations.

5.3.4.2.3.1 Poll-bit functions. A command PDU with the P-bit set to 1 shall be used to solicit (poll) a response PDU with the F-bit set to 1 from the addressed station on a data-link connection. Only one PDU with a P-bit set to 1 shall be outstanding in a given direction at a given time on the data-link connection between any specified pair of stations. Before a station issues another PDU on the same data-link connection with the P-bit set to 1, the station shall have received a response PDU with the F-bit set to 1 from the addressed station. If no valid response PDU is received within a system-defined P-bit timer time-out period, the resending of a command PDU with the P-bit set to 1 shall be permitted for error recovery purposes.

5.3.4.2.3.2 Final-bit functions. The F-bit set to 1 shall be used to acknowledge the receipt of a command PDU with the P-bit set to 1. Following the receipt of a command PDU with the P-bit set to 1, the station shall send a response PDU with the F-bit set to 1 on the appropriate data-link connection at the first possible opportunity. *First possible opportunity* is defined as transmitting the frame ahead of other frames at the next network access opportunity. If a prioritized net access scheme is employed, the response PDU shall be assigned an URGENT priority. The station shall be permitted to send appropriate response PDUs with the F-bit set to 0 at any net access opportunity without the need for a command PDU.

5.3.5 Commands and responses. This section defines the commands and associated responses. Definitions of the set of commands and responses for each of the control field formats for Type 1 and Type 2 operations, respectively, are contained in 5.3.5.1 and 5.3.5.2. The C/R bit, the LSB of the source address field, is used to distinguish between commands and responses. The following discussion of commands and responses assumes that the C/R bit has been properly decoded. Some of the commands described in the following paragraphs require a response at the earliest opportunity. Response PDUs requiring "earliest opportunity" transmission shall be queued ahead of all other PDUs for transmission during the next network access opportunity. If a prioritized net access scheme is in effect, the response PDU shall assume the priority level of the highest PDU queued or the mid (PRIORITY) level, whichever is greater.

5.3.5.1 Type 1 operation commands and responses. Type 1 commands and responses are all U PDUs. The U PDU encodings for Type 1 operations are listed in Figure 12.

FIRST CONTROL FIELD BIT DELIVERED
TO/RECEIVED FROM THE PHYSICAL LAYER

↓

1	2	3	4	5	6	7	8	Bit Position
1	1	0	0	P/F	0	0	0	UI Command/Response
1	1	0	0	P/F	1	1	0	URR Command/Response
1	1	0	1	P/F	0	0	0	URNR Command/Response
1	1	1	1	P/F	1	0	1	XID Command/Response
1	1	0	0	P/F	1	1	1	Test Command/Response

Figure 12. Type 1 operation control-field bit assignments.

5.3.5.1.1 Unnumbered information command. The unnumbered information PDU (UI PDU) shall be used to send information to one or more stations. The P-bit of the control field of the UI PDU is used by the transmitter to request that the receiver(s) acknowledge receipt of the transmitted UI PDU or to specify that an acknowledgment is not required. The UI PDU shall be addressed to an individual, group, or global address. The source address shall be the individual address of the transmitting station.

5.3.5.1.2 Unnumbered receive-ready command. The unnumbered receive-ready (URR) command PDU shall be transmitted to one or more stations to indicate that the sending station is ready to receive UI PDUs. The URR PDU shall be addressed to an individual, group, or global address. The source address shall be the individual address of the transmitting station.

5.3.5.1.3 Unnumbered receive-not-ready command. The unnumbered receive-not-ready (URNR) command PDU shall be transmitted to one or more stations to indicate that the sending station is busy and cannot receive UI PDUs. The URNR PDU shall be addressed to an individual, group, or global address. The source address shall be the individual address of the transmitting station.

5.3.5.1.4 Exchange identification command. The exchange identification (XID) command PDU shall be used to request the link parameters and to announce a station's presence on the network. The XID command PDU with the P-bit set to 1 shall cause the destination station to respond with an XID response PDU, with the F-bit set to 1, after the appropriate RHD period (see Appendix C). The XID command PDU, with the P-bit set to 0, shall be used by a station to announce its presence on the net. The information field of an XID PDU shall consist of an 8-bit XID format identifier field plus one or more group identifier fields described in Appendix E. The XID command PDU shall be addressed to either an individual, global, or the special net control address. The source address may be an individual address or the special net entry address.

5.3.5.1.5 Test command. The test command (TEST) shall be used to cause the destination station to respond with the TEST response at the earliest opportunity, thus performing a basic test of the transmission path. An information field is optional with the TEST command PDU. It may contain any bit pattern, but is limited to a maximum length of 128 octets. If present, however, the received information field shall be returned, if possible, by the addressed station in the TEST response PDU. The TEST command PDU shall be addressed to an individual, group, or global destination address. The source address shall be an individual address.

5.3.5.1.6 Unnumbered receive-ready response. The URR response shall be used to reply to a UI command that requested an acknowledgment (P-bit set to 1). The URR response shall be the first PDU sent by the receiving station upon receiving a UI command after the appropriate RHD period (see Appendix C). The source and destination shall be individual addresses.

5.3.5.1.7 Exchange identification response. The XID response shall be used to reply to an XID command that has the P-bit set to 1. The XID response PDU shall be the first PDU sent by the receiving station upon receiving an XID command PDU, after the appropriate RHD period (see Appendix C). The contents of the XID response information field is described in Appendix E. The source address shall be an individual or net control address. The destination address shall be an individual or the special net entry address.

5.3.5.1.8 Test response. The TEST response shall be used to reply to the TEST command at the earliest opportunity. If an information field was present in the TEST command PDU, the TEST response PDU shall contain the same information field contents. If the station cannot accept the information field of the TEST command, a TEST response without an information field may be returned. The source and destination addresses shall be an individual or net control address.

5.3.5.1.9 Unnumbered receive-not-ready response. The URNR response PDU shall be used to reply to a UI command with the P-bit set to 1, if the UI command cannot be processed due to a busy condition. The URNR response is the first PDU transmitted after the appropriate RHD period (see Appendix C). The URNR response shall have the F-bit set to 1 and shall be addressed to the source of the UI command.

5.3.5.2 Type 2 operation commands and responses. Type 2 commands and responses consist of I, S, and U PDUs.

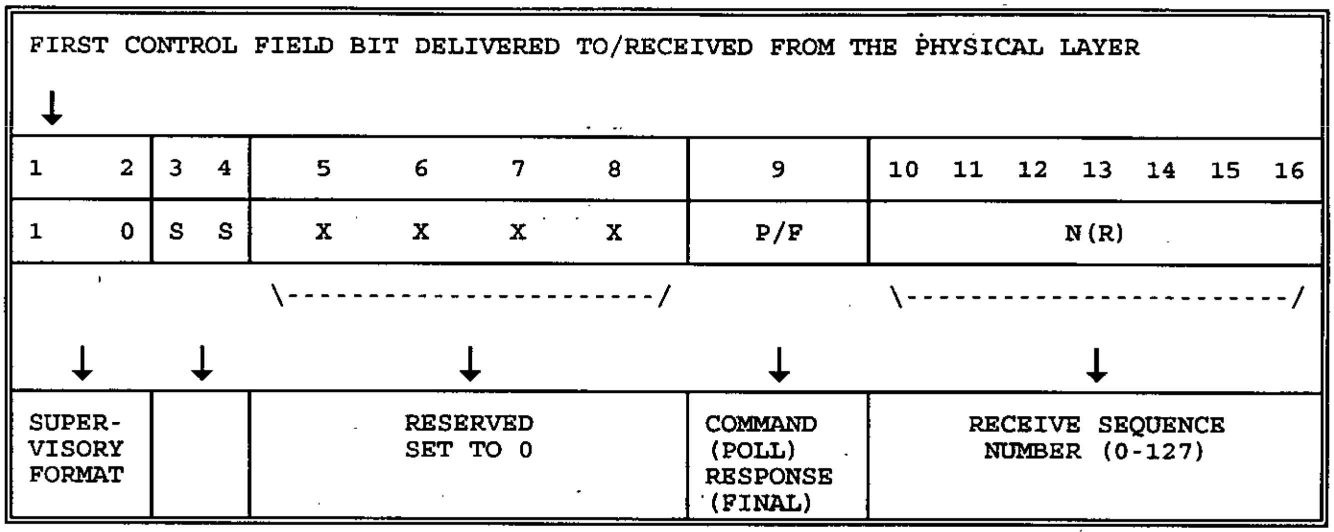
5.3.5.2.1 Information-transfer-format command and response. The function of the information (I) command and response shall be to transfer sequentially numbered PDUs that contain an information field across a data-link connection. The encoding of the I PDU control field for Type 2 operation shall be as listed in Figure 13.

FIRST CONTROL FIELD BIT DELIVERED TO/RECEIVED FROM THE PHYSICAL LAYER ↓			
1	2 3 4 5 6 7 8	9	10 11 12 13 14 15 16
0	N(S)	P/F	N(R)
INFORMATION TRANSFER FORMAT	SEND SEQUENCE NUMBER (0-127)	COMMAND (POLL) RESPONSE (FINAL)	RECEIVE SEQUENCE NUMBER (0-127)

Figure 13. Information-transfer-format control field bits.

The I PDU control field shall contain two sequence numbers: N(S), which shall indicate the sequence number associated with the I PDU; and N(R), which shall indicate the sequence number (as of the time the PDU is sent) of the next expected I PDU to be received, and, consequently, shall indicate that the I PDUs numbered up through N(R)-1 have been received correctly.

5.3.5.2.2 Supervisory-format commands and responses. Supervisory (S) PDUs shall be used to perform numbered supervisory functions such as acknowledgments, temporary suspension of information transfer, or error recovery. S PDUs shall not contain an information field and, therefore, shall not increment the send-state variable at the sender or the receive-state variable at the receiver. Encoding of the S PDU control field for Type 2 operation shall be as shown in Figure 14. An S PDU shall contain an N(R), which shall indicate, at the time of sending, the sequence number of the next expected I PDU to be received. This shall acknowledge that all I PDUs numbered up through N(R)-1 have been received correctly, except in the case of the selective reject (SREJ) PDU. The use of N(R) in the SREJ PDU is explained in 5.3.5.2.2.4.



COMMANDS	SS	RESPONSES
RECEIVE READY (RR)	00	RECEIVE READY (RR)
REJECT (REJ)	01	REJECT (REJ)
RECEIVE NOT READY (RNR)	10	RECEIVE NOT READY (RNR)
SELECTIVE REJECT (SREJ)	11	SELECTIVE REJECT (SREJ)

Figure 14. Supervisory-format control field bits.

5.3.5.2.2.1 Receive-ready (RR) command and response. The RR PDU shall be used by a station to indicate it is ready to receive I PDUs. I PDUs numbered up through N(R)-1 shall be considered as acknowledged.

5.3.5.2.2.2 Reject (REJ) command and response. The REJ PDU shall be used by a station to request the resending of I PDUs, starting with the PDU numbered N(R). I PDUs numbered up through N(R)-1 shall be considered as acknowledged. It shall be possible to send additional I PDUs awaiting initial sending after the resent I PDUs. With respect to each direction of sending on a data-link connection, only one "sent REJ" condition shall be established at any given time. The "sent REJ" condition shall be cleared upon receipt of an I PDU with an N(S) equal to the N(R) of the REJ PDU. The "sent REJ" condition may be reset in accordance with procedures described in 5.3.6.2.5.4.

5.3.5.2.2.3 Receive-not-ready (RNR) command and response. The RNR PDU shall be used by a station to indicate a busy condition (a temporary inability to accept subsequent I PDUs). I PDUs numbered up through N(R)-1 shall be considered as acknowledged. I PDUs numbered N(R) and any subsequent I PDUs received shall not be considered as acknowledged; the acceptance status of these PDUs shall be indicated in subsequent exchanges.

5.3.5.2.2.4 Selective-reject (SREJ) command and response. The selective reject PDU is used by a station to request retransmission of the single I PDU numbered N(R). If the P-bit in the SREJ PDU is set to 1, then I PDUs numbered up to N(R)-1 shall be considered acknowledged. If the P-bit is set to 0, then the N(R) of the SREJ PDU does not indicate acknowledgment of any I PDUs. Each SREJ exception condition shall be cleared (reset) upon receipt of an I PDU with an N(S) equal to the N(R) of the SREJ PDU. A data station may transmit one or more SREJ PDUs, each containing a different N(R) with the P-bit set to 0, before one or more earlier SREJ exception conditions have been cleared. I PDUs that have been transmitted following the I PDU designated by the SREJ PDU shall not be retransmitted as the result of receiving the SREJ PDU. Additional I PDUs awaiting initial transmission may be transmitted following the retransmission of the specific I PDU requested by the SREJ PDU. The SREJ is used to recover from receipt of frames with various types of errors, including sequence number errors due to lost frames and FCS errors.

5.3.5.2.3 Unnumbered-format commands and responses. Unnumbered (U) commands and responses shall be used in Type 2 operations to extend the number of data-link connection control functions. The U PDUs shall not increment the state variables on the data-link connection at either the sending or the receiving station. Encoding of the U PDU control field shall be as shown in Figure 15.

FIRST CONTROL FIELD BIT DELIVERED TO/RECEIVED FROM THE PHYSICAL LAYER

↓

1	2	3	4	5	6	7	8	
1	1	1	1	P	1	1	0	SABME Command
1	1	0	0	P	0	1	0	DISC Command
1	1	1	1	P	0	0	1	RSET Command
1	1	0	0	F	1	1	0	UA Response
1	1	1	1	F	0	0	0	DM Response
1	1	1	0	F	0	0	1	FRMR Response

Figure 15. Unnumbered-format control field bits.

5.3.5.2.3.1 Set asynchronous balanced mode extended (SABME) command. The SABME command PDU shall be used to establish a data-link connection to the destination station in the asynchronous balanced mode (ABM). No information shall be permitted with the SABME command PDU. The destination station shall confirm receipt of the SABME command PDU by sending a UA response PDU on that data-link connection at the earliest opportunity. Upon acceptance of the SABME command PDU, the destination station send- and receive-state variables shall be set to 0. If the UA response PDU is received correctly, then the initiating station shall also assume the asynchronous balanced mode with its corresponding send- and receive-state variables set to 0. Previously sent I PDUs that are unacknowledged when this command is executed shall remain unacknowledged. Whether or not a station resends the contents of the information field of unacknowledged outstanding I PDUs shall be decided at a higher layer.

5.3.5.2.3.2 Disconnect (DISC) command. The DISC command PDU shall be used to terminate an asynchronous balanced mode previously set by a SABME command PDU. It shall be used to inform the destination station that the source station is suspending operation of the data-link connection and the destination station should assume the logically disconnected mode. No information field shall be permitted with the DISC command PDU. Prior to executing the command, the destination station shall confirm the acceptance of the DISC command PDU by sending a UA response PDU on that data-link connection. Previously sent I PDUs that are unacknowledged when this command is executed shall remain unacknowledged. Whether or not a station resends the contents of the information field of unacknowledged outstanding I PDUs shall be decided at a higher layer.

5.3.5.2.3.3 Reset (RSET) command. The RSET command PDU shall be used by a station in an operational mode to reset the V(R) in the addressed station. No information field is permitted with the RSET command PDU. The addressed station shall confirm acceptance of the RSET command by transmitting a UA response PDU at the earliest opportunity. Upon acceptance of this command, the V(R) of the addressed station shall be set to 0. If the UA response PDU is received correctly, the initializing station shall reset its V(S) to 0.

5.3.5.2.3.4 Unnumbered acknowledgment (UA) response. The UA response PDU shall be used by a station on a data-link connection to acknowledge receipt and acceptance of the SABME, DISC, and RSET command PDUs. These received command PDUs shall not be executed until the UA response PDU is sent. No information field shall be permitted with the UA response PDU.

5.3.5.2.3.5 Disconnect mode (DM) response. The DM response PDU shall be used to report status indicating that the station is logically disconnected from the data-link connection and is in asynchronous disconnected mode (ADM). No information field shall be permitted with the DM response PDU.

5.3.5.2.3.6 Frame reject (FRMR) response. The FRMR response PDU shall be used by the station in the ABM to report that one of the following conditions, which is not correctable by resending the identical PDU, resulted from the receipt of a PDU from the remote station:

a. The receipt of a command PDU or a response PDU that is invalid or not implemented. Below are three examples of invalid PDUs:

   (1) the receipt of an S or U PDU with an information field that is not permitted,
   (2) the receipt of an unsolicited F-bit set to 1, and
   (3) the receipt of an unexpected UA response PDU.

b. The receipt of an I PDU with an information field that exceeded the established maximum information field length that can be accommodated by the receiving station for that data-link connection.

c. The receipt of an invalid N(R) from the remote station. An invalid N(R) shall be defined as one that signifies an I PDU that has previously been sent and acknowledged, or one that signifies an I PDU that has not been sent and is not the next sequential I PDU waiting to be sent.

d. The receipt of an invalid N(S) from the remote station. An invalid N(S) shall be defined as an N(S) that is greater than or equal to the last sent N(R) + *k*, where *k* is the maximum number of outstanding I PDUs. The parameter *k* is the window size indicated in the XID PDU.

The responding station shall send the FRMR response PDU at the earliest opportunity. An information field shall be returned with the FRMR response PDU to provide the reason for the PDU rejection. The information field shall contain the fields shown in Figure 16. The station receiving the FRMR response PDU shall be responsible for initiating the appropriate mode setting or resetting corrective action by initializing both directions of transmission on the data-link connection, using the SABME and DISC command PDUs, as applicable.

<table>
<tr><td colspan="7">FIRST CONTROL FIELD BIT DELIVERED TO/RECEIVED FROM THE PHYSICAL LAYER
↓</td></tr>
<tr><td>1-------------16</td><td>17</td><td>18--24</td><td>25</td><td>26--32</td><td>33--36</td><td>37--40</td></tr>
<tr><td>REJECTED PDU CONTROL FIELD</td><td>0</td><td>V(S)</td><td>C/R</td><td>V(R)</td><td>WXYZ</td><td>V000</td></tr>
</table>

Figure 16. FRMR information field format.

Notes to Figure 16:

a. Rejected PDU control field shall be the control field of the received PDU that caused the FRMR exception condition on the data-link connection. When the rejected PDU is a U PDU, the control field of the rejected PDU shall be positioned in bit positions 1-8, with 9-16 set to 0.

b. V(S) shall be the current send-state variable value for this data-link connection at the rejecting station (bit 18 = low-order bit).

c. C/R set to 1 shall indicate that the PDU causing the FRMR was a response PDU, and C/R set to 0 shall indicate that the PDU causing the FRMR was a command PDU.

d. V(R) shall be the current receive-state variable value for this data-link connection at the rejecting station (bit 26 = low-order bit).

e. W set to 1 shall indicate that the control field received and returned in bits 1 through 16 was invalid or not implemented. Examples of invalid PDU are defined as:

   (1) the receipt of an S or U PDU with an information field that is not permitted,
   (2) the receipt of an unsolicited F-bit set to 1, and
   (3) the receipt of an unexpected UA response PDU.

f. X set to 1 shall indicate that the control field received and returned in bits 1 through 16 was considered invalid because the PDU contained an information field that is not permitted with this command or response. Bit W shall be set to 1 in conjunction with this bit.

g. Y set to 1 shall indicate that the information field received exceeded the established maximum information field length which can be accommodated by the rejecting station on that data-link connection.

h. Z set to 1 shall indicate that the control field received and returned in bits 1 through 16 contained an invalid N(R).

i. V set to 1 shall indicate that the control field received and returned in bits 1 through 16 contained an invalid N(S). Bit W shall be set to 1 in conjunction with this bit.

5.3.6 Description of procedures by type. The procedures for each operation type are described in 5.3.6.1 and 5.3.6.2 (and their subparagraphs)

5.3.6.1 Description of Type 1 procedures. The procedures associated with Type 1 operation are described in 5.3.6.1 through 5.3.6.1.5.11.

5.3.6.1.1 Modes of operation. In Type 1 operation, no modes of operation are defined. A station using Type 1 procedures shall support the entire procedure set whenever it is operational on the network.

5.3.6.1.2 Procedure for addressing. The address fields shall be used to indicate the source and destinations of the transmitted PDU. The first bit in the source address field shall be used to identify whether a command or a response is contained in the PDU. Individual, group, special, and global addressing shall be supported for destination addresses. The source address field shall contain an individual or special address.

5.3.6.1.3 Procedure for using the P/F bit. The station receiving a UI, XID, or TEST command PDU with the P-bit set to 1 shall send an appropriate response PDU with the F-bit set to 1.

5.3.6.1.4 Procedures for logical data-link set-up and disconnection. Type 1 operation does not require any prior data-link connection establishment (set-up), and hence no data-link disconnection. Once the service access point has been enabled within the station, information may be sent to, or received from, a remote station also participating in Type 1 operation.

5.3.6.1.5 Procedures for information transfer

5.3.6.1.5.1 Sending UI command PDUs. Information transfer from an initiating station to a responding station shall be accomplished by sending the UI command PDU. When a sending station sends a UI command PDU with the P-bit set to 1, it shall start an acknowledgment timer for that transmission and increment an internal transmission count variable. If no URR response PDU is received before the timer runs out, the sending station shall resend the UI command PDU, increment the internal transmission count variable, and restart the acknowledgment timer. If a URR response PDU is still not received, this resending procedure shall be repeated until the value of the internal transmission count variable is equal to the value of the logical link parameter N4, as described in 5.3.7.1.1c, at which time an acknowledgment failure status shall be reported to the data-link user. An internal transmission count shall be maintained for each UI information exchange (where P-bit = 1) between a pair of sending and receiving stations. Both the acknowledgment timer and the internal transmission count, for that exchange, shall not affect the information exchange with other receiving stations.

If a URNR response PDU is received in response to a UI command with the P-bit set to 1, the receiving station shall designate the sending station as busy. The retransmission of the UI command shall follow the rules for the busy condition. Transmission of UI commands to that station shall be discontinued until the busy state is cleared. UI PDUs that have the P-bit set to 0 are not acknowledged nor retransmitted.

5.3.6.1.5.2 Receiving UI command PDUs. Reception of the UI command PDU with P-bit set to 0 shall not be acknowledged. A station shall acknowledge the receipt of a valid UI command PDU, which has the P-bit set to 1 and contains the station individual address, by sending a URR response PDU to the originator of the command UI PDU. If the receiving station is unable to accept UI PDUs due to a busy condition, it shall respond with a URNR response PDU.

5.3.6.1.5.3 Sending URR response PDUs. A URR response PDU, with the F-bit set to 1, shall be sent only upon receipt of a UI command PDU, with the P-bit set to 1. The URR response PDU shall be sent to the originator of the associated UI command PDU.

5.3.6.1.5.4 Sending URNR response PDUs. A URNR response PDU, with the F-bit set to 1, shall be sent by the remote station to advise the originator of the associated UI command PDU that it is experiencing a busy condition and is unable to accept UI PDUs.

5.3.6.1.5.5 Receiving acknowledgment. After sending a UI command PDU with the P-bit set to 1, the sending station shall expect to receive an acknowledgment in the form of a URR response PDU from the station to which the command PDU was sent. Upon receiving such a response PDU, the station shall stop the acknowledgment timer associated with the transmission for which the acknowledgment was received and reset the associated internal transmission count to zero. If the response was a URNR response PDU, the sending station will stop sending UI PDUs to that remote station until an RR command PDU is received, indicating termination of the busy condition.

5.3.6.1.5.6 Sending URNR command PDUs. A URNR command PDU, with the P-bit set to 0, may be sent at any time to indicate a busy condition.

5.3.6.1.5.7 Receiving URNR command PDUs. Receipt of the URNR indicates that the sending station is busy and no additional UI PDUs should be sent until the sending station regains its ability to receive messages. The URNR command PDU does not contain any acknowledgment information.

5.3.6.1.5.8 Sending URR command PDUs. A URR command PDU, with the P-bit set to 0, may be sent by a station at any time to indicate the regaining of its ability to receive messages.

5.3.6.1.5.9 Receiving URR command PDUs. The receipt of the URR command PDU cancels the prior receipt of a URNR and indicates that the sending station is now operational.

5.3.6.1.5.10 Using XID command and response PDUs. XID procedures are as defined in 5.3.5.1.3 and described in Appendix E.

5.3.6.1.5.11 Using TEST command and response PDUs. The TEST function provides a facility to conduct loop-back tests of the station-to-station transmission path. The TEST function may be initiated by any authorized station within the data-link layer. Successful completion of the test consists of sending a TEST command PDU with a particular information field to the designated destination address and receiving, in return, the identical information field in a TEST response PDU. The length of the information field is variable from 0 to 128 octets. Any TEST command PDU received in error shall be discarded and no response PDU sent. In the event of a test failure, it shall be the responsibility of the TEST function initiator to determine any future actions.

5.3.6.2 Description of Type 2 procedures. The procedures associated with Type 2 operation are described in 5.3.6.2.1 through 5.3.6.2.8.

5.3.6.2.1 Modes. Two modes of operation are defined for Type 2 operation: an operational mode and a nonoperational mode.

5.3.6.2.1.1 Operational mode. The operational mode shall be the ABM. ABM is a balanced operational mode in which a data-link connection has been established between two stations. Either station shall be able to send commands at any time and initiate response transmissions without receiving explicit permission from the other station. Such an asynchronous transmission shall contain one or more PDUs that shall be used for information transfer and to indicate status changes in the station (for example, the number of the next expected I PDU; transition from a ready to a busy condition, or vice versa; occurrence of an exception condition). A station in ABM receiving a DISC command PDU shall respond with the UA response PDU if it is capable of executing the command. ABM consists of a data-link connection phase, an information transfer phase, a data-link resetting phase, and a data-link disconnection phase.

5.3.6.2.1.2 Nonoperational mode. The nonoperational mode shall be the ADM. ADM differs from ABM in that the data-link connection is logically disconnected from the physical medium such that no information (user data) shall be sent or accepted. ADM is defined to prevent a data-link connection from appearing on the physical medium in a fully operational mode during unusual situations or exception conditions. Such operation could cause a sequence number mismatch between stations or a station's uncertainty of the status of the other station. A data-link connection shall be system-predefined as to the conditions that cause it to assume ADM. Below are three examples of possible conditions, in addition to receiving a DISC command PDU, that shall cause a data-link connection to enter ADM:

a. the power is turned on,
b. the data-link layer logic is manually reset, or
c. the data-link connection is manually switched from a local (home) condition to the connected-on-the-data-link (on-line) condition.

A station on a data-link connection in ADM shall be required to monitor transmissions received from its physical layer to accept and respond to one of the mode-setting command PDUs (SABME, DISC), or to send a DM response PDU at a medium access opportunity, when required. In addition, since the station has the ability to send command PDUs at any time, the station may send an appropriate mode-setting command PDU. A station in ADM receiving a DISC command PDU shall respond with the DM response PDU. A station in ADM shall not establish a FRMR exception condition. ADM consists of a data-link disconnected phase.

5.3.6.2.2 Procedure for addressing. The address fields for a PDU shall be used to indicate the individual source and up to 16 destinations. The first bit in the source address field shall be used to identify whether a command or response is contained in the PDU. A single data-link connection can be established between any two stations on the network.

5.3.6.2.3 Procedures for using the P/F bit. The station receiving a command PDU (SABME, DISC, RR, RNR, REJ, or I) with the P-bit set to 1 shall send a response PDU with the F-bit set to 1. The response PDU returned by a station to a SABME or DISC command PDU with the P-bit set to 1 shall be a UA or DM response PDU with the F-bit set to 1. The response PDU returned by a station to an I, RR, or REJ command PDU with the P-bit set to 1 shall be an I, RR, REJ, RNR, DM, or FRMR response PDU with the F-bit set to 1. The response PDU returned by a station to an RNR command PDU with the P-bit set to 1 shall be an RR, REJ, RNR, DM, or FRMR response PDU with the F-bit set to 1.

NOTE: The P-bit is usable by the station in conjunction with the timer recovery condition. (See 5.3.6.2.5.9.)

5.3.6.2.4 Procedures for data-link set-up and disconnection

5.3.6.2.4.1 Data-link connection phase. Either station shall be able to take the initiative to initialize the data-link connection.

5.3.6.2.4.1.1 Initiator action. When the station wishes to initialize the link, it shall send the SABME command PDU and start the acknowledgment timer. Upon receipt of the UA response PDU, the station shall reset both the V(S) and V(R) to 0 for the corresponding data-link connection, shall stop the acknowledgment timer, and shall enter the information transfer phase. When receiving the DM response PDU, the station that originated the SABME command PDU shall stop the acknowledgment timer, shall not enter the information transfer phase, and shall report to the higher layer for appropriate action. Should the acknowledgment timer run out before receiving the UA or DM response PDU, the station shall resend the SABME command PDU and restart the acknowledgment timer. After resending the SABME command PDU N2 times, the station shall stop sending the SABME command PDU and shall report to the higher layer for the appropriate error recovery action to initiate. The value of N2 is defined in 5.3.7.1.2.e. Other Type 2 PDUs received (commands and responses) while attempting to connect shall be ignored by the station.

5.3.6.2.4.1.2 Respondent action. When a SABME command PDU is received, and the connection is desired, the station shall return a UA response PDU to the remote station, set both the V(S) and V(R) to 0 for the corresponding data-link connection, and enter the information transfer phase. The return of the UA response PDU shall take precedence over any other response PDU that may be pending at the station for that data-link connection. It shall be possible to follow the UA response PDU with additional PDUs, if pending. If the connection is not desired, the station shall return a DM response PDU to the remote station and remain in the link disconnected mode. For a description of the actions to be followed upon receipt of a SABME or DISC command PDU, see 5.3.6.2.4.4.

5.3.6.2.4.2 Information transfer phase. After having sent the UA response PDU to an SABME command PDU or having received the UA response PDU to a sent SABME command PDU, the station shall accept and send I and S PDUs according to the procedures described in 5.3.6.2.5. When receiving an SABME command PDU while in the information transfer phase, the station shall conform to the resetting procedure described in 5.3.6.2.6.

5.3.6.2.4.3 Data-link disconnection phase. During the information transfer phase, either station shall be able to initiate disconnecting of the data-link connection by sending a DISC command PDU and starting the acknowledgment timer (see 5.3.7.1.2.a). When receiving a DISC command PDU, the station shall return a UA response PDU and enter the data-link disconnected phase. The return of the UA response PDU shall take precedence over any other response PDU that may be pending at the station for that data-link connection. Upon receipt of the UA or DM response PDU from the remote station, the station shall stop its acknowledgment timer and enter the link disconnected mode. Should the acknowledgment timer run out before receiving the UA or DM response PDU, the station shall resend the DISC command PDU and restart the acknowledgment timer. After sending the DISC command PDU N2 times, the sending station shall stop sending the DISC command PDU, shall enter the data-link disconnected phase, and shall report to the higher layer for the appropriate error recovery action. The value of N2 is defined in 5.3.7.1.2.e.

5.3.6.2.4.4 Data-link disconnected phase. After having received a DISC command PDU from the remote station and returned a UA response PDU, or having received the UA response PDU to a sent DISC command PDU, the station shall enter the data-link disconnected phase. In the disconnected phase, the station shall react to the receipt of an SABME command PDU, as described in 5.3.6.2.4.1, and shall send a DM response PDU in answer to a received DISC command PDU. When receiving any other Type 2 command PDU with the P-bit set to 1, the station in the disconnected phase shall send a DM response PDU with the F-bit set to 1. Other Type 2 PDUs received by the station while in the disconnected phase shall be ignored. In the disconnected phase, the station shall be able to initiate a data-link connection.

5.3.6.2.4.5 Contention of unnumbered mode-setting command PDUs. A contention situation on a data-link connection shall be resolved in the following way: If the sent and received mode-setting command PDUs are the same, each station shall send the UA response PDU at the earliest opportunity. Each station shall enter the indicated phase either after receiving the UA response PDU, or after its acknowledgment timer expires. If the sent and received mode-setting command PDUs are different, each station shall enter the data-link disconnected phase and shall issue a DM response PDU at the earliest opportunity.

5.3.6.2.5 Procedures for information transfer. The procedures that apply to the transfer of I PDUs in each direction on a data-link connection during the information transfer phase are described in 5.3.6.2.5.1 through 5.3.6.2.5.11. When used, the term *number one higher* is in reference to a continuously repeated sequence series, that is, 127 is 1 higher than 126, and 0 is 1 higher than 127 for the modulo-128 series.

5.3.6.2.5.1 Sending I PDUs. When the station has an I PDU to send (that is, an I PDU not already sent, or having to be resent as described in 5.3.6.2.5.5), it shall send the I PDU with an N(S) equal to its current V(S) and an N(R) equal to its current V(R) for that data-link connection. At the end of sending the I PDU, the station shall increment its V(S) by 1. If the acknowledgment timer is not running at the time that an I PDU is sent, the acknowledgment timer shall be started. If the data-link connection V(S) is equal to the last value of N(R) received plus *k* (where *k* is the maximum number of outstanding I PDUs; see 5.3.6.7.1.2.g), the station shall not send any new I PDUs on that data-link connection, but shall be able to resend an I PDU as described in 5.3.6.2.5.6 or 5.3.6.2.5.9. When a local station on a data-link connection is in the busy condition, the station shall still be able to send I PDUs, provided that the remote station on this data-link connection is not also busy. When the station is in the FRMR exception condition for a particular data-link connection, it shall stop transmitting I PDUs on that data-link connection.

5.3.6.2.5.2 Receiving an I PDU. When the station is not in a busy condition and receives an I PDU whose N(S) is equal to its V(R), the station shall accept the information field of this PDU, increment by 1 its V(R), and act as follows:

a. If an I PDU is available to be sent, the station shall be able to act as in 5.3.6.2.5.1 and acknowledge the received I PDU by setting N(R) in the control field of the next sent I PDU to the value of its V(R). The station shall also be able to acknowledge the received I PDU by sending an RR PDU with the N(R) equal to the value of its V(R).

b. If no I PDU is available to be sent by the station, then the station shall either:

   (1) send an RR PDU with the N(R) equal to the value of its V(R) at the earliest opportunity; or

   (2) if the received PDU was not a command PDU with the P-bit set to 1, wait for some period of time bounded by the probability of the remote acknowledgment timer expiry, for either an I PDU to become available for transmission or to accumulate additional I PDUs to be acknowledged in a single RR PDU, subject to window size constraints.

c. If receipt of the I PDU caused the station to go into the busy condition with regard to any subsequent I PDUs, the station shall send an RNR PDU with the N(R) equal to the value of its V(R). If I PDUs are available to send, the station shall be able to send them (as in 5.3.6.2.5) prior to or following the sending of the RNR PDU.

When the station is in a busy condition, the station shall be able to ignore the information field contained in any received I PDU on that data-link connection. (See 5.3.6.2.5.10.)

5.3.6.2.5.3 Receiving incorrect PDUs. When the station receives an invalid PDU or a PDU with an incorrect destination or source address, the entire PDU shall be discarded.

5.3.6.2.5.4 Receiving out-of-sequence PDUs. When the station receives one or more I PDUs whose N(S)s are not in the expected sequence, that is, not equal to the current V(R) but is within the receive window, the station may respond by sending a REJ or a SREJ PDU.

5.3.6.2.5.4.1 Reject response. When only one I PDU has been received out-of-sequence before the next respond opportunity, the station shall discard the information field of the I PDU and send a REJ PDU with the N(R) set to the value of V(R). The station shall then discard the information field of all I PDUs until the expected I PDU is correctly received. When receiving the expected I PDU, the station shall acknowledge the PDU, as described in 5.3.6.2.5.2. The station shall use the N(R) and P-bit indications in the discarded I PDU. On a given data-link connection, only one "sent REJ" exception condition from a given station to another given station shall be established at a time. A REJ and SREJ exception condition cannot be active at the same time. A "sent REJ" condition shall be cleared when the requested I PDU is received. The "sent REJ" condition shall be able to be reset when a reject timer time-out function runs out. When the station perceives by reject timer time-out that the requested I PDU will not be received, because either the requested I PDU or the REJ PDU was in error or lost, the station shall be able to resend the REJ PDU up to N2 times to reestablish the "sent REJ" condition. The value of N2 is defined in 5.3.7.1.2.e.

5.3.6.2.5.4.2 Selective reject response. When more than one I PDU has been received out-of-sequence before the next respond opportunity, the station shall retain the information field of the out-of-sequence I PDUs and send a SREJ PDU for each missing I PDU. A station may transmit one or more SREJ PDUs, each containing a different N(R) with the P-bit set to 0. However, a SREJ PDU shall not be transmitted if an earlier REJ condition has not been cleared. When the station perceives by the reject timer time-out that the requested I PDU will not be received, because either the requested I PDU or the SREJ PDU was in error or lost, the station shall be able to repeat the SREJ PDU in order to reestablish the "sent SREJ" condition up to N2 times.

5.3.6.2.5.5 Receiving acknowledgment. When correctly receiving an I or S PDU, even in the busy condition (see 5.3.6.2.5.10), the receiving station shall consider the N(R) contained in this PDU as an acknowledgment for all the I PDUs it has sent on this data-link connection with an N(S) up to and including the received N(R) minus one. The station shall reset the acknowledgment timer when it correctly receives an I or S PDU with the N(R) higher than the last received N(R) (actually acknowledging some I PDUs). If the timer has been reset and there are outstanding I PDUs still unacknowledged on this data-link connection, the station shall restart the acknowledgment timer. If the timer then runs out, the station shall follow the procedures in 5.3.6.2.5.11 with respect to the unacknowledged I PDUs.

5.3.6.2.5.6 Receiving an SREJ PDU. If the received transmission is an SREJ command or response PDU, the I PDU corresponding to the N(R) being rejected shall be retransmitted. If the I PDU is not available for retransmission, a synchronization error exists and the station that received the SREJ PDU shall respond with an RSET PDU.

5.3.6.2.5.7 Receiving an RSET PDU. Upon receipt of the RSET command PDU, the receiving station shall reply with a UA response PDU and shall then set its V(R) to zero for the initiating station.

5.3.6.2.5.8 Receiving an REJ PDU. When receiving an REJ PDU, the station shall set its V(S) to the N(R) received in the REJ PDU control field. The station shall resend the corresponding I PDU as soon as it is available. If other unacknowledged I PDUs had already been sent on that data-link connection following the one indicated in the REJ PDU, then those I PDUs shall be resent by the station following the resending of the requested I PDU. If retransmission beginning with a particular PDU occurs due to check pointing (see 5.3.6.2.5.11) and an REJ PDU is received, which would also start retransmission with the same I PDU [as identified by the N(R) in the REJ PDU], the retransmission resulting from the REJ PDU shall be inhibited.

5.3.6.2.5.9 Receiving an RNR PDU. A station receiving an RNR PDU shall stop sending I PDUs on the indicated data-link connection at the earliest possible time and shall start the busy-state timer, if not already running. When the busy-state timer runs out, the station shall follow the procedure described in 5.3.6.2.5.11. In any case, the station shall not send any other I PDUs on that data-link connection before receiving an RR or REJ PDU, or before receiving an I response PDU with the F-bit set to 1, or before the completion of a resetting procedure on that data-link connection.

5.3.6.2.5.10 Station-busy condition. A station shall enter the busy condition on a data-link connection when it is temporarily unable to receive or continue to receive I PDUs due to internal constraints; for example, receive buffering limitations. When the station enters the busy condition, it shall send an RNR PDU at the earliest opportunity. It shall be possible to send I PDUs waiting to be sent on that data-link connection prior to or following the sending of the RNR PDU. While in the busy condition, the station shall accept and process supervisory PDUs and return an RNR response PDU with the F-bit set to 1 if it receives an S or I command PDU with the P-bit set to 1 on the affected data-link connection. To indicate the clearance of a busy condition on a data-link connection, the station shall send an I response PDU with the F-bit set to 1 if a P-bit set to 1 is outstanding, an REJ response PDU, or an RR response PDU on the data-link connection with N(R) set to the current V(R), depending on whether or not the station discarded information fields of correctly received I PDUs. Additionally, the sending of a SABME command PDU or a UA response PDU shall indicate the clearance of a busy condition at the sending station on a data-link connection.

5.3.6.2.5.11 Waiting acknowledgment. The station maintains an internal retransmission count variable for each data-link connection, which shall be set to 0 when the station receives or sends a UA response PDU to a SABME command PDU, when the station receives an RNR PDU, or when the station correctly receives an I or S PDU with the N(R) higher than the last received N(R) (actually acknowledging some outstanding I PDUs). If the acknowledgment timer, busy-state timer, or the P-bit timer runs out, the station on this data-link connection shall enter the timer recovery condition and add 1 to its retransmission count variable. The station shall then start the P-bit timer and send an S command PDU with the P-bit set to 1. The timer recovery condition shall be cleared on the data-link connection when the station receives a valid I or S PDU from the remote station with the F-bit set to 1. If, while in the timer recovery condition, the station correctly receives a valid I or S PDU with:

a. the F-bit set to 1 and the N(R) within the range from the last value of N(R) received to the current V(S) inclusive, the station shall clear the timer recovery condition, set its V(S) to the received N(R), stop the P-bit timer, and resend any unacknowledged PDUs; or

b. the P/F bit set to 0 and the N(R) within the range from the last value of N(R) received to the current V(S) inclusive, the station shall not clear the timer recovery condition but shall treat the N(R) value received as an acknowledgment for the indicated previously transmitted I PDUs. (See 5.3.6.2.5.5.)

If the P-bit timer runs out in the timer recovery condition, the station shall add 1 to its retransmission count variable. If the retransmission count variable is less than N2, the station shall resend an S PDU with the P-bit set to 1 and restart its P-bit timer. If the retransmission count variable is equal to N2, the station shall initiate a resetting procedure, by sending a SABME command PDU, as described in 5.3.6.2.6. N2 is a system parameter defined in 5.3.7.1.2.e.

5.3.6.2.6 Procedures for mode resetting. The resetting phase is used to initialize both directions of information transfer according to the procedure described in 5.3.6.2.6.1 through 5.3.6.2.6.3. The resetting phase shall apply only during ABM. Either station shall be able to initiate a resetting of both directions by sending a SABME command PDU and starting its acknowledgment timer.

5.3.6.2.6.1 Receiver action. After receiving a SABME command PDU, the station shall return one of two types of responses, at the earliest opportunity:

a. a UA response PDU and reset its V(S) and V(R) to 0 to reset the data-link connection, or

b. a DM response PDU if the data-link connection is to be terminated.

The return of the UA or DM response PDU shall take precedence over any other response PDU for that data-link connection that may be pending at the station. It shall be possible to follow the UA PDU with additional PDUs, if pending.

5.3.6.2.6.2 Initiator action. If the UA PDU is received correctly by the initiating station, it shall reset its V(S) and V(R) to 0 and stop its acknowledgment timer. This shall also clear all exception conditions that might be present at either of the stations involved in the reset. The exchange shall also indicate clearance of any busy condition that may have been present at either station involved in the reset. If a DM response PDU is received, the station shall enter the data-link disconnected phase, shall stop its acknowledgment timer, and shall report to the higher layer for appropriate action. If the acknowledgment timer runs out before a UA or DM response PDU is received, the SABME command PDU shall be resent and the acknowledgment timer shall be started. After the timer runs out N2 times, the sending station shall stop sending the SABME command PDU, shall report to the higher layer for the appropriate error recovery actions to initiate, and shall enter the ADM. The value of N2 is defined in 5.3.7.1.2.e. Other Type 2 PDUs, with the exception of the SABME and DISC command PDUs, received by the station before completion of the RSET procedure shall be discarded.

5.3.6.2.6.3 Resetting with the FRMR PDU. Under certain FRMR exception conditions (listed in 5.3.6.2.8), it shall be possible for the initiating station, by sending an FRMR response PDU, to ask the remote station to reset the data-link connection. Upon receiving the FRMR response PDU (even during a FRMR exception condition), the remote station shall either initiate a resetting procedure, by sending a SABME command PDU, or initiate a disconnect procedure, by sending a DISC command PDU. After sending an FRMR response PDU, the initiating station shall enter the FRMR exception condition. The FRMR exception condition shall be cleared when the station receives or sends a SABME or DISC command PDU or DM response PDU. Any other Type 2 command PDU received while in the FRMR exception condition shall cause the station to resend the FRMR response PDU with the same information field as originally sent. In the FRMR exception condition, additional I PDUs shall not be sent, and received I and S PDUs shall be discarded by the station. It shall be possible for the station to start its acknowledgment timer on the sending of the FRMR response PDU. If the timer runs out before the reception of a SABME or DISC command PDU from the remote station, it shall be possible for the station to resend the FRMR response PDU and restart its acknowledgment timer. After the acknowledgment timer has run out N2 times, the station shall reset the data-link connection by sending a SABME command PDU. The value of N2 is defined in 5.3.7.1.2.e. When an additional FRMR response PDU is sent while the acknowledgment timer is running, the timer shall not be reset or restarted.

5.3.6.2.7 Procedures for sequence number resetting. This resetting procedure, employing the RSET command, is used to reinitialize the receive-state variable V(R) in the addressed station and the send-state variable V(S) in the local station. The addressed station shall confirm acceptance of the RSET command by transmission of a UA response at the earliest opportunity. Upon acceptance of this command, the addressed station V(R) shall be set to 0. If the UA response is received correctly, the initializing station shall reset its V(S) to 0. The RSET command shall reset all PDU rejection conditions in the addressed station, except for an invalid N(R) sequence number condition, which the addressed station has reported by a FRMR PDU. The RSET command may be sent by the station that detects an invalid N(R) to clear such a frame rejection condition in place of sending a FRMR frame. To clear an invalid N(R) frame rejection condition with an RSET command, the RSET command shall be transmitted by the station that detects the invalid N(R). When the RSET command is transmitted, the responsibility for all unacknowledged I PDUs reverts to a higher level. Whether the content of the information field of such acknowledged I PDUs is reassigned for transmission or not is decided at a higher level.

5.3.6.2.8 FRMR exception conditions. The station shall request a resetting procedure by sending an FRMR response PDU, as described in 5.3.6.2.6, after receiving, during the information transfer phase, a PDU with one of the conditions identified in 5.3.5.2.3.6. The coding of the information field of the FRMR response PDU that is sent is given in 5.3.5.2.3.6. The other station shall initiate a resetting procedure by sending a SABME command PDU, as described in 5.3.6.2.6, after receiving the FRMR response PDU.

5.3.7 Data-link initialization. The XID command and response messages, formatted as shown in Table III and described in Appendix E, are used to establish and control link parameters. The join network request message contains the link operating parameters such as keytime delay, priority, and net access method. Initialization is caused by an operator or system request. The Join Request is sent to the default network control (NETCON) destination address, which shall be the station assigned to perform NETCON station responsibilities. The NETCON station verifies link parameters and provides values for missing or incorrect parameters to ensure that the new station will not disrupt the net. The NETCON station will reply with either a Join Reject or Join Accept PDU. If the initializing station receives a Join Reject PDU, it should not attempt any link activity until the correct parameters have been obtained.

NOTE: Link initialization may also occur without an XID PDU exchange. Prearrangement by timing, voice, written plans, or orders provides the operator with the necessary frequency, link address, data rate, and other parameters to enter a net and establish a link. With the prearranged information, an operator may begin link activity on the net and initialization is assumed when the new station senses the net and transmits its first message.

5.3.7.1 List of data-link parameters. This MIL-STD defines a number of data-link parameters for which the system-by-system range of values are determined at network establishment. The definitions of these parameters for the two types of operation are summarized in 5.3.7.1.1 through 5.3.7.1.2.

5.3.7.1.1 Type 1 logical data-link parameters. The logical data-link parameters for Type 1 operation shall be as follows:

a. Acknowledgment timer. The acknowledgment timer is a data-link parameter that shall define the timeout period (TP) during which the station shall expect an acknowledgment from a specific station. TP shall take into account any delay introduced by the physical sublayer. The value of TP is described in Appendix C.

b. Busy-state timer. The busy-state timer is a data-link parameter that defines the time interval following receipt of the URNR command PDU during which the station shall wait for the other station to clear the busy condition. Its value shall be no less than three times the acknowledgment timer.

c. Maximum number of transmissions, N4. N4 is a data-link parameter that indicates the maximum number of times that an UI or XID command PDU is sent by a station trying to accomplish a successful information exchange. Normally, N4 is set large enough to overcome the loss of a PDU due to link error conditions. The maximum number of times that a PDU is retransmitted following the expiration of the acknowledgement timer is established at protocol initialization. This value is in the range of 0 through 5 and defaults to 2. The retransmission of PDUs may be overridden by the Response Mode parameter, which is described in 5.3.10.2, or the Number of Retransmissions parameter of the DL-Unitdata Request, described in 5.3.14.

d. Maximum number of octets in a UI PDU. This is a data-link parameter that denotes the maximum number of octets in a UI PDU. The maximum number of octets, also referred to as maximum transmission units (MTUs), is 3,524.

e. Minimum number of octets in a PDU. The minimum-length valid data-link PDU shall contain 2 flags, 2 addresses, one 8-bit control field, and the FCS. The minimum number of octets in a valid data-link PDU shall be 9.

5.3.7.1.2 Type 2 data-link parameters. The data-link connection parameters for Type 2 operation shall be as follows:

a. Acknowledgment timer. The acknowledgment timer is a data-link connection parameter that shall define the time interval during which the station shall expect to receive acknowledgment to one or more outstanding I PDUs or an expected response to a sent U command PDU. Time values are established at protocol initialization and are in the range of 1 to 30 minutes in 30-second increments, and of 0 to 1 minute in 1-second increments. An instance of the acknowledgment timer may be adjusted according to the number of destination addresses in the frame. Default is 2 minutes.

b. P-bit timer. The P-bit timer is a data-link connection parameter that defines the time interval during which the station shall expect to receive a frame with the F-bit set to 1 in response to a sent Type 2 command with the P-bit set to 1. Time values are established at protocol initialization and are in the range of 10 to 60 seconds in increments of 1 second. Default is 10 seconds.

c. Reject timer. The reject (REJ) timer is a data-link connection parameter that defines the time interval during which the station shall expect to receive a reply to a sent REJ PDU. The reject timer value shall be equal to or less than twice the acknowledgment timer.

d. Busy-state timer. The busy-state timer is a data-link connection parameter that defines the time interval that a station shall wait, following receipt of the RNR PDU, for the other station to clear the busy condition. The busy-state timer value shall be no less than three times the acknowledgment timer.

e. Maximum number of transmissions, N2. N2 is a data-link connection parameter that indicates the maximum number of times that a PDU is sent, following the running out of the acknowledgment timer, the P-bit timer, or the reject timer. The maximum number of times that a PDU is retransmitted following the expiration of the timers is established at protocol initialization. This value is in the range of 0 through 5 and defaults to 2. The retransmission of PDUs may be overridden by either of two parameters: the Response Mode parameter, which is described in 5.3.10.2; or the Number of Retransmissions parameter of the DL-Unitdata Request, which is described in 5.3.14.

f. Maximum number of octets in an I PDU, N1. N1 is a data-link connection parameter that denotes the maximum number of octets in an I PDU. The default is 3,555 octets.

g. Maximum number of outstanding I PDUs, *k*. The maximum number (*k*) of sequentially numbered I PDUs that the station may have outstanding (that is, unacknowledged) at any given time is a data-link connection parameter, which shall never exceed 127. A lower value for *k* may be established using the XID Join Message.

h. Minimum number of octets in a PDU. A minimal-length valid data-link connection PDU shall contain exactly 2 flags, 2 address fields, 1 control field, and the FCS. Thus, the minimum number of octets in a valid data-link connection PDU shall be 9 or 10, depending on whether the PDU is a U PDU, or an I or S PDU, respectively.

5.3.8 Frame transfer. After the station has joined the net, it can begin to send frames. The data-link layer shall request the transmission of a frame by issuing a Unitdata request to the physical layer.

5.3.8.1 Type 1 PDU transmission. The data-link layer initiates transmission by building a transmission unit and passing it to the physical layer. The elements of a transmission unit include one or more (see data-link concatenation below) Type 1 PDUs (flag-to-flag), the inserted 0 bits, an optional FEC code, and an optional time dispersal code. To request transmission, a physical layer (PL) Unitdata request is issued by the data-link layer protocol after a transmission unit has been constructed. If the random net access scheme is active, a PL-unitdata request shall be issued for each transmission unit in first-in first-out order. If a prioritized net access scheme is active, a PL-unitdata request shall be issued for each transmission unit in priority order. Transmission units of the same priority shall be in first-in first-out order. For any net access scheme that considers access priority, only PDUs at an equal or higher access priority shall be concatenated with other PDUs. Not all Type 1 PDUs may be concatenated at the data-link layer or physical layer. Only PDUs that do not require a TP timer (acknowledgment) may be concatenated by using one of the methods described in 5.3.8.1.1 and 5.3.8.1.2.

5.3.8.1.1 Type 1 data-link concatenation. The sending station may concatenate certain PDUs by using one or two flags to separate each PDU. The combined length of the concatenated PDUs, before 0-bit insertion, may not exceed the established maximum PDU size for a single PDU (see 5.3.7.1.1.e). The PDUs are concatenated after the 0-bit insertion algorithm is applied. FEC, with or without TDC, is optionally applied before the transmission unit is passed to the physical layer in a PL-unitdata request. Type 1 data-link concatenation is shown in Figure 17.

5.3.8.1.2 Type 1 physical-layer concatenation. More than one PDU (if they are not concatenated at the data-link layer) may be passed to the physical layer without waiting for an intervening net-access delay period. The combined length of all the PDUs, before 0-bit insertion, shall not exceed the maximum PDU size for a single PDU. PDUs concatenated by the physical layer may not require a TP timer to be set by the sending station. The physical layer shall transmit each transmission unit following the complete physical layer procedures but without an intervening delay. Type 1 physical layer concatenation is shown in Figure 18.

5.3.8.2 Type 2 PDU transmission. The data-link layer initiates transmission by building a transmission unit and passing it to the physical layer. The elements of a transmission unit include one or more (see data-link concatenation, below) Type 2 PDUs (flag-to-flag), the inserted 0 bits, an optional FEC code, and an optional TDC. To request transmission, a PL unitdata request is issued by the data-link layer protocol after a transmission unit has been constructed. If the random net access scheme is active, a PL-unitdata request shall be issued for each transmission unit in first-in first-out order. If a prioritized net access scheme is active, a PL-unitdata request shall be issued for each transmission unit in priority order. Transmission units of the same priority shall be in first-in first-out order. Any Type 2 PDUs may be concatenated at the data-link layer or physical layer. For any net access scheme that considers access priority, only PDUs at an equal or higher access priority shall be concatenated with other PDUs.

5.3.8.2.1 Type 2 data-link concatenation. The sending station may concatenate any PDUs by using one or two flags to separate each PDU. The combined length of the concatenated PDUs, before 0-bit insertion, may not exceed the established maximum PDU size for a single PDU (see 5.3.7.1.1.c). The PDUs are concatenated after the 0-bit insertion algorithm is applied. FEC, with or without TDC, is optionally applied before the transmission unit is passed to the physical layer in a PL-unitdata request. Type 2 data-link concatenation is shown in Figure 19.

5.3.8.2.2 Type 2 physical-layer concatenation. More than one PDU (if they are not concatenated at the data-link layer) may be passed to the physical layer without waiting for an intervening net-access delay period. The combined length of all the PDUs, before 0-bit insertion, shall not exceed the maximum PDU size for a single PDU. The physical layer shall transmit each transmission unit following the complete physical layer procedures, but without an intervening delay. Type 2 physical layer concatenation is shown in Figure 20.

5.3.8.3 Type 1 and Type 2 PDU transmissions. Type 1 and Type 2 PDUs shall be queued for transmission without regard to the PDU type. If the random net-access scheme is active, both Type 1 and Type 2 PDUs are placed in a single first-in first-out ordered queue. If the prioritized net access scheme is active, both Type 1 and Type 2 PDUs are placed in the appropriate priority-level queue, with each level queue using a single first-in first-out order. If the first PDU in the highest priority level queue (or only queue) may be concatenated, then other PDUs may be concatenated with that PDU even if a PDU that does not allow concatenation is queued ahead of them. The PDU that did not allow concatenation shall be at the head of its appropriate queue for the next net access period. If the first PDU in the highest priority level queue (or only queue) does not allow concatenation, it shall be the only PDU transmitted in that net access period.

5.3.9 Flow control. Flow control provides the capability of reducing the allowed input rate of information to prevent congestion to the point where normal operation may become impossible. The control-field sequence numbers are available for this service.

5.3.9.1 Type 1 flow control. Type 1 transmissions can be acknowledged or unacknowledged. Acknowledged and unacknowledged operations can perform flow control using URR and URNR messages. These messages announce the station's ability to accept incoming frames.

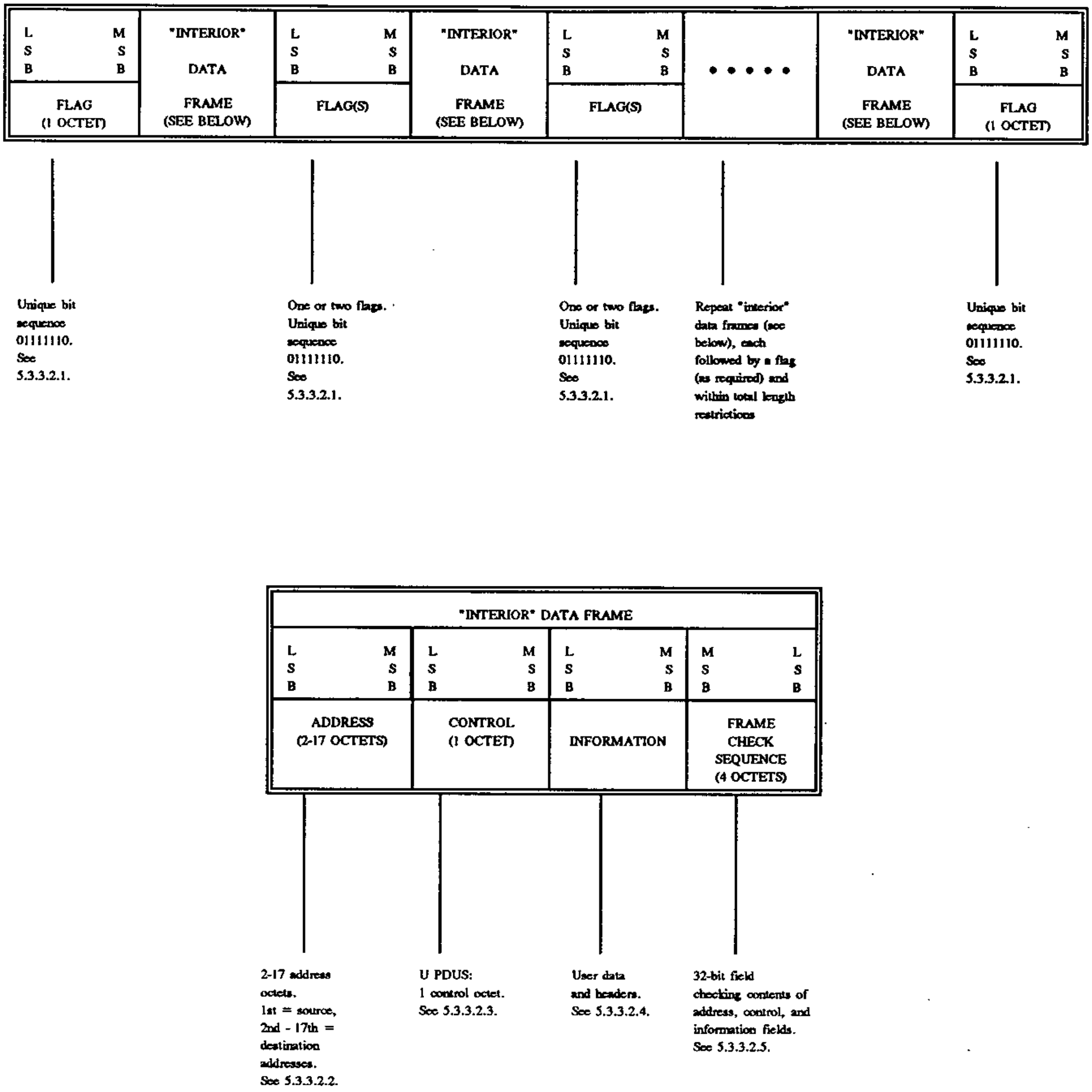


Figure 17. Type 1 data-link concatenation.

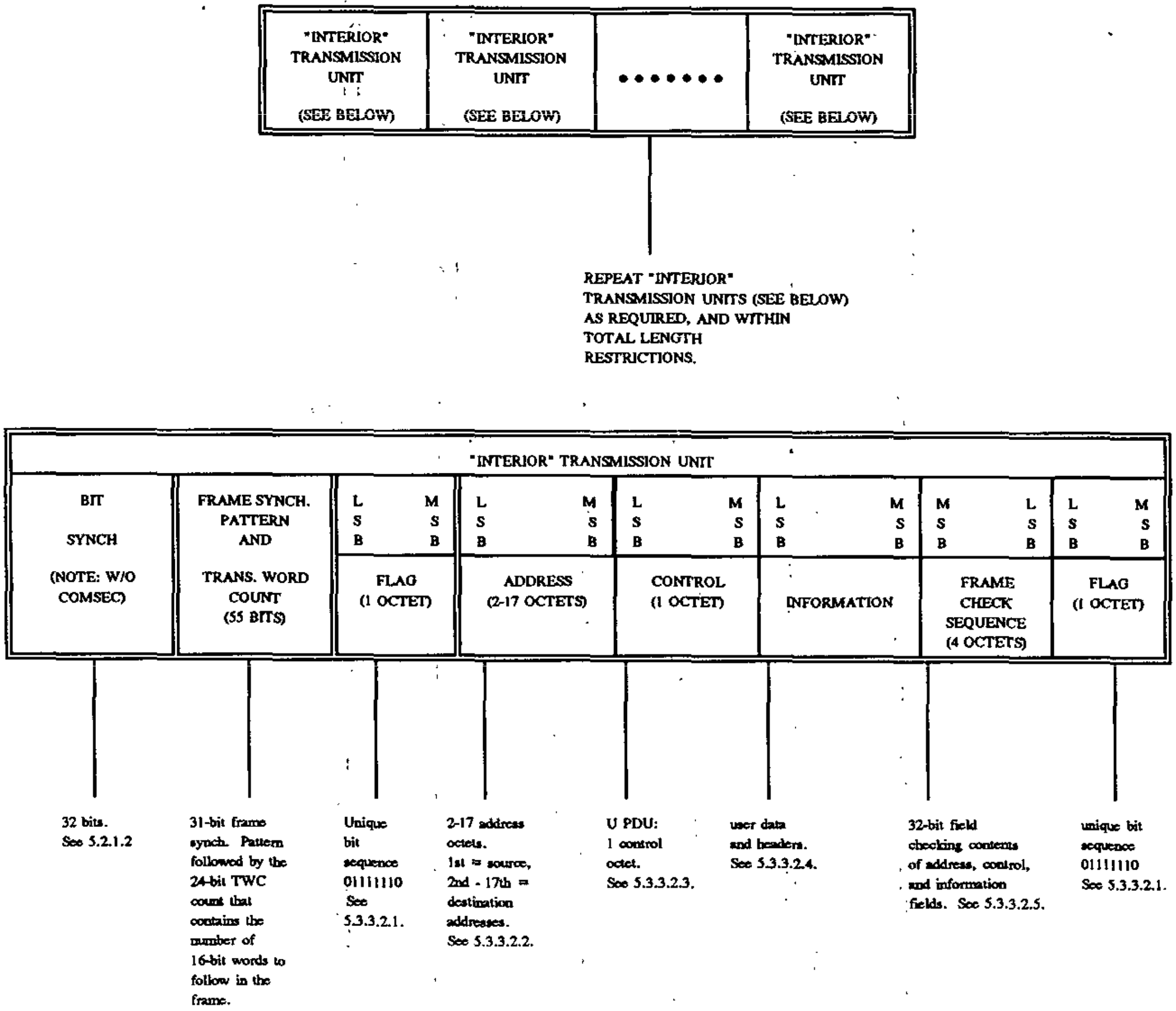


Figure 18. Type 1 physical-layer concatenation.

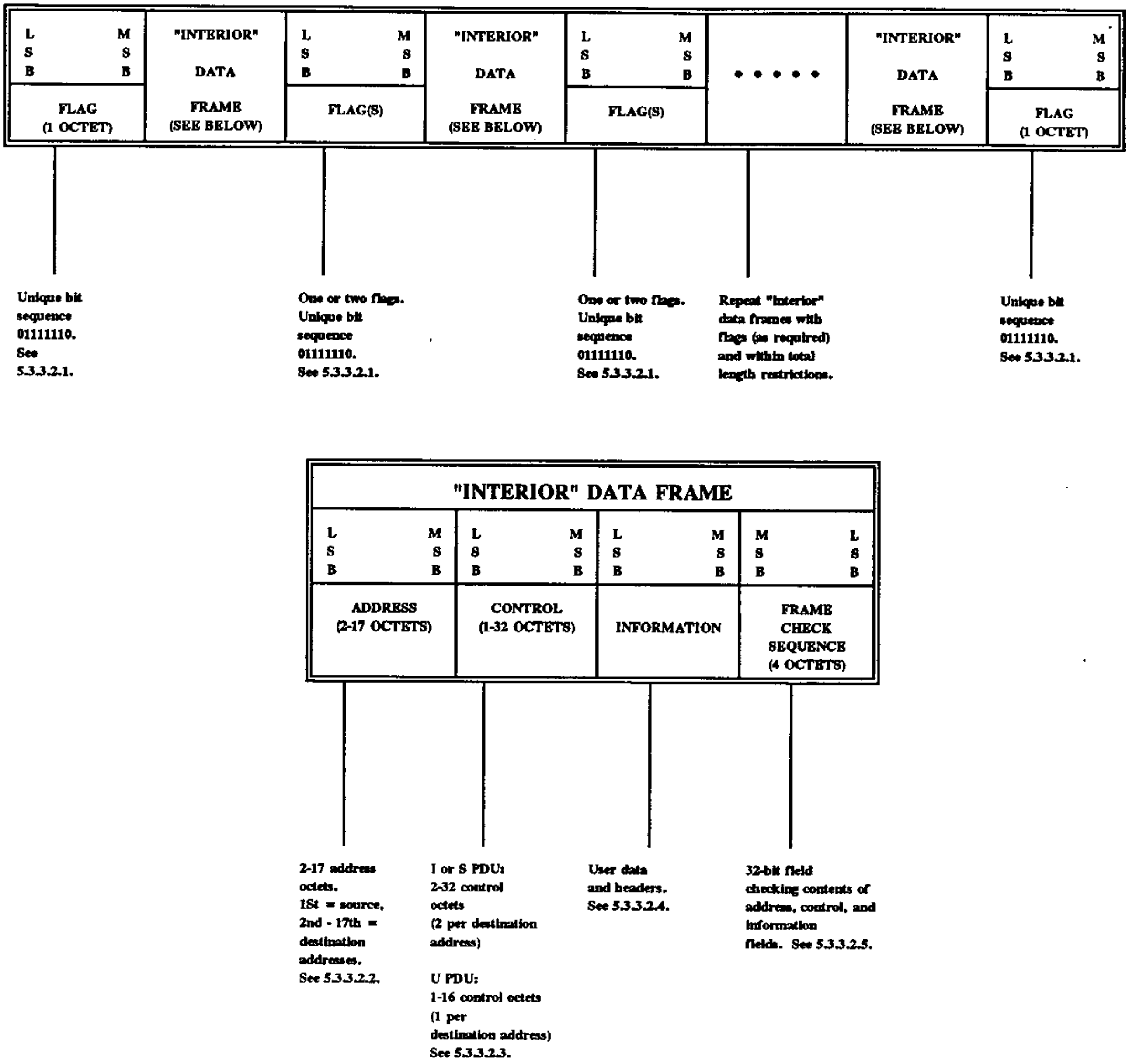


Figure 19. Type 2 data-link concatenation.

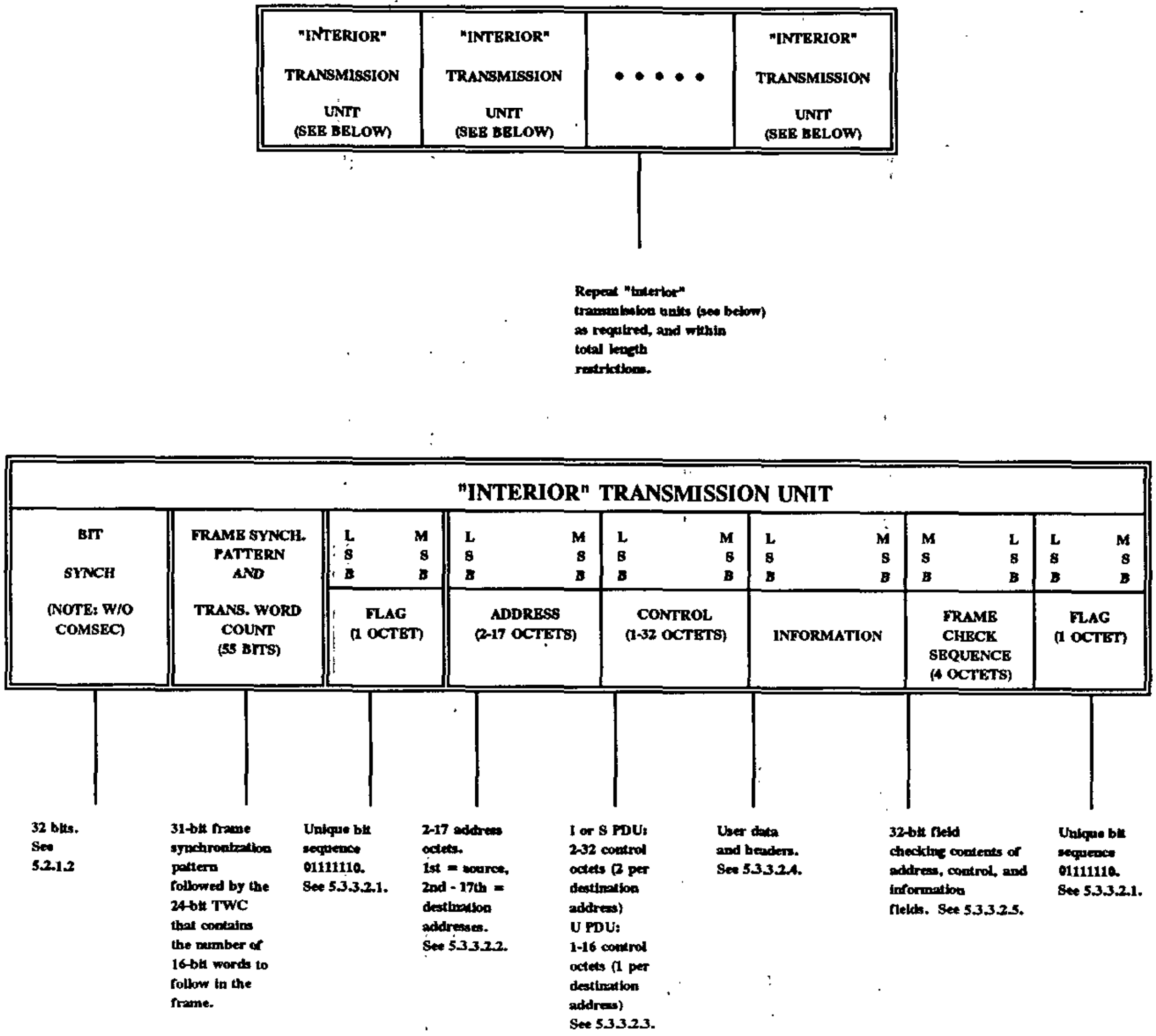


Figure 20. Type 2 physical-layer concatenation.

5.3.9.2 Type 2 flow control. The send and receive sequence numbers, N(S) and N(R), are used in conjunction with the send- and receive-state variables, V(S) and V(R), to control data flow. Flow control is implemented by the window method. The window defines the maximum number of undelivered frames a given user may have outstanding. The maximum number (*k*) of sequentially numbered I PDUs that may be outstanding (that is, unacknowledged) at any given time is a data-link connection parameter, which shall never exceed 127. The incremental updating of N(R) acts as the positive acknowledgment of transmitted frames up to, but not including, that frame number. The window flow-control mechanism requires that the highest sequence number transmitted by the user be less than the sum of the last received N(R) plus *k*. Window size (*k*) is a feature that is agreed upon by the users at initialization. The larger the window, the greater the traffic loading a given user places on a single channel. If flow control requires that the window must be limited, an XID exchange can be used to temporarily reduce the value of *k*.

5.3.10 Acknowledgment and response. All UI or I PDUs that require an acknowledgment shall be acknowledged except for the five cases listed below:

a. the control field of the received PDU specifies that no acknowledgment is required,

b. the response mode (described in 5.3.10.1), has been set to Off,

c. the receiving station is a group (including global) addressee only,

d. the receiving station's individual address is not in the address field, and

e. the PDU is invalid.

5.3.10.1 Acknowledgment. Acknowledgments are applicable for both Type 1 and Type 2 operations.

5.3.10.1.1 Type 1 acknowledgment. Each PDU, with the P-bit set to 1, shall be acknowledged before another PDU is transmitted. This is defined as a coupled acknowledgment. All UI, TEST, and XID command PDUs that have the P-bit set to 1 shall be acknowledged. The RHD procedures (see Appendix C) shall be followed by all stations on the network to allow each responding station an interval in which they can transmit their acknowledgment.

5.3.10.1.2 Type 2 acknowledgment. I, SABME, and DISC PDUs shall activate the acknowledgment timer. The Type 2 operation does not use the RHD timer, which allows receiving stations to send their acknowledgments during the current net access period. All acknowledgments are transmitted in another net access period. The priority of a response PDU is discussed in Appendix C. An I PDU acknowledgment does not necessarily correspond on a one-to-one basis with the I PDU and does not necessarily apply to the immediately preceding I PDU.

5.3.10.2 Response mode. The protocol shall allow an operator to initiate Response mode as an override feature that, when invoked, prevents any transmission (including retransmission) without explicit permission from the operator. As a security feature, the operator shall be able to turn off automatic transmissions but still continue to receive. Normal protocol exchanges shall occur when the response mode is ON. Only the operator can initiate a transmission when the Response mode is OFF. The Response mode shall override the Number of Retransmissions parameter in the DL-unitdata request. The default value of the Response mode is ON. If the Response mode is OFF during Type 2 operations, the flow control mechanism and retransmission timers may cause the connection to be lost.

5.3.11 Invalid frame. A frame is invalid if it has one or more of the following characteristics:

a. not bounded by a beginning and ending flag,

b. too short,

c. too long,

d. has an invalid address or control field, and

e. has an FCS error.

A frame is too short if it contains less than 9 bytes. A frame is too long if it exceeds the maximum PDU length as described in 5.3.7.1.1.e for Type 1 and 5.3.7.1.2.f for Type 2. Any invalid frame shall be discarded.

5.3.12 Retransmission. The data-link layer will retransmit a command frame waiting for a response. The default number of retransmissions is 2, but the data-link layer protocol may be initialized to automatically retransmit 0 to 5 times. An operator may override the system settings by requesting the number of retransmissions in the application layer request. The network layer shall provide the retransmission parameter value in the data-link unitdata request (see 5.3.14). If the response mode is OFF, no automatic retransmissions shall be made.

5.3.13 Error detection and correction. FEC coding alone, or FEC coding in unison with TDC, may be used to provide error detection and correction (EDAC) capabilities to compensate for errors induced during transmission. If selected, the FEC process shall be used to encode the data-link frame of 5.3.3. If selected, the

TDC process shall be applied to the FEC-encoded data-link frame and to the fill bits. Three modes of EDAC shall be supported: EDAC OFF, EDAC ON with TDC, and EDAC ON without TDC (NOTE: EDAC ON without TDC may be used when the transmission channel provides the TDC capability). The EDAC mode shall be selectable.

5.3.13.1 Forward-error-correction coding. When FEC is selected, the half-rate Golay (24,12,7) cyclic block code, described in detail in Appendix F, shall be used for FEC. The half-rate Golay (24,12,7) codeword block shall be formed by adding a zero to the Golay (23,12,7) codeword block. The generator polynomial to obtain the 11 check bits shall be

$$g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

where

$$g(x) \textit{ is a factor of } x^{23} + 1$$

5.3.13.2 Forward-error-correction preprocessing. When FEC is selected, data bits shall be divided into a sequence of 12-bit segments for Golay encoding. The total number of segments shall be an integral number. If the data bits do not divide into an integral number of segments, fill bits, consisting of 1 to 11 0's, shall be added at the end to form an integral number of segments. A URR response PDU shall be duplicated, including the beginning and ending flag, when TDC is selected. Fill bits shall be added to an S, URR, and URNR Frame and may be added to an I, UI, and XID Frame. When the frame length is less than 96 bits, and the TDC is selected, the entire frame is reproduced within the transmission. This provides a station with two opportunities to receive an error-free frame.

5.3.13.3 Time-dispersive coding. TDC bit interleaving may be selected in unison with FEC. When TDC is selected, data shall be formatted into a sequence of TDC blocks composed of sixteen 24-bit Golay (24, 12) codewords (that is, there are 384 FEC-encoded bits per TDC block). Each TDC block shall contain a total of 16 FEC codewords. If the last TDC block of a message contains less than 16 FEC codewords, fill codewords shall be added to complete the TDC block. These 24-bit fill codewords shall be created by Golay-encoding an alternating sequence of 12-bit data words, with the first word composed of 12 ones followed by a word composed of 12 zeros. The fill codewords shall alternate until the TDC block is filled. The TDC block shall be structured into a 16 x 24 matrix (the Golay codewords appear as rows), as shown in Figure 21. (A_1 through A_{24} are the bits of the first Golay codeword. A_{25} is the first bit of the second Golay codeword). Each TDC block matrix shall be rotated to form a 24 x 16 matrix. The Golay codewords now appear as columns, as shown in Figure 22. The TDC block is transmitted row by row with the LSB (A_1) of the first row first. At the receiver, the TDC-encoded bit stream shall be structured into a 24 x 16 matrix. Each received TDC block matrix shall be rotated to form the original 16 x 24 matrix, as shown in Figure 21. The TDC decoder at the receiver shall perform the inverse of the TDC encoding process.

A_1	A_2		A_{23}	A_{24}
A_{25}	A_{26}		A_{47}	A_{48}
A_{49}	A_{50}		A_{71}	A_{72}
A_{361}	A_{362}		A_{383}	A_{384}

Golay Codeword in each row
A_1, A_2, A_3, . . . , A_{24}

Figure 21. 16 x 24 matrix before interleaving.

A_1	A_{25}		A_{337}	A_{361}
A_2	A_{26}		A_{338}	A_{362}
A_3	A_{27}		A_{339}	A_{363}
A_{24}	A_{48}		A_{360}	A_{384}

Golay codeword in each column
Transmit sequence: row by row
A_1, A_{25}, . . . , A_{337}, A_{361}

Figure 22. Transmitter's 24 x 16 matrix after interleaving.

5.3.14 Link layer interactions. The data-link layer interacts with both the next higher and next lower layer to pass or receive information regarding services requested or performed. Three primitives are used to pass information for the sending and receiving of data across the upper layer boundary.

a. Requests for transmission of data are sent by the upper layer, using the data-link layer (DL) unitdata request primitive, with the following parameters:

DL-Unitdata Request	Destination(s)
	Source
	Quality of Service
	Precedence
	Type of Service
	Reliability Requested
	Type 2 Poll-Bit Setting
	Number of Retransmissions
	Data/Data Length

b. Indications are provided to the upper layer when data is received through the unitdata Indication primitive, with the following parameters:

DL-Unitdata Indication	Destination
	Source
	Quality of Service
	Reliability Requested
	Type of Service
	Type 2 Poll-Bit Setting
	Data/Data length
DL Status Indication	Acknowledgment failure
	Connection

c. Descriptions of the above parameters follow:

(1) The destination can be 1 to 16 individual or multicast (including global) addresses.

(2) The source address is the individual address of the outgoing link.

(3) Quality-of-service parameters are used in determining the service provided by the data-link layer.

(a) Precedence parameters are used by the prioritized transmission scheme and can be used to order outgoing queues. The precedence levels available to the network will be mapped into three levels (urgent, priority, and routine) in the data-link layer. Precedence levels in the network layer shall be mapped as follows:

Network Precedence	**Data-Link Precedence**
System Control (SYSCON) URGENT	URGENT
PRIORITY	PRIORITY
ROUTINE	ROUTINE

The data-link level will take SYSCON and URGENT and map them into URGENT, which is the highest precedence for the prioritized transmission scheme.

(b) Type of Service is a parameter to request Type 1 (connectionless) or Type 2 (connection-oriented) operations of the data-link layer. It is also used to inform the network layer of the type-of-service delivery requirements for data forwarded to another system.

(c) Reliability requested parameter is the reliability variable used to indicate if a Type 1 data-link acknowledgment is to be requested.

(d) Type 2 Poll-Bit Setting is used to request that the poll bit be set in the I PDU containing the data in this request. It is also used to inform the network layer of the poll-bit-setting delivery requirements for data forwarded to another system.

(e) Number of Retransmissions is the variable used to provide to the data-link layer the number of automatic retransmissions allowed. Legal values of the parameter are 0 to 5.

(4) Data/Data Length is the block of data exchanged between the data-link layer and its upper layer user, and an indication of the data's length.

(5) Acknowledgment Failure is an indicator to inform the upper layer if a Type 1 data-link acknowledgment was not received from the remote station when reliability was requested.

(6) Connection is an indicator to inform the upper layer if a Type 2 connection has been established or disconnected.

5.4 Network layer. The network layer shall be used to route data within the network. The broadcast protocol shall provide the means for routing, packet addressing, precedence, and interconnection.

5.4.1 Network protocol data unit. The network PDU (NPDU) shall be composed of a network header and data, as shown in Figure 23.

Network Header	Data

FIGURE 23. Network protocol data-unit structure.

5.4.2 Network header. The network header shall consist of 10 fields, as shown in Table V. The joining of network header fields shall occur before the data is passed to the data-link layer. The network header shall be linearly joined (constructed) in order from field 1 through field 9. If a field consists of multiple American Standard Code for Information Interchange (ASCII) characters, the leftmost character shall be joined first. If a field consists of multiple binary-coded decimal (BCD) digits, the leftmost digit is the high order digit and shall be joined first. Field 9 may be repeated to contain up to 16 routing indicators (RIs).

5.4.2.1 Field 1 - version number. This field shall indicate the network header version number. This 4-bit field shall have the signed decimal value of -1 (binary 1111). In the future, this field may have allowable values from -1 through 14. The version number is used to distinguish the received header format from other versions of the network header that may have existed previously. Packets received with a version number value other than the approved numbers shall be discarded.

5.4.2.2 Field 2 - time-to-live. The time-to-live field shall indicate the maximum amount of time the NPDU may remain in the network. It shall be an unsigned integer from 0 to 15. This field places an upper bound on the lifetime of the NPDU to prevent systems from continuously forwarding an undeliverable NPDU due to erroneous routing information. The field may also be used to discard NPDUs that have not been delivered during the lifespan of the data. (Data may become obsolete after a period of time, due to the transmission of more current information or a retransmission of the original data.) Each network layer that receives the NPDU shall decrement this field by 1. Once the field is decremented to 0, the NPDU may be locally processed but it shall not be forwarded.

TABLE V. Network header fields.

E	end-of-message
SSN	Station Serial Number
L	Destination List Bit
R	Reserved
ORI	Originator Routing
D	Delivery/Redundancy
J	Final/Intermediate (0/1)
DRI	Destination Routing

(up to 16 DRIs)

8 (MSB)	7	6	5	4	3	2	1 (LSB)
[1] VERSION NUMBER				[2] TIME-TO-LIVE			
[3] MESSAGE FRAME NUMBER							
E	1st DIGIT			2nd DIGIT			
[4] SSN 1st DIGIT				SSN 2nd DIGIT			
SSN 3rd DIGIT				[5] PRECEDENCE			
[6] CLASSIFICATION				[7] MESSAGE TYPE			
L	R	R	ORI AREA CODE [8]				
R	R	R	ORI SUBNET CODE				
R	R	R	ORI SYSTEM CODE				
D	R	J	DRI AREA CODE [9]				
R	R	R	DRI SUBNET CODE				
R			DRI SYSTEM CODE				
⋮			⋮				
D	R	J	DRI AREA CODE				
R	R	R	DRI SUBNET CODE				
R			DRI SYSTEM CODE				
END OF ROUTING [10]							

5.4.2.3 Field 3 - message frame number. This field shall be used to designate the sequential order of frames (packets) making up the NPDU. The field shall contain two BCD digits. The first frame of each NPDU shall be designated 01 to identify the start of message. Subsequent frames (if any) shall be numbered sequentially to a maximum of 40. The last frame segment shall have the MSB of the first digit set to 1 (E bit) to designate this frame as the end of message. The message frame number for an NPDU that is not segmented shall be 81 BCD (1000 0001) to indicate a 1-frame message.

5.4.2.4 Field 4 - station serial number. This field shall be used to sequentially identify the message that the station is sending over the link. The field shall be 12 bits long. The field shall be coded by using a 4-bit BCD for each decimal digit.

The station serial number (SSN) shall be represented by values ranging from 000-999. The SSN shall be incremented by 1 each time a message NPDU is generated by the station. When the SSN value is 999, and it is incremented by 1, it shall be set to 000.

5.4.2.5 Field 5 - tactical system message precedence. This field shall be used to specify the precedence of the message. The field shall be 4 bits long. The precedence levels shall be coded as shown in Table VI.

TABLE VI. Message precedence levels.

PRECEDENCE	CODE
SYSCON (network control)	0001
Urgent	0010
Priority	0011
Routine	0100-1111

MSB LSB

5.4.2.6 Field 6 - security classification. This field shall be used to specify the security classification of the message. This field shall be 4 bits long. The selected security classification level shall not exceed the classification level of the link. The classification levels shall be coded as shown in Table VII.

TABLE VII. Security classifications.

CLASSIFICATION LEEL	CODE
Top Secret	1000
Secret	0100
Confidential	0010
Unclassified	0001

MSB LSB

5.4.2.7 Field 7 - message type. This field shall be used to identify the basic types of messages that will be in the user data field. This field shall be 4 bits long. The types of messages shall be coded as shown in Table VIII. In the future, SYSCON messages may be generated by the network protocol for control and management of the network. Perishable messages contain information that has value for a limited time period. Nonperishable messages contain information of lasting value.

TABLE VIII. Types of messages.

MESSAGE	CODE
SYSCON	1111
Nonperishable K Series	1110
Perishable K Series	0111

MSB LSB

5.4.2.8 Field 8 - originator routing indicator (ORI). This field shall contain the RI of the message originator and the destination list bit, bit L in Figure 24, which is used to interpret field 9. The field shall be 24 bits long. An ORI is the network layer source address. The interpretation of the addresses for routing purposes (that is, area, subnet, and system codes) depends on the network configuration chosen by the network authority.

Originator Routing Indicator Subfields

MSB LSB

L Bit	Subfield 1	Subfield 2	Subfield 3

L Bit = 0 Field 9 represents multiple destinations
L Bit = 1 Field 9 represents a path to a single destination

Destination Routing Indicator Subfields

MSB LSB

D Bit		J Bit	Subfield 1	Subfield 2	Subfield 3

Multiple Destinations (L Bit = 0):

D Bit = 0	The receiving end system shall process the DRI
D Bit = 1	The receiving end system shall ignore the DRI and proceed to the next DRI
J Bit = 0	DRI represents a final destination
J Bit = 1	DRI represents an intermediate destination

Source Path to a Single Destination (L Bit = 1):

D Bit = 0	Identifies the next system to receive the packet (or the final destination)
D Bit = 1	The initial setting for all DRIs except the one representing the next system to receive the packet
J Bit = 0	The setting if source routing is used
J Bit = 1	Prohibited if using source routing

FIGURE 24. Routing indication subfields.

5.4.2.9 Field 9 - destination routing indicator (DRI). This field shall be used to identify the RI of the message addressee. This field shall be extendable to accommodate up to 16 final destinations or a source routing list of up to 16 RIs for 15 intermediate and 1 final destination address. Each RI shall be 24 bits long. A DRI is the network layer destination address. The interpretation of the addresses and address subfields (that is, area, subnet, and system codes) for routing purposes depends on the network configuration chosen by the network authority.

5.4.2.9.1 Destination list. When the L bit of the ORI (field 8) is set to 0, field 9 shall contain up to 16 addresses that represent intermediate destinations and 1 or more final destinations. Field 9 shall provide processing and routing information to the receiving end or intermediate system for 1 or multiple final destinations. An example of routing to multiple destinations is provided in Appendix I.

5.4.2.9.1.1 Redundant information indicator. The first bit of the DRI, the D bit in Figure 24, represents a redundant information indicator. When a D bit is set to 0, the receiving end system shall process the associated DRI. When a D bit is set to 1, the corresponding end system has received redundant information and shall ignore the associated DRI.

5.4.2.9.1.2 Routing indicator type. The third bit of the DRI, the J bit in Figure 24, represents the type of RI (intermediate or final). When a J bit is set to 0, the DRI represents a final destination. When a J bit is set to 1, the DRI indicates an intermediate destination. Up to 8 intermediate addresses and up to 16 final destinations are permitted in field 9. Only a single intermediate address shall be associated with one or more final destinations.

5.4.2.9.2 Source path list. When the L bit of the ORI is set to 1, field 9 shall contain the path to the final destination. Field 9 shall contain a single destination address, and the path designated by the list of intermediate destinations must be followed exactly. The D bit of every destination address is set to 1 except for that of the next system designated to receive the packet. The J bit of every destination address is set to 0 (not used) when source routing (L bit set to 1) is used. When an end system receives a packet containing source routing information, it shall inspect the destination list to determine the first DRI with the D bit set to 0. If this is not the address of the receiving system, then the packet is discarded. If it is the address of the receiving system, then the receiving system determines if this is the last address in the destination list. If it is the last address, the receiving system proceeds to locally process the packet. If it is not the last address, then this system sets the D bit corresponding to its RI to 1, sets the D bit of the next DRI on the list to 0, and forwards the packet to that address.

5.4.2.10 Field 10 - end of routing. This field shall be used to designate end-of-routing information as well as the end of the network header. It shall contain the 8-bit binary codeword 00101110 with the rightmost bit as the LSB.

5.4.3 Network-layer procedures. The information conveyed in the network header allows a network or intermediate system to perform routing, forwarding, message segmentation, and relay functions.

5.4.3.1 Packet routing. The routing function shall be implemented at both end and intermediate destination systems. The relay function (forwarding packets received from a remote system) shall be implemented in systems that act as intermediate systems.

5.4.3.1.1 Implementation. The routing function shall determine the path for a packet whose destination network address is not equal to 0. The operator shall have the ability to turn the relay capability off to prohibit the transmission of remotely originated frames. Routing information shall be entered automatically or by the operator. A route shall be determined by a system table (directory), or the originating system can specify a route within the header (source routing).

5.4.3.1.2 Directory routing. In directory routing, the network layer shall obtain the data link address(es) associated with the destination network address(es). There shall be one or more unique destination addresses in the network header if directory routing is to be performed.

5.4.3.1.2.1 Transmitting and routing procedures. To route information to multiple destinations, the source shall set the L-bit of the ORI (field 8) to 0 and proceed as described below.

a. In building the network header, the source shall initialize the D bit of each destination address to 0.

b. If the source has direct connectivity with the final destination(s), the J-bit(s) shall be initialized to 0 and the final network destination address(es) shall be mapped to the data-link address(es) of the final destination(s). All final destination addresses with direct connectivity with the source shall be listed first in the destination list before any intermediate destination addresses.

c. If the source does not have direct connectivity with the final destination(s), then the final destination(s) shall be preceded by an intermediate address with the J-bit initialized to 1. The source shall map the network address of the intermediate destination to the applicable data-link address having direct connectivity with the source. The address(es) immediately following an intermediate destination shall be the final destination(s) presumed to have connectivity with the intermediate destination. The J-bit(s) of the final destination(s) shall be set to 0. The network address(es) of the final destination(s) following an intermediate address are assumed not to have direct connectivity with the source and shall not be mapped to data-link address(es).

d. In the event the intermediate destination is unknown or unreachable, the source shall fill the intermediate address with all 0's (except for the J-bit, which is set to 1) to allow any receiving system an opportunity to route the NPDU.

e. An intermediate address following an intermediate address shall not be permitted. The last address in the destination list shall always be a final destination.

5.4.3.1.2.2 Receiving end routing procedures. Upon receiving the network header, the receiving end system shall completely analyze fields 8 and 9 and proceed as described below.

a. If the D-bit is set to 1, the receiving end system shall ignore the destination address and proceed to the next destination address. If a DRI's D-bit is set to 0, the receiving end system shall continue to analyze the destination address.

b. If a J-bit is set to 0 and the destination address does not belong to the receiving end system, then the receiving end system shall ignore the destination address and move on to the next address in the destination list. If a J-bit is set to 0 and the destination address belongs to the receiving end system, then the receiving end system is a final destination and shall process the information (message) and set the D-bit of its DRI to 1. The receiving end system shall continue to analyze the destination list.

c. If a J-bit is set to 1 and the destination address does not belong to the receiving end system, then the receiving end system shall ignore the destination address and subsequent final addresses, and move on to the next intermediate address in the destination list. If a J-bit is set to 1 and the destination address belongs to the receiving end system or the destination address consists of all 0's, then the receiving end system is an intermediate destination for the following final destination(s) up to the next intermediate address (J-bit set to 1).

d. If the receiving end system is an intermediate destination, then it shall determine if it has direct connectivity with the final destination(s) or not. If the receiving end system (intermediate destination) has direct connectivity, it shall map the network address(es) to the data-link address(es) of the final destination(s), set the D-bit of its own address to 1, and continue to analyze the destination list. If the receiving end system (intermediate address) does not have direct connectivity to the following final destination(s), it shall replace the current network address (its own) in the network header with the address of the applicable intermediate address, if known, and map that address to the applicable data-link address. If the next intermediate destination is unknown or unreachable, the receiving end system shall replace its network address with all 0's (except for J-bit set to 1). The receiving end system shall continue to analyze the remainder of the destination list.

e. If the receiving end system receives all 0's in an intermediate address with the J-bit set to 1, the receiving end system shall attempt to route the information. If unable, the receiving end system shall take no further action and continue to analyze the remainder of the destination list.

5.4.3.1.2.3 Routing tables. Routing tables must provide initial connectivity information on the nodes that will provide routing and relay support for the source and intermediate destinations. The device or system must be initialized with connectivity tables as part of the parametric initialization loading. As connectivity is lost or gained, the tables shall be updated by either manual or automated means. The structure and management of the directory table is not part of this protocol.

5.4.3.1.2.4 Routing history. Using the routing procedures for multiple destinations explained in 5.4.2.9.1 will provide (at a minimum) a 1-hop routing history. Those systems supporting a routing and relay function may use this information in developing and updating routing tables.

5.4.3.1.3 Source routing. In source routing, the path is determined by the originator (source) of the message. Field 9, Destination Routing Indicator, of the network header shall contain a list of up to 15 intermediate systems and 1 final destination to define a routing path. All of the network addresses in the list shall uniquely define an end system. The route shall indicate a complete path that will be strictly followed.

5.4.3.1.4 Packet filter. A subnet may restrict incoming traffic for security or to conserve bandwidth. Field 7, Message Type, shall be used by a relay to limit unwanted packets from being forwarded into a subnet. In the future, if a nonperishable message is not delivered due to a filter, the filtering station should report the nondelivery to the originating network layer by using a nonperishable discard notification packet.

5.4.3.1.5 Data-link acknowledgment. The network layer shall pass data-link acknowledgment requirements.

5.4.3.2 Packet addressing. Field 8, Originator Routing Indicator, and field 9, Destination Routing Indicator, are used to facilitate the routing of packets (messages) through a network. An address authority shall select a scheme for assigning the values that are adequate for the network topology and functions.

5.4.3.2.1 Address format. A 0 value is the broadcast address and shall not be assigned to an end system. The value and assignment of addresses should be determined by the network authority. Field 8, Originator Routing Indicator, addresses shall always use the entire uniquely assigned network address.

5.4.3.2.2 Addressee with no relay. When all the destination addresses in an NPDU are reachable without relay through an intermediate system, field 9 may be 0 (broadcast address) and shall be the only DRI. In this mode, the data-link layer address shall specify the local destination stations. If multiple recipients are involved, field 9 shall contain only one broadcast network address. The application header shall contain the specific addresses to facilitate distribution to multiple recipients. The address field of the data-link layer header may contain multiple destinations.

5.4.3.2.3 Destinations through relay. When a destination must be reached through an intermediate system, the destination address shall be non-zero and shall uniquely define a remote end system. When an intermediate system to a final destination is unknown, a zero DRI (with the J bit set to 1) may be used to allow any intermediate system receiving the NPDU an opportunity to route it.

5.4.3.2.4 Packet precedence. Packet precedence is determined by the message precedence contained in field 5 of the network header. Precedence shall be used to queue messages for transmittal, relay, and delivery to the destination end system. Highest priority frames shall be transmitted first, then the next highest level priority frames, and continue on until the lowest priority frames are transmitted. Within each precedence, frames shall be queued first-in first-out. Packets being relayed shall be placed at the front of the proper precedence queue. The precedence level of a received message shall be reported to the application layer.

5.4.3.3 Network flow and congestion control. Control shall be performed on newly originated messages or those being relayed if routing has been implemented. Several different mechanisms are implemented for flow control at the network layer.

5.4.3.3.1 Traffic queuing. The network layer shall queue traffic for transmission according to precedence and order of arrival at each outgoing link. Messages with the highest priority shall be transmitted before all other messages.

5.4.3.3.2 Discard control. If a subnet is temporarily congested, traffic may be discarded at a relay to avoid propagation of the congestion. The relay shall discard message frames by precedence with the lowest precedence discarded first.

5.4.3.4 End-to-end error recovery (message accountability). Message accountability shall be achieved by applying the following end-to-end error recovery procedures:

a. The link layer shall use the DL-status indication (see 5.3.14) to notify the network layer of delivery failure if link acknowledgment was requested and not received, and if retransmission attempts have been exhausted.

b. If a failure occurs at an intermediate system, a delivery failure SYSCON message may be generated. When the originating network layer receives a delivery failure SYSCON message, the information may be given to the System Management Protocol at the application layer for operator or task notification.

c. The station serial number (SSN), field 4 of the network header, shall be passed to the upper layer to be used by either the operator or application layer for receipt/compliance action.

5.4.3.5 Message segmentation. Message segmenting shall be performed if the message received by the network layer (either from an upper-layer protocol or received from the subnetwork) is too large for the subnetwork in which it will be transmitted. During protocol initialization, the network layer must learn the maximum transmission unit (MTU) size of the data-link layer. The minimum MTU size is 256 octets. The default and maximum MTU sizes are 3500 octets. A packet shall not be segmented into more than 40 segments. The originating end system or an intermediate system (router) shall perform segmentation when a complete (unsegmented) NPDU is routed into a network whose MTU is less than the size of the NPDU (tactical network header and data). When the network layer protocol receives an N-unitdata request containing a data length longer than the maximum MTU size (minus the network header length) times 40 segments, the network layer protocol shall return an error condition to the network layer user.

5.4.3.5.1 Segmentation. If a complete NPDU is larger than the MTU size, the local system shall split the data received from the upper layer protocol, or from the subnetwork, into segments equal to the MTU minus the network header length. Each segment shall have a network header with the same SSN for each segment and a sequentially assigned Message Frame Number. Each segment shall be sent to the same next intermediate or end system. The network segmentation example in Figure 25 assumes an MTU of 256 octets. Each segment of the NPDU shall have the same SSN to identify the segments as members of the same message during reassembly. Only the final segment may be less than the MTU and shall have the first bit of the Message Frame Number set to 1 to indicate the final segment.

5.4.3.5.2 Reassembly. Reassembly shall be implemented in a system. The final destination system must save each received segment until the entire message has been received and reassembled. The SSN is used to identify NPDU segments as belonging to the same message. The Message Frame Number is used to sequentially order NPDU segments that contain the same SSN. An end system shall be able to reassemble at least two messages at a time. If the message reassembly limit has been reached, segments for additional messages shall be discarded. A timer shall be associated with

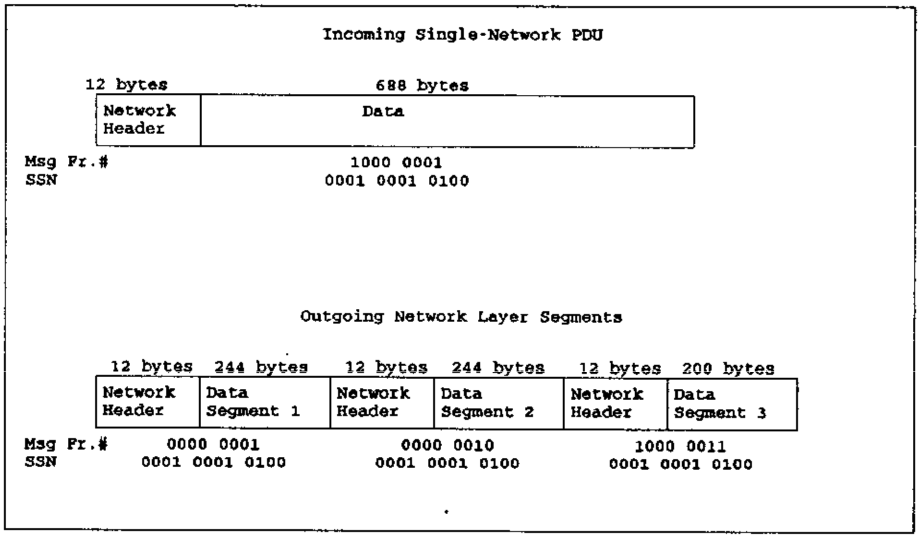


Figure 25. Network segmentation example.

the reassembly process. If no new segments have been received after a specified period of time, the partially reassembled message shall be deleted from the end system.

5.4.4 Next-layer interactions. The network layer protocol interacts with the lower data-link layer and the upper layer protocol.

5.4.4.1 Data-link layer. During initialization procedures, the network layer shall obtain the classmark of the link and the link's MTU size. Data-link acknowledgment is required for nonperishable messages but not for perishable message types (see 5.4.4.2.f).

5.4.4.2 Upper-layer protocol. Three primitives are used to pass information about the sending and receiving of data across the protocol layer boundaries. The network protocol layer expects to receive (a) DRIs; (b) an indication if source routing is requested, and the associated path list; (c) security classmark; (d) precedence level; (e) quality of service; (f) type of service delivered (connectionless or connection-oriented); and (g) message type/characteristics. See 5.6.4 for the parameter format and values. The primitives and their associated parameters are presented below.

a. Data is sent by the upper layer, using the network layer unitdata request primitive with the following parameters:

N-Unitdata request

- Destination(s)
- Originator ID
- Quality of Service
  - Precedence
  - Security
  - Type of Service
  - Reliability Requested
  - Quick Acknowledgment
- Message Type
- Options
  - Type of Routing
  - List of Intermediate Destinations
- Data/Data Length

b. The upper layer is notified when data is received through the Unitdata indication primitive with the following parameters:

N-Unitdata indication	Destination(s)
	Originator ID
	Quality of Service
	  Precedence
	  Security
	Station Serial Number
	Message Type
	Data/Data Length

c. The upper layer is notified when a data request cannot be processed through the network layer Status Indication primitive with the following parameters:

N-Status Indication	Error Type
	  Data Length Exceeded
	  Path Unknown

d. Parameter descriptions

(1) Destination(s). The destination parameter shall contain one or more routing indicators identifying the destination end systems. The format and values of these RIs are described in 5.6.4.

(2) Originator. The originator parameter shall identify the upper layer protocol that is originating the request or receiving the indication. The upper layer is identified by the message processor type (K series).

(3) Quality of Service

(a) Precedence. The precedence parameter specifies the precedence of the message. Precedence values are described in 5.6.4.

(b) Security. The security parameter specifies the security classification and is based on the data contained in the message. Security values are described in 5.6.4.

(c) Type of Service. The type of service parameter indicates the connectionless or connection-oriented type of link layer service. Type of service values are described in 5.6.4.

(d) Reliability Requested. The reliability requested parameter is the variable used to indicate if a Type 1 service (connectionless) data-link acknowledgment is required.

(e) Quick Acknowledgment. The quick acknowledgment parameter is used with the Type 2 service (connection-oriented) and indicates that this send request contains data that should receive a faster-than-usual acknowledgment response from the recipient.

(4) Station Serial Number. The SSN value contained in the network layer header shall be passed to the upper layer protocol. The application layer use of this parameter is described in 5.6.1.1.7.

(5) Options. The options parameter is used to request the source routing service. If the service is requested, the destination parameter shall contain a single final destination RI, and the options parameter shall contain the list of intermediate destination RIs. The format and values of the RIs are described in 5.6.4.

(6) Message Type. The message type parameter shall be used to indicate if a message is perishable or nonperishable and to identify the upper layer message protocol (K series) in the network header.

(7) Data/Data Length. The data parameter contains the upper layer protocol data and an indication of its length.

(8) Error Type. The error parameter is used to inform the network layer user of an error condition when the network layer cannot process a Unitdata request.

5.5 Presentation layer. The presentation layer shall provide transmission syntax, message transformation, code conversion, and data formatting functions. The DMTD shall use the variable message format (VMF) syntax and structure as described in Appendix G. The message syntax and message construction procedures are defined below.

5.5.1 VMF syntax. The syntax for a VMF message shall be implemented using the following flags:

a. field presence indicator (FPI)
b. field recurrence indicator (FRI)
c. group presence indicator (GPI)
d. group recurrence indicator (GRI)

5.5.1.1 Field presence indicator. The FPI shall be used to flag the presence or absence of an optional field in a predefined formatted message. The FPI shall be implemented using a single bit. The FPI shall not be used for mandatory or single bit fields. The FPI shall be used to flag only those optional fields containing information. When an optional field is present, the FPI that precedes the argument of that field shall be set to 1. When an optional field is not present, its FPI shall be set to 0.

5.5.1.2 Field recurrence indicator. The FRI shall be used to flag the presence or absence of fields repeated in a predefined formatted message. The FRI shall be implemented using a single bit. The FRI shall immediately precede the argument of a repeatable field. For optional fields, the first FRI shall immediately follow the FPI. An FRI shall precede every argument of a repeatable field to indicate if the field is repeated after the subsequent argument. The FRI shall be set to 1 to indicate that the field is repeated. The FRI shall be set to 0 to indicate that a field is not repeated. Subsequent occurrences of a repeatable field shall not be preceded by an FPI, but always shall be preceded by an FRI.

5.5.1.3 Group presence indicator. A group is two or more associated fields that normally appear together. The GPI shall be used to flag the presence or absence of groups in a predefined formatted message. The GPI shall be implemented using a single bit. The first field of a group shall be preceded by a GPI to indicate the presence or absence of the group. The GPI shall be set to 1 to indicate the presence of a group. The GPI shall be set to 0 to indicate the absence of a group.

5.5.1.4 Group recurrence indicator. The GRI shall be used to flag the presence or absence of groups repeated in a predefined formatted message. The GRI shall be implemented using a single bit. The first information field of a repeatable group shall be preceded by a GPI. If the GPI=1, indicating presence of the group, it shall be immediately followed by a GRI to indicate recurrence of the group after the first iteration. The GRI shall be set to 1 to indicate that a group is to be repeated. The GRI shall be set to 0 to indicate that a group is not to be repeated. Immediately following the GRI shall be a presence indicator (FPI or GPI), if required. Subsequent occurrences of a repeatable group shall be preceded only by a GRI to indicate whether the group will be repeated after this iteration of data.

5.5.2 VMF syntax indicator implementation rules. The rules for implementation of presence and recurrence indicators shall be as follows:

a. Group indicators shall take precedence over (appear before) field indicators.

b. Presence indicators shall take precedence over recurrence indicators.

c. If any field of a repeatable group is mandatory, the group shall be mandatory. If the mandatory field appears in a nested group, the outer group (or groups) within which it is (they are) nested shall also be mandatory. Mandatory repeatable groups shall not require a GPI. A GRI shall be used to flag the group as repeatable.

d. Mandatory fields shall not be preceded by FPIs. An FRI shall precede the mandatory field if the field is repeatable.

e. If a presence indicator is set to 0, a recurrence indicator shall not be included.

f. Upon completion of the last field of a repeatable group of fields that is to reoccur, and after all included nested groups of fields have been considered, computer logic shall return to consider the GRI for that repeatable group (the GPI is not required). The same concept applies to individually repeatable fields. After presenting or processing field data that was preceded by an FRI with a value of 1, computer logic shall return to consider the FRI (the FPI is not required).

g. Prior to presenting data for the last allowable occurrence of the field or group of fields, the recurrence indicator value shall be set to 0.

h. An end-of-text flag shall not be used. FPIs and GPIs set to 0 shall be used to account for data fields or repeatable groups that have been omitted.

5.5.3 <u>End-of-literal field marker</u>. The end-of-literal field marker, an ASCII DELETE character (11111111), is used to indicate the end of free-text, character-oriented, literal fields only. The maximum literal field size is specified, for each such field, in the VMF TIDP, Vol II. The end-of-literal field marker shall not be used if the characters fill the field. The message processing software shall be capable of recognizing either the end-of-literal field marker or the field maximum length to detect the end of the free text.

5.5.4 <u>Data-field construction procedures</u>. The following message construction procedures prescribe the sequence in which VMF message components and the application header fields are linearly joined before passing data to the next lower protocol layer. VMF messages are constructed with elemental data fields ordered as specified in Volume III of the VMF TIDP. The network header fields are ordered as shown in Table V. The application header fields are ordered as shown in Table IX. Data elements for the messages and application header are specified in Volume II of the VMF TIDP. There are three representations for data elements:

7-bit ASCII characters, 4-bit BCD digits, and binary numbers. All fields shall be joined MSB first.

5.5.4.1 ASCII data element. In a data element composed of a string of 7-bit ASCII characters, the leftmost character shall be stored in memory first.

5.5.4.2 Binary-coded-decimal data element. In a data element composed of more than 1 BCD digit, the leftmost digit is the high-order digit and shall be stored first.

TABLE IX. Application header.

Field Number	DFI/DUI	Field Name	CAT	Repeat Code	Data Length (bits)
1	4097/001 4097/002	Receipt Compliance	M		4
2	4081/001 4085/019	Message Designator	M		17
3	See Table XII	Date and Time	O		34
4	4100/001	Originator	O		56
5	4100/002	Recipient	O	R*n*	56
6	4100/003	Information	O	R(16-*n*)	56
7	4101/001	Control and Release Marking	O		14
8	4076/001	Cannot Process (CANTPRO) Reason Code	O		6

NOTE: $n \leq 16$.

5.5.4.3 Binary data element. In a data element composed of a binary code, it shall be stored as a single data field.

5.5.5 Next-layer interaction. Two primitives are used to pass information for the sending and receiving of data across the upper-layer boundary. Data is sent by the application layer, using the presentation Unitdata request primitive with the following parameters:

P-Unitdata request
- Destination(s)
- Originator
- Quality of Service
  - Precedence
  - Security
  - Reliability Requested
  - Type of Service

Message Type
Options
  List of Intermediate
  Destination(s)
Data

The application layer is notified when data is received through the Unitdata indication primitive with the following parameters:

P-Unitdata indication
Destination
  Originator
  Quality of Service
  Precedence
  Security
Message Type
  Station Serial Number
Data

If the message is designated as perishable, the application layer will not pass an acknowledge request. Perishable messages do not require link-layer acknowledgment.

5.6 Application layer. The application layer shall provide the message-handling protocols.

5.6.1 Application protocol data unit. The application protocol data unit shall be composed of an application header and a user data field, as shown in Figure 26.

Application Header	User Data

FIGURE 26. Application protocol data unit structure.

5.6.1.1 Application header. The application header shall consist of eight fields, as shown in Table IX. The application header contains mandatory (M) and optional (O) fields. A FPI shall be used to flag the presence or absence of an optional field. Presence indicators are discussed in Appendix G.

5.6.1.1.1 Field 1 - receipt/compliance. This field shall be a 4-bit binary codeword representing the receipt/compliance (R/C) codes shown in Table X. There are nine R/C codes used: three that a message originator uses to make a request; and six that a recipient uses to form a response R/C message. The pertinent DFI/DUI codes are 4097/001 and 4097/002. (See Appendix H.)

5.6.1.1.2 Field 2 - message designator. This field, consisting of two subfields, shall contain a 7-bit binary codeword that identifies the functional area of a specific message using the codewords shown in Table XI, and a 10-bit binary codeword that

TABLE X. Receipt/compliance codes.

Type of Receipt/compliance	Code	Used by
Operator Response Required (ORR)	0000	Originator
No Reply/Response Required (NRR)	0001	Originator
Machine Receipt Required (MRR)	0010	Originator
Machine Receipt (MR)	0011	Recipient
Cannot Process (CANTPRO)	0100	Recipient
Operator Acknowledge (OPRACK)	0101	Recipient
Will Comply (WILCO)	0110	Recipient
Have Complied (HACO)	0111	Recipient
Cannot Comply (CANTCO)	1000	Recipient

MSB LSB

TABLE XI. Functional area designator codewords.

FUNCTIONAL AREA	CODEWORD
Network Control	0000000
To be determined	0000001
Fire Support	0000010
To be determined	0000011
To be determined	0000100
To be determined	0000101
To be determined	0000110
To be determined	0000111

MSB LSB

represents the number that identifies a specific message within a functional area. The message number value shall range from 1 to 999. The functional area designator combined with the message number shall point to the applicable message of 5.7.1 that will appear in the user data field. The pertinent data field identifier/data use identifier (DFI/DUI) codes for these subfields are as follows: 4081/001 for the functional area designator, and 4085/019 for the message number.

5.6.1.1.3 Field 3 - date and time. This field shall contain date and time information. This field shall be 34 bits long and shall contain groups of data representing the year, month, day, hour, minute, and time zone of the message. Coding for each data element shall be in accordance with the Data Element Definitions in Appendix H. Specifically, the data elements that shall be used are shown in Table XII. Each data element is linearly joined to build the date and time field.

TABLE XII. Date and time group data elements

ELEMENT	CODE	BITS
Year	4098/001	7
Month	4099/001	4
Day	4019/001	5
Hour	792/001	5
Minute	797/004	6
Time Zone	4035/001	7

5.6.1.1.4 Fields 4, 5, 6 - originator, recipient, information addressees. These fields shall contain addresses consisting of 8 ASCII characters (56-bits) that represent the names of the originating and receiving person(s) or process(es). The receiving application layer shall use the recipient and information fields to determine how the message shall be handled after the decoding process. The value in these fields depends on the person or process receiving the message. If a person is to be designated, the fields shall uniquely identify the individual so that the message may be routed to a specific mailbox or terminal. If a process is to be designated, these fields shall uniquely identify the process (such as, fire support execution or fire support planning). The process must be associated with an end system to define the address uniquely. The recipient and information addressee fields shall be extendable to a combined total of 16 addressees. The pertinent DFI/DUI codes for these fields are as follows: 4100/001 for the originator, 4100/002 for the recipient, and 4100/003 for the information addressees.

5.6.1.1.5 Field 7 - control and release marking. This shall be a 14-bit, 2-ASCII-character field indicating the restrictions or requirements for special handling, access control, and releasability of the message. The pertinent DFI/DUI code is 4101/001, Control and Release Marking.

5.6.1.1.6 Field 8 - cannot process reason code (CANTPRO). This field shall be a 6-bit binary code indicating why a particular message cannot be processed by a recipient or information addressee. It shall be used only in R/C messages. The pertinent DFI/DUI code is 4076/001, CANTPRO reason code.

5.6.1.1.7 Message accountability. The application header shall be used for the detection of duplicate messages and to associate an R/C message with the requesting message. The received fields of SSN (passed from the network header), date and time, and originator are used to uniquely identify a message. These three fields of the received R/C message are compared with the SSN, Date/Time, and Originator fields of the original message. Duplicate messages shall be discarded.

5.6.2 User data field. This field shall contain the application process messages specified in 5.7.1.

5.6.3 Message acknowledgment. Message acknowledgment reports on a receiving station's receipt of and intentions with respect to a received message. The acknowledgment protocols are implemented in the R/C message format.

5.6.3.1 Receipt/compliance messages. R/C messages are used by the originator to request a specific R/C response from the receiving station, or appropriate operator, for selective acknowledgment of message receipt and compliance with the message instructions. R/C messages (request and response) are conveyed in the R/C field of the application header. A receiving station responds to the originator by sending an R/C message with a recomposed application header and, if appropriate, the CANTPRO reason code field. Depending on the type of R/C request from the originator or the type of system involved, the R/C response may be machine-generated (automatic) or operator-generated (manual).

5.6.3.2 Message implementation. Implementations of the VMF message contents depend on the operational facilities supported by the system and on the total information exchange requirements (IERs) of those facilities. Certain message error detection restrictions and rules shall apply when systems implement VMF messages. These restrictions depend on the message type (perishable or nonperishable) and message field category (M or O).

5.6.3.2.1 Perishable messages. Perishable messages are those messages designated to contain information considered invalid after a short time period. These messages will not require recovery procedures. The R/C message protocol does not apply to perishable messages.

5.6.3.2.2 Nonperishable messages. Nonperishable messages are those messages that require a higher degree of delivery effort by the communications protocols. They contain information with a longer lifespan than the perishable messages. An originator may request an R/C message response to nonperishable messages. A recipient may choose to notify the originator by sending an error R/C message in response to a nonperishable message even if an R/C was not requested by the originator. Below are some examples of R/C responses by a receiving station:

a. R/C error processing of text header. If a system receives a message number that it does not implement, it responds by sending a CANTPRO code 15 (Agency Does Not Recognize This Message Number) R/C message to the originator. Other processing procedures depend on the category of the field(s) that cannot be processed.

b. Mandatory message field error processing. Every VMF message shall contain information in each mandatory field. If the received message does not contain valid information in one or more of the mandatory fields, the receiving station shall return a CANTPRO code 1 (Field Content Invalid) R/C message to the originator.

c. Optional message field error processing. The implementing system may choose not to implement any optional field of the message for transmission, reception, or both. Once a system chooses not to implement a field for transmission, it must account for that field through flagging each time the message is transmitted.

   (1) If the received message contains data in optional fields that the receiving system does not implement, the receiving system shall ignore the content of those fields. The reception of data in optional fields not implemented by the receiving system does not alone mandate the transmission of an R/C message indicating an error.

   (2) A received message, which does not contain data in optional fields that the receiving system implements, does not, of itself, require the transmission of an R/C message indicating an error.

5.6.3.3 Receipt/compliance message format/content. There are two R/C message formats: (a) a recomposed message header used when the R/C message contains an operator acknowledge (OPRACK), will comply (WILCO), have complied (HAVCO), machine receipt (MR), CANTPRO (with a CANTPRO Reason Code other than Field Content Invalid), or cannot comply (CANTCO) R/C type; and (b) a recomposed message header with R/C flags and associated error fields attached, which is used only when the response requires a CANTPRO (Field Content Invalid) R/C message. Figures 27a and 27b illustrate the two R/C message formats.

Recomposed Header

FIGURE 27a. Simple R/C message format.

Recomposed Text Header	R/C Flag M	Error Field M	. . .	R/C Flag N	Error Field N	R/C Flag = 0

FIGURE 27b. CANTPRO-field content invalid R/C format.

5.6.3.3.1 Lower-layer parameters. Some of the parameters contained in the Unitdata request to send the R/C are the same as those in the received Unitdata indication. Other parameters are independent of the Unitdata indication. The precedence and security values passed to the lower-layer protocol with the R/C message are identical to the precedence and security parameters received with the message being acknowledged. The destination RI of the response contains the originator RI parameter from the associated original message. An R/C message should request error recovery procedures by the lower layer. The originator ID shall identify the message processor (K-series).

5.6.3.3.2 Application header fields. Field 1, Receipt/Compliance, identifies the type of response the R/C message is sending (such as CANTPRO or WILCO). Field 2, Message Number; field 3, Date and Time; and field 7, Control and Release Markings of the outgoing R/C message shall contain the same information as the received message application header. Field 4, Originator, contains the local name used in field 5, Recipient, or field 6, Information, of the incoming message. Field 5, Recipient, contains the contents of the received field 4, Originator. Field 6 is unused. Field 8, CANTPRO Reason Code, is only present when a CANTPRO value is contained in the R/C field.

5.6.3.3.3 Error fields. When the CANTPRO Reason Code field of a R/C message has a value of 1 (Field Content Invalid), the text portion of the R/C message shall include the field or fields (from the original message) that resulted in the CANTPRO rejection response. Each of these error fields shall appear in the order received and shall be preceded by an R/C flag.

5.6.3.3.4 Receipt/compliance flag. The R/C flag is a 12-bit field with values from 1 through 4095. An R/C flag with a value of 0 indicates the end of the R/C error field. In computing the value of the R/C flag (sequential position of the field received in error), numbering is begun with the first data field of the body of the message. The count is continued throughout the body of the message, including each data element field, but excluding all flag fields (presence and repeatability flags).

5.6.3.4 Message retransmission timer. A retransmission capability may be provided for the automatic retransmission of a message that has not received a reply when R/C is requested. A timer shall exist to schedule the automatic retransmission. Only one automatic retransmission is provided. Additional retransmissions must be requested by the operator. Expiration time shall be operator-selectable with a range of 5 to 75 seconds. Upon expiration of the timer, provided the requested reply has not been received, the message shall be retransmitted. If a reply is not received prior to expiration of the timer on this second transmission, the operator shall be notified to determine if additional retries are required. The automatic retransmission of a message is a system parameter selected by the operator. If the parameter is set to ON, the first retransmission shall occur without operator intervention. If the parameter is set to OFF, operator approval shall be required before a retransmission may occur.

5.6.4 Lower-layer protocol interaction. The application protocol shall supply to the lower-layer protocol information required by that protocol to provide its services. The application layer shall receive from the lower-layer protocol information pertaining to the status of the message.

5.6.4.1 Parameters to the lower-layer protocol. The application layer shall pass addressing, quality-of-service, and option information to the lower-layer protocol (presentation Unitdata request). The parameter values are defined in 5.6.4.1.1 through 5.6.4.1.5.

5.6.4.1.1 Originator and destination addresses. The application layer shall map the Originator, Recipient, and Information names to network layer addresses. The network layer addresses are RIs and consist of 3 alphabetic characters. Each character is 8 bits long and is contained in a 3-octet field. The 5 LSBs of the 8-bit field contain the 5 LSBs of the ASCII representation of the character. Table XIII shows the format and appropriate values used by the application layer for the RIs.

TABLE XIII. Values for the routing indicator.

Subfield	Values	Bit Representation MSB -> LSB
Subnet Address	Characters A-Z	00000001 - 00011010
Area Address	Characters A, B, D - Y	00000001, 00000010, 00000100 - 00011001
End System Address	Characters A - Z	00000001 - 00011010

5.6.4.1.2 Originator ID. The originator ID parameter identifies the application layer process that is requesting the delivery service. This parameter shall have the value 1 to identify the K-series message process.

5.6.4.1.3 Quality-of-service parameters. The application layer requests a quality of service for each message that it sends. Quality-of-service parameters include the precedence level, security classification, and level of effort.

a. Precedence. The precedence parameter specifies the precedence used in delivery. The three values, 1-3, indicate a delivery precedence and are reserved for machine-readable messages. Value 1 demands the fastest delivery service and shall be restricted to a very small percentage of highly critical messages. Value 2 demands a fast-message delivery service. Value 3 requests the normal delivery service. Below is the bit representation of the precedence values:

Message Delivery	
	MSB LSB
Urgent	0001
Priority	0010
Routine	0011

b. Security. The security parameter specifies the security classification and is based upon the data contained in the message. Below is the security classification range and corresponding bit representations:

Security Classification	
	MSB LSB
Top Secret	1000
Secret	0100
Confidential	0010
Unclassified	0001

c. Level-of-effort. The level-of-effort parameter indicates to the lower layer when error recovery procedures should be applied and if it should be at the expense of overall network efficiency. The application layer shall determine if it requires connection-oriented or connectionless service from the lower layers. The connection-oriented service is reliable and network efficient (generally a speedy service, but may have delays). The connection-oriented service can provide a speedier error recovery service using the quick acknowledgment option. The connectionless service can be "best effort" (fast and network efficient, but not reliable) or "acknowledged" (fast and reliable, but reduces overall network efficiency).

Level-of-effort	
Connection-Oriented	1
Connection-Oriented with Quick Acknowledgment	2
Connectionless - Best effort	3
Connectionless - Acknowledged	4

5.6.4.1.4 Options. The application layer may request source routing, and it may provide to the lower-layer protocol a list of 1 to 15 intermediate RIs. The single destination RI is contained in the destination parameter. The determination of the path to the final destination is outside the scope of this protocol.

5.6.4.1.5 Message type. Message type identifies whether the message is perishable or nonperishable as follows:

Message type	
	MSB LSB
Nonperishable K-series	1110
Perishable K-series	0111

5.6.4.2 Parameters from the lower-layer protocol. The application layer shall receive from the lower-layer protocol those parameters that specify the originator RI, the destination ID, security, precedence, and the SSN of the received message. The values of the RIs, security, and precedence shall be the same as those in 5.6.4.1.1 to 5.6.4.1.5. The SSN is defined in 5.4.2.4.

5.7 Application process.

The application process shall provide the messages that satisfy information exchange requirements.

5.7.1 Message formats. K-Series messages summarized in Volume III of the VMF TIDP shall be used for joint information exchange.

6.. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Subject term (key word) listing. The follow key words and phrases apply to this MIL-STD.

Data Communications Protocol
Digital Message Transfer Device
Error Detection and Correction
Segmentation
Relay
Open Systems Interconnection
Packets
Variable Message Format

6.2 Issue of the DoD Index of Specifications and Standards. When this MIL-STD is used in procurement, the applicable issue of the DoDISS must be cited in the solicitation.

6.3 Interoperability considerations. This section addresses some of the aspects that terminal designers and systems engineers must consider when applying MIL-STD-188-220 in their communications system designs. The proper integration of MIL-STD-188-220 into the total system design will ensure the interoperability of stations that exchange information over a data communications link consisting of a DMTD, a transmission channel, and a DMTD or C4I system.

6.3.1 Transmission channel. For the purpose of this MIL-STD, the transmission channel (from the transmitter to the receiver) is considered transparent to the DMTD subsystem. However, the transmission channel must be interoperable within itself. The transmission channel may be secured or nonsecured, using such media as line-of-sight (LOS) radio, high frequency (HF) radio, wireline, and SATCOM.

6.3.2 Physical interface. The specifics of the physical interface for connecting DMTDs to the equipment that implements the transmission channel are beyond the scope of this MIL-STD. The actual physical connections will depend on the interface characteristics required by the particular transmission equipment. These unique physical interface characteristics may be defined in the equipment specifications or in technical interface specifications. Therefore, the requirements for the electrical features (such as data, clock, and control) and mechanical features (such as connectors, pin assignments, and cable) of the connection between the DMTD and the associated transmission channel equipment is left to the equipment designer. The data signaling format (that is, NRZ, FSK, CDP) is specified in this MIL-STD at the standard interface, because it is an interoperability parameter. The design philosophy is that what appears at the input end of the transmission channel must be the same at the output end.

6.3.3 COMSEC interoperability. The COMSEC function provides a link encryption capability. In the traditional COMSEC mode of operation, the COMSEC function (normally implemented in ancillary equipment) is considered part of the transmission channel. In the embedded COMSEC mode, the COMSEC function is an integral part of the DMTD subsystem.

6.3.4 Single-thread data-link diagrams. Tables XIV and XV depict various single-thread data-link communications scenarios that may be implemented for DMTD-to-DMTD connectivity or DMTD-to-C4I node connectivity.

TABLE XIV. Single-thread data links with external COMSEC.

DMTD (Station A)				TRANSMISSION CHANNEL					DMTD OR C4I NODE (Station B)		
TERM	KG	MODEM		COMSEC	XMIT	RCV	COMSEC		MODEM	KG	TERM
			STANDARD INTERFACE	NONSECURE TRANSMISSION CHANNEL				STANDARD INTERFACE			
*	None	NRZ/FSK/DPSK			LOS TACTICAL RADIO				NRZ/FSK/DPSK	None	*
*	None	FSK/PSK/CDP			NB/WB WIRELINE				FSK/PSK/CDP	None	*
*	None	NRZ/FSK/DPSK			HF RADIO				NRZ/FSK/DPSK	None	*
*	None	NRZ/FSK/DPSK			SINGLE-CHANNEL SATCOM				NRZ/FSK/DPSK	None	*
				SECURE TRANSMISSION CHANNEL							
*	None	NRZ		LOS TACTICAL RADIO W/INTEGRATED COMSEC/TRANSEC					NRZ	None	*
*	None	NRZ		WB COMSEC	LOS TACTICAL RADIO		WB COMSEC		NRZ	None	*
*	None	NRZ		WB COMSEC	WB WIRELINE		WB COMSEC		NRZ	None	*
*	None	NRZ		NB COMSEC	HF RADIO		NB COMSEC		NRZ	None	*
*	None	NRZ		WB COMSEC	SINGLE-CHANNEL SATCOM		WB COMSEC		NRZ	None	*
		NRZ		NB COMSEC	SINGLE-CHANNEL SATCOM		NB COMSEC		NRZ		

* The specific interoperability parameters are addressed in 5.0.

LEGEND:
KG: key generator
NB: narrowband
WB: wideband

TABLE XV. Single-thread data links with embedded COMSEC.

DMTD (Station A)				TRANSMISSION CHANNEL					DMTD OR C4I NODE (Station B)		
TERM	KG	MODEM		COMSEC	XMIT	RCV	OMSEC		MODEM	KG	TERM
EMBEDDED COMSEC			STANDARD	NONSECURE TRANSMISSION CHANNEL				STANDARD	EMBEDDED COMSEC		
*	EMBEDDED	NRZ/FSK/DPSK			LOS TACTICAL RADIO				NRZ/FSK/DPSK	EMBEDDED	*
*	EMBEDDED	FSK/PSK/CDP			NB/WB WIRELINE				FSK/PSK/CDP	EMBEDDED	*
*	EMBEDDED	NRZ/FSK/DPSK			HF RADIO				NRZ/FSK/DPSK	EMBEDDED	*
*	EMBEDDED	NRZ/DPSK			SINGLE-CHANNEL SATCOM				NRZ/DPSK	EMBEDDED	*
EMBEDDED COMSEC			INTERFACE	SECURE TRANSMISSION CHANNEL				INTERFACE	EMBEDDED COMSEC		
*	EMBEDDED	NRZ		LOS TACTICAL RADIO W/INTEGRATED COMSEC/TRANSEC					NRZ	EMBEDDED	*
*	EMBEDDED	NRZ		WB COMSEC	LOS TACTICAL RADIO		WB COMSEC		NRZ	NONE	*
*	EMBEDDED	NRZ		WB COMSEC	WB WIRELINE		WB COMSEC		NRZ	EMBEDDED	*
*	EMBEDDED	NRZ		NB COMSEC	HF RADIO		NB COMSEC		NRZ		*
*	EMBEDDED	NRZ		WB COMSEC	SINGLE-CHANNEL SATCOM		WB COMSEC		FSK	EMBEDDED	*
				NB COMSEC	SINGLE-CHANNEL SATCOM		NB COMSEC				

* The specific interoperability parameters are addressed in 5.0.

Legend:
KG: key generator
NB: narrowband
WB: wideband

APPENDIX A

ABBREVIATIONS AND ACRONYMS

10. GENERAL

10.1 Scope. This appendix contains a list of abbreviations and acronyms pertinent to MIL-STD-188-220.

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS. This section is not applicable to this appendix.

30. ABBREVIATIONS AND ACRONYMS

ABM	asynchronous balanced mode
ADM	asynchronous disconnected mode
ASCII	American Standard Code for Information Interchange
BCD	binary-coded decimal
bps	bit(s) per second
C	consecutive repeatable indicator
C4I	command, control, communications, computers, and intelligence
CANTCO	cannot comply
CANTPRO	cannot process
CDP	conditioned diphase
COMSEC	communications security
C/R	command/response
d/c	don't care
DCA	Defense Communications Agency
DCAC	Defense Communications Agency circular
DCS	Defense Communications System
DFI	data field identifier

APPENDIX A

DISC	disconnect
DISA	Defense Information Systems Agency
DL	data-link layer
DM	disconnect mode
DMTD	digital message transfer device
DoD	Department of Defense
DoDISS	Department of Defense Index of Specifications and Standards
DPSK	differential phase-shift keying
DRI	destination routing indicator
DUI	data use identifier
EDAC	error detection and correction
F	final
FCS	frame check sequence
FED-STD	federal standard
FEC	forward error correction
FIPS	federal information processing standard
FPI	field presence indicator
FRI	field recurrence indicator
FRMR	frame reject
FSK	frequency-shift keying
GPI	group presence indicator
GRI	group recurrence indicator
HAVCO	have complied
HDLC	high-level data link control
HF	high frequency

H-NAD	hybrid net access delay
Hz	hertz
I	information; iterative repeatable indicator
IER	information exchange requirement
I PDU	information PDU
ISO	International Organization for Standardization
JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability and Engineering Organization
kbps	kilobit(s) per second
KG	key generator
kHz	kilohertz
KT	keytime delay
LOS	line of sight
LSB	least significant bit
M	mandatory
MI	message indicator
MIL-STD	military standard
MR	machine receipt
MRR	machine receipt required
MSB	most significant bit
MTU	maximum transmission unit
(*n*)	repeatability factor
NAC	net access control
NAD	net access delay
NATO	North Atlantic Treaty Organization

NB	narrowband
NETCON	network control
NMCS	National Military Command System
NPDU	network protocol data unit
N(R)	receive sequence number
NRR	no reply/response required
NRZ	non-return-to-zero
NS	number of stations
N(S)	send-sequence number
O	optional
OPRACK	operator acknowledge
ORI	originator routing indicator
ORR	operator response required
OSI	Open Systems Interconnection
OTAR	over-the-air rekeying
P	poll
PDU	protocol data unit
P/F	poll/final
PL	physical layer
P-NAD	priority net access delay
PSK	phase-shift keying
QT	quiet timer
R	repeatable field indicator
R/C	receipt/compliance
REJ	reject
RHD	response hold delay

RI	routing indicator
Rn	repeatable field within group n
R-NAD	random net-access delay
RNR	receive not ready
RR	receive ready
RSET	reset
S	supervisory
SABME	set asynchronous balanced mode extended
SATCOM	satellite communications
SP	subscriber precedence
S PDU	supervisory PDU
SREJ	selective reject
SSN	station serial number
ST	satellite time delay
STANAG	Standardization Agreement (NATO)
SYSCON	system control
TBD	to be determined
TDC	time-dispersive coding
TEST	test
TIDP	technical interface design plan
TL	traffic load
TP	timeout period
TWC	transmission word count
U	unnumbered
UA	unnumbered acknowledgment
UI	unnumbered information

U PDU	unnumbered PDU
URNR	unnumbered receive not ready
URR	unnumbered receive ready
VMF	variable message format
V(R)	receive-state variable
V(S)	send-state variable
WB	wideband
WILCO	will comply
XID	exchange identification

APPENDIX B

LAYER INTERACTIONS

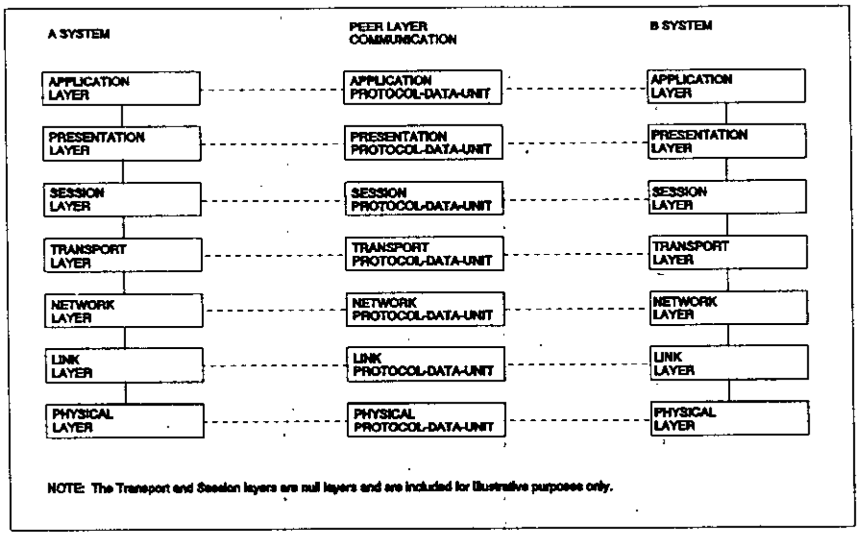
10. GENERAL

10.1 Scope. This appendix describes the interface protocol between the layers of the DMTD model architecture.

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS. This section is not applicable to this appendix.

30. EXCHANGING INFORMATION. An interface exists between each pair of adjacent layers. The interface defines which functions and services the lower layer offers to the upper one. In the case of two automated systems exchanging information, layer *n* of one system carries on a conversation with layer *n* of another system. The rules and conventions used in this conversation are known collectively as the layer *n* protocol, as illustrated in Figure B-1 for a DMTD network. A protocol is used for communication between entities in different systems. In general, an entity is anything capable of sending or receiving information, and a system is a physically distinct object that contains one or more entities. The entities comprising the corresponding or equivalent layers on different systems are called peer processes. These peer processes require standardized protocols to define the services performed and functions provided to communicate with each other. In reality, no data are transferred directly from layer *n* on one system to layer *n* on another (except in the lowest layer). Instead, each layer in the transmitting system passes data and control information to the layer immediately below it, until the lowest layer is reached. At the lowest layer, there is physical communication with the other system, as opposed to the virtual communication used by the higher layers. At the receiving system, data and control information is passed upward from the lowest layer to the corresponding peer processes at successively higher layers, thus creating a virtual link between processes. In Figure B-1, virtual communication is shown by the dotted lines and physical communication is shown by the solid lines.



NOTE: The Transport and Session layers are null layers and are included for illustrative purposes only.

FIGURE B-1. Layer interactions.

30.1 Physical layer

30.1.1 Physical-layer services provided. The physical layer provides a number of services to the upper layer protocols. These services are as follows:

a. Physical connection provides an interface allowing a signal to proceed from one circuit, line, or transmission component to another.

b. Sequencing is the process of ensuring that bits are delivered to the receiving DMTD in the same sequence in which they were transmitted by the sending DMTD.

c. Quality-of-service parameters provide a planned and systematic pattern of actions necessary to provide adequate confidence that a circuit conforms to established technical performance specifications. Quality-of-service is characterized by error rate, service availability, transmission rate, and transit delay.

30.1.2 Physical layer functions. The physical layer performs the following functions:

a. COMSEC preamble and postamble are a series of bits added by the transmitting COMSEC equipment to allow synchronization by the receiving COMSEC equipment.

b. KT and bit synchronization functions provide for the transmitter and equipment start-up and turnaround times along with a bit pattern to allow the end-to-end link to be established. The KT function supports a net busy detection capability used by the link layer in net access management.

c. Transmission synchronization provides a transmitted pattern of bits for receivers on the same net to detect a message and indicate incoming data to the processor.

d. Transmission and information rates are measured in the number of bits transmitted per second. The transmission rate may not be the same as the information rate. The use of FEC increases the number of bits transmitted, but not all bits contain information.

30.2 <u>Link layer</u>

30.2.1 <u>Link-layer services provided</u>. Link-layer services are focused upon connecting stations on a data link and providing for error-free transmission of data in a format acceptable to all stations on the link. Services provided by the link layer are defined below:

a. Data-link connection services provide the management procedures for initiating, maintaining, and terminating a sustained data exchange between stations on the same link.

b. A data-link service unit is a finite sequence of bits that represent information and usually consists of control, message header, and data parts arranged in a specific format known as a *frame*.

c. Sequencing is the process of ensuring that frames are delivered to the receiving DMTD in the same sequence as they were transmitted by the sending DMTD.

d. Error control is the process of ensuring that bit errors introduced by the transmission system are detected and corrected.

e. Flow control is the control of the rate at which data is transmitted from one station so that it is equal to the rate at which it can be received or buffered at another station.

f. Quality-of-service parameters provide a planned and systematic pattern of actions necessary to provide adequate confidence that a circuit conforms to established technical performance specifications.

30.2.2 Link-layer functions. The following functions are performed by the link layer:

a. Frame formatting is the structure or arrangement of user data and control data in a frame. The size and content of the various data fields in a frame are defined by the protocol.

b. Frame addressing involves the addition of an address field to a frame (service data unit).

c. Commands and responses provide the data control and status signals used to ensure the transfer of information, provide ready-to-receive or not-ready-to-receive status, and send link acknowledgments.

d. Network access is a protocol that allocates use of a single channel among competing users by establishing access rules based on a fixed or dynamic algorithm known to all stations on the network.

e. Data-link control signals provided by the link layer establish and release data-link connections over physical circuits for the transmission of data frames, acknowledgments, or control frames.

f. Frame transfer (information transfer) is the process of moving data from one point to another.

g. Acknowledgment provides a positive response control signal generated at the receiving end, indicating data was received or rejected.

h. Flow-control procedures are included in the protocol to limit the input rate of information to prevent overload.

i. Retransmission is the repetition of a message, signal, or other transmission previously sent by a given transmitter.

j. Error detection and correction procedures are included in protocols (1) to detect errors by using codes designed to reveal whether any bits have been changed, (2) to correct errors by automatic retransmission or through FEC coding schemes, and (3) to increase the probability of being able to correct errors through the use of bit interleaving schemes.

30.3 Network layer

30.3.1 Network-layer services provided. The network layer provides the following services:

a. Network addresses are destination codes consisting of signals that indicate the address of the next-higher-layer entity to which the transmission is directed.

b. Network connections are logical pathways established between next-higher-layer entities.

c. Network service-data-unit transfer provides for the exchange of network service-data-units. These units have a distinct beginning and end, and the integrity of the unit content is maintained by the network layer. No limit is imposed on the maximum size of the network service-data-units. Network service-data-units are transferred transparently between transport entities.

d. Quality-of-service parameters are a planned and systematic pattern of actions necessary to provide adequate confidence that a circuit conforms to established technical performance specifications. The quality-of-service parameters include the following factors:

   (1) Residual errors that may arise from alteration, loss, duplication, disordering, misdelivery of network service-data-units, or other causes.

   (2) Service availability, which is the probability that a requested network connection can be established.

   (3) Reliability, which is the probability that a device will perform its intended function for a specified period of time under stated conditions, and which is indicated by the mean time between failures and mean time to repair an established network connection.

(4) Throughput, which is the information transfer capacity.

(5) Transit delay, which includes variations on the transit delay.

(6) Delay for network connection establishment.

e. Error notification is a method by which errors that occur in transmission are detected, and the receiving entity notifies the sending entity that errors have occurred. Unrecoverable errors detected by the network layer are reported to the application entities.

f. Sequencing is the process of controlling the order of the network service-data-units to ensure that the frames are delivered to the receiving application entity in the same sequence as they were transmitted by the sending application entity.

g. Flow control is the procedure of controlling the transfer rate of packets, or other network service-data-units, between two specified points in a data network.

30.3.2 Network-layer functions. The following functions are performed by the network layer protocols:

a. Network header provides the means of determining and prescribing the path or method for forwarding network service-data-units to network entities.

b. Network routing supports the primary function of the network layer to deliver a packet from the source to the destination. The path to the destination may involve several intermediate systems along the way. This layer must know the topology of the communication subnet to choose the appropriate path.

c. Network connections provide for establishing, maintaining, and terminating logical connections or paths between network entities, providing services between transport entities, and making use of link connections provided by the link layer.

d. Message blocking is the grouping of information bits information into a finite string, which is then transmitted as a unit.

e. Packet addressing is the coded representation of the destination of a packet or service-data-unit.

f. Packet precedence is a service established to enable a user to exercise precedence over other users, or to enable a packet to be transmitted with greater precedence than other packets.

g. End-to-end error recovery (message accountability) is the set of established functions and protocols that pertain to the control of integrity and errors in the functions performed by the network layer to ensure accuracy and transparency for the upper layers.

h. Interconnection provides functions, such as relaying and routing, which are combined with the functions performed by the individual subnetwork to provide transmissions between end systems that may or may not be attached directly to the same subnetwork. An internetting protocol identifies a style of interconnection capable of operating over a series of interconnected subnetworks and over different types of subnetworks.

30.4 Presentation layer

30.4.1 Presentation-layer services provided. The following services are provided by the presentation layer:

a. Data syntax transformation executes the process whereby the restructuring of characters or groups of characters assures that a translation of information from one format occurs in a way that it is recognizable in another format.

b. Data formatting is the predetermined arrangement of bits, characters, fields, groups, lines, and punctuation marks.

30.4.2 Presentation-layer functions. The following functions are performed by the presentation layer:

a. Negotiation of syntax establishes the dialogue between the presentation entities on behalf of the application entities to determine the form the data will have during the initiation phase. The negotiations will determine what conversions are needed (if any) and where they will be performed.

b. The presentation layer interacts with both the next-higher and lower layer to pass or receive information regarding services requested and performed.

30.5 Application layer

30.5.1 Application-layer services provided. The application processes exchange data by means of application protocols and presentation services. As the only layer in the communications environment that directly provides services to the users, the application layer necessarily provides all services directly comprehensible to the users. Such services include, but are not limited to the following:

a. identification of intended communications partners (by name, by address, by description);

b. agreement on privacy mechanisms required;

c. authentication of intended communicants;

d. determination of acceptable quality-of-service (response time, tolerable error rate, cost vis-a-vis the previous considerations);

e. synchronization of cooperating applications;

f. selection of dialogue discipline, including initiation and release procedures;

g. agreement on procedure for data validity commitment;

h. identification of constraints on data syntax (character sets, data structure); and

i. information transfer.

30.5.2 Application-layer functions. The application layer contains all functions that support communication between open systems and that are not already performed by the lower layers. Pertinent functions are listed and defined below.

a. The application header is appended to the front of a message. It provides information to message processing functions, communications routing and switching equipment, application functions, and users/operators to ensure that message delivery, distribution, acknowledgment, timeliness, accountability, and security requirements are met. The application header provides the capability for specifying action and information addressees, security requirements (including special handling, access, or releasability restrictions), receipt/compliance (message acknowledgment) requirements, dating, and other accountability requirements.

b. Message acknowledgment is a return-to-sender code or character from the recipient of a message, verifying receipt of the text.

c. Application management functions are performed to ensure correct operations initiating, monitoring, and terminating activities between users. These management functions include the following:

(1) initialization of parameters representing application processes;

(2) initiation, maintenance, and termination of application processes;

(3) allocation and deallocation of resources to application processes;

(4) detection and prevention of resource interference and deadlock;

(5) integrity and commitment control;

(6) security control; and

(7) checkpointing and recovery control.

d. System management relates to the management of various resources and their status across all layers of the communications environment. Typical functions that fall into this category are as follows:

(1) Activation/deactivation management, including the following:

(a) activation, maintenance, and termination of resources distributed in open systems, including data links and communication media;

(b) program loading functions;

(c) establishment, maintenance, and release of connections between management entities; and

    (d) open systems parameter initialization/modification.

(2) Monitoring, including the following:

    (a) reporting status or status changes, and

    (b) reporting statistics.

(3) Error control, including the following:

    (a) error detection and some diagnostic functions, and

    (b) reconfiguration and restart.

APPENDIX C

NET ACCESS CONTROL ALGORITHM

10. GENERAL

10.1 Scope. This appendix describes the net access control (NAC) algorithm to be used in the DMTD.

10.2 Application. This appendix is a mandatory part of MIL-STD-188-220. The information contained herein is intended for compliance.

20. APPLICABLE DOCUMENTS. This section is not applicable to this appendix.

30. NET ACCESS CONTROL. The NAC protocol shall be used to detect the presence of active transmissions on a multiple-subscriber-access communications network and shall provide a means to preclude data transmissions from conflicting on the network. The stations shall implement the following four basic subfunctions:

a. net busy sensing

b. response hold delay (RHD)

c. timeout period (TP)

d. net access delay (NAD)

30.1 Net busy sensing function. The net busy function is used to establish the presence of a digital signal at the receiving station due to activity on the net. The particular implementation of this function depends on the station configuration in use: embedded COMSEC, external COMSEC, or no COMSEC. Net busy must be detected within a time period of $(32/n)$ seconds, where n is equal to the bit rate. Upon detection of a net busy, the data-link net busy indicator shall be set. The value of time to set the net busy indicator shall be a variable used in the RHD and TP timers, and shall be the same for all stations on the network. Setting the data-link net busy sensing indicator shall inhibit all message transmissions, including response-type messages. The data net-busy sensing indicator shall be reset upon indication from the physical layer that digital data is no longer detected by the net-busy sensing function.

30.2 Response hold delay. Two RHD values are calculated to determine the time that an addressed receiving station delays before sending a Type 1 response PDU upon receiving a Type 1 command PDU (UI, XID) requesting acknowledgment (that is, P-bit set to 1). An RHD period is the amount of time required for a single station to respond. The individual RHD is the time at which a particular station accesses the network. The individual RHD value to be used shall be determined by the position of the receiving station's address in the UI PDU destination portion of the address field. The value of all non-integer variables (that is, KT, E, S, T, and C) in the RHD equations are rounded to the nearest one-thousandth. The calculated values for RHD_i, TP, and NAD are rounded to the nearest tenth.

a. Each RHD period shall depend on five factors: the keytime delay; the currently selected transmission rate; the time for equipment turnaround; the time to transmit the crypto device preamble and postamble; and the time to transmit one status frame (72 bits if the FEC/TDC function is not selected), or one FEC-coded status frame (144 bits), or one FEC/TDC block (384 bits if the FEC/TDC function is selected). All stations on a subnet shall use the same values in calculating RHD.

b. One RHD_0 period shall be calculated by the following formula:

$$RHD_0 = KT + S + T$$

where

KT = Keytime delay, which is defined as the time interval from the start of a transmission event (such as an operation of a push-to-talk activation of a transmit command) to the start of the bit synchronization field. KT compensates for the transmission equipment (radio and COMSEC) start up and turnaround times to allow an end-to-end radio link to be established. The KT range shall be 0 to 5.6 seconds in 0.1-second increments. The KT parameter shall be the same value for all stations on the net. The minimum selectable value shall be the time required by the station experiencing the longest equipment delay time.

The term E shall be the sum of the following 4 time elements:

(1) The equipment turnaround time that is equal to the time to change from transmit to receive state, or the carrier drop-out time, whichever is greater

(2) The additional transmission time that is required by the cryptographic function. (See Appendix D.)

(3) The satellite delay time (ST) parameter that is required when determining NAD. The ST range shall be 0 to 2.0 seconds in 0.25-second increments when satellite transmission is used. A delay time of 0.0 seconds shall be used when satellite transmission is not used. The default time for satellite transmissions is 2.0 seconds. The ST parameter shall be the same value for all stations on the net.

The term *S* shall be the sum of the times required to transmit the following parameters:

(1) Bit synchronization by the physical layer. The value shall be $32/n$ if the physical layer is performing the bit synchronization procedure. The value shall be 0 if bit synchronization is performed by an external cryptographic device (the time is included in the variable *E*).

(2) The transmission synchronization pattern ($31/n$).

(3) The TWC ($24/n$).

(4) Plus one status frame ($72/n$) if the FEC/TDC function is not selected, or one FEC-coded status frame ($144/n$), or one FEC/TDC frame block ($384/n$) if the FEC/TDC is selected.

The term *T* is a tolerance term that compensates for the maximum deviation of other parameters. This term shall be selectable within a range of 0.0 to 0.5 seconds in 0.1-second increments, with 0.5 second as its default value.

c. The individual addressed stations' response hold delay (RHD_i) shall be calculated by

$$RHD_i = (i - 1)\ x\, RHD_0 + E - C$$

The variable i (where $1 \leq i \leq 16$) is the individual station's position in the destination portion of the address field.

The term *C* is the cryptographic device preamble time. The preamble transmission time required by the cryptographic function may vary, depending on factors such as the COMSEC approach (external or embedded), equipment, and transmission rate. The value can range nominally from 0.30 to 25 seconds for traditional COMSEC; from 0.36 to 1.6 seconds for narrowband COMSEC, and from 0.02 to 4.0 seconds for embedded COMSEC (as specified in the standard).

The values for *KT*, *C*, *E*, *S*, and *T* can be initialized locally or learned, using the XID messages described in Appendix C.

30.3 Timeout period. TP is the time all stations shall wait before they can schedule the NAD. During this window of time, the transmitting station shall wait to receive the anticipated response frame(s), if any, from all the addressed stations. TP shall equal 0 if no immediate Type 1 response (URR or XID) is expected (that is, P-bit set to 0). TP shall be computed after the station's equipment configuration has been established. If the equipment configuration is modified, TP shall be recomputed using the new parameters. The TP variable settings shall be the same for all stations on a subnet. A retransmission shall be executed whenever TP has been exceeded without acknowledgments having been received from all destinations. Prior to retransmission, the address field of the frame shall be modified automatically to delete the destination station(s) that previously acknowledged the frame. If EDAC is enabled, it is possible for the receiving stations to begin the NAD at different times as a result of the error correction processing time. To ensure that the receiving stations begin their NADs at the same time, the error correction processing time shall be subtracted from the calculated TP. Operationally, TP shall be used as follows:

a. Upon termination of a message transmission that requires an immediate response, the transmitting station shall set the TP timer. If the transmitting station does not receive all the expected responses (URR, URNR, or XID) within TP, and if the operator has selected the retransmission subfunction, the station shall automatically go into the retransmission sequence. If any other frame is received when a response-type frame (URR, URNR, or XID) is expected, procedures for the newly received frame type shall be followed and the TP procedures established for the previous UI or XID frame shall be discarded.

b. The TP shall be calculated by all stations on the net/link as follows. The value of all non-integer variables (that is, RHD_0, E, and C) in the TP equation are rounded to the nearest one-thousandth. The calculated value of TP is rounded to the nearest tenth.

$$TP = j \times (RHD_0) + E - C$$

where

j = The total number of destination individual link addresses for this transmitted frame

TP = 0 if no link acknowledgment has been requested

Note: *RHD*, *E*, and *C* were previously described.

30.4 Net access delay. NAD is defined as the time a station with a message to send shall wait to send a frame after the TP timer has expired. There are three schemes for calculating NAD. The random net access delay (R-NAD) scheme provides all stations with an equal chance to access the network. The prioritized net access delay (P-NAD) scheme ensures the highest precedence station with the highest priority message will access the net first. The hybrid net access delay (H-NAD) scheme combines random access with the preferential access by frame priority. The random and hybrid schemes might result in a collision (the same NAD value for two stations). The prioritized scheme always produces a unique NAD value for each station. In all of the NAD schemes, if the TP timer is active, the stations with frames to transmit shall wait for the TP timer to expire before the NAD is set. If the TP timer is not active, the station shall calculate its NAD using the proper NAD scheme for the network. Each NAD scheme produces a set of allowed access periods. The net may be accessed only at the beginning of one of those periods. If the NAD is larger than the length of time since the last TP timer expired, then the station may determine the next appropriate access period (if any) and access the network. Below are the frame reception and transmission procedures:

a. A station shall analyze a received frame to determine if a TP timer must be set. After the frame check sequence has been verified, the address and control fields are analyzed. If the received frame is either an XID or UI frame and the poll bit is set to 1, then a TP timer is set. Any other pending frames for transmission shall be placed on hold. If the received frame was not an XID or UI frame with the poll bit set, an R-NAD or H-NAD value shall be calculated and initiated if the net busy status is clear. The P-NAD values are constant and do not need to be recalculated. The values of all non-integer variables (that is, KT, C, ST, and B) in the NAD equation are rounded to the nearest one-thousandth. The calculated value of NAD is rounded to the nearest tenth.

b. If a station does not have a frame to transmit, a quiet timer (QT) shall be activated at the expiration of the TP timer. If a station later has a frame to transmit, it may compare its NAD value to the QT and access the net during its next appropriate NAD period. The prioritized schemes (H-NAD and P-NAD) must use a NAD period equal to or larger than the appropriate precedence level NAD value. If the QT value is greater than the largest NAD period that any station on the net could calculate, then any station with a frame to send may immediately access the net after testing the net busy indicator.

c. All stations shall continue to sense the link for data net busy and withhold transmission until the appropriate NAD period has expired. NAD shall be calculated as follows:

$$NAD = F \times (KT + C) + B + ST$$

where

F = the integer value derived from the P-NAD, H-NAD, or R-NAD calculation method described below

KT = the value of the keytime delay

C = the CRYPTO device preamble transmission time

B = the time to detect net busy. B shall be negotiated on the interface or predetermined. Its default value is $32/n$ where n is the bit rate.

ST = the satellite interface delay time.

NOTE: KT, C, ST, and B are initialized locally or learned using the XID messages described in Appendix E.

30.4.1 <u>Random net access delay</u>. The R-NAD calculation method shall ensure that each station has an equal chance of accessing the network. The random nature also may provide a resolution if an access conflict occurs. Each attempt to access the net potentially can use a NAD value different from the station's previous value. The integer value of F shall be obtained from a pseudorandom number generator. The range of the pseudorandom number depends on the number of stations (NS) in the network. F shall be an integer value (truncated) in a range between 0 and

(3/4)NS. *NS* can be learned through the XID join exchange, or fixed by a system parameter established at initialization.

30.4.2 Prioritized net access delay. The P-NAD calculation method shall ensure that the net access precedence order assigned to subscribers is preserved. Each station shall calculate three unique P-NAD values, one for each of the three frame precedence levels. The integer value of *F* shall be calculated as:

$$F = SP + MP + IS$$

where

SP = the subscriber precedence: SP = (subscriber rank -1) for the initial transmission; and $SP = 0$ for subsequent transmissions.

MP = the message priority: $MP = 0$ for all urgent messages; $MP = (NS + 1)$ for all priority messages; and $MP = 2 \times (NS + 1)$ for all routine messages, where NS is the number of subscribers on the network.

IS = the initial/subsequent factor: $IS = 0$ for the initial transmission, and $IS = NS$ for subsequent transmissions.

30.4.3 Hybrid net access delay. The H-NAD calculation method ensures that net access delay times are shorter for higher priority frames, while maintaining equal access chances for all stations. Each priority level has a distinct range of pseudorandom *F* values determined by the number of stations in the subnetwork, the network percentage of the particular priority level frames, and the traffic load. The integer value of *F* shall be calculated as

$$F = MIN + RAND \times (MAX - MIN)$$

where MAX and MIN are integer values defining the ranges:

RAND = pseudorandom number in the range 0.0 to 1.0

Urgent_MIN = 0, for urgent frames
Urgent_MAX = USIZE + 1, for urgent frames

Priority_MIN = Urgent_MAX + 1, for priority frames
Priority_MAX = Priority_MIN + PSIZE + 1, for priority frames

Routine_MIN = Priority_MAX + 1, for routine frames
Routine_MAX = Routine_MIN + RSIZE + 1, for routine frames

USIZE = the additional number of random numbers generated for urgent frames

PSIZE = the additional number of random numbers generated for priority frames

RSIZE = the additional number of random numbers generated for routine frames

where

the minimum MIN/MAX range size is 2. The additional range sizes (xSIZE) are integers based on the percent of frames expected at a specific priority level (%priority_level) and the number of stations adjusted (ADJ_NS) by the expected traffic load (TL). NS, %priority_level, and TL, may be input using the XID frames or by system input. xSIZE is rounded to the nearest non-negative integer.

$USIZE = \%U \times ADJ\_NS,$ $\%U$ = percentage of urgent frames (default 25%)

$PSIZE = \%p \times ADJ\_NS,$ $\%P$ = percentage of priority frames (default 25%)

$RSIZE = \%R \times ADJ\_NS,$ $\%R$ = percentage of routine frames or 100% - $(\%U + \%P)$ (default 50%)

where

the adjusted number of stations increases if the expected TL is heavy and decreases if the traffic load is light. The minimum random number range at each of the three priority levels is 2, so 6 stations are subtracted from the adjusted number of stations.

$$ADJ\_NS = INT(NS \times TL) - 6$$

$$or = 1$$

$$(whichever\ is\ greater)$$

TL = 1.2 Heavy Traffic Load
1.0 Normal Traffic Load
0.8 Light Traffic Load

APPENDIX D-1

COMMUNICATIONS SECURITY STANDARDS

10. GENERAL

10.1 Scope. This appendix describes the COMSEC interoperability parameters for the DMTD subsystem. It defines the technical requirements for backward-compatible (traditional) and forward-compatible (embedded) interface modes. See classified Appendix D-2 for additional information.

10.2 Application. This appendix is a mandatory part of this MIL-STD. The information contained herein is intended for compliance.

10.3 Interoperability. This appendix cannot guarantee the DMTD user end-to-end interoperability. The selection of COMSEC and signaling is a function of communications media. Traditional COMSEC equipment is specific to communications media and may not be compatible due to signaling differences. The systems integrators and systems planners must ensure that compatible media and signaling are chosen if interoperability is desired. This COMSEC specification will provide for interoperability of the underlying encryption algorithm.

20. APPLICABLE DOCUMENTS

a. (U) ON431125 WINDSTER Cryptographic Standards

b. (U) DS-68 INDICTOR Cryptographic Standards

30. DEFINITIONS. Refer to Appendix A.

40. GENERAL REQUIREMENTS. The backward-compatible mode applies when link encryption for DMTD subsystems is provided by external COMSEC devices. These external COMSEC devices may be standalone equipment (such as the VINSON and KG-84) or communications equipment with embedded COMSEC (such as SINCGARS). The forward-compatible mode shall apply for all future DMTD subsystems that will embed COMSEC within the DMTD. The backward-compatible mode may also be emulated using embedded COMSEC devices.

50. DETAILED REQUIREMENTS

50.1 Traditional COMSEC transmission frame. The traditional COMSEC transmission frame shall be composed of the following components, as shown in Figure D-1.

a. COMSEC synchronization

b. Bit synchronization

c. Transmission synchronization

d. Data field

e. COMSEC postamble

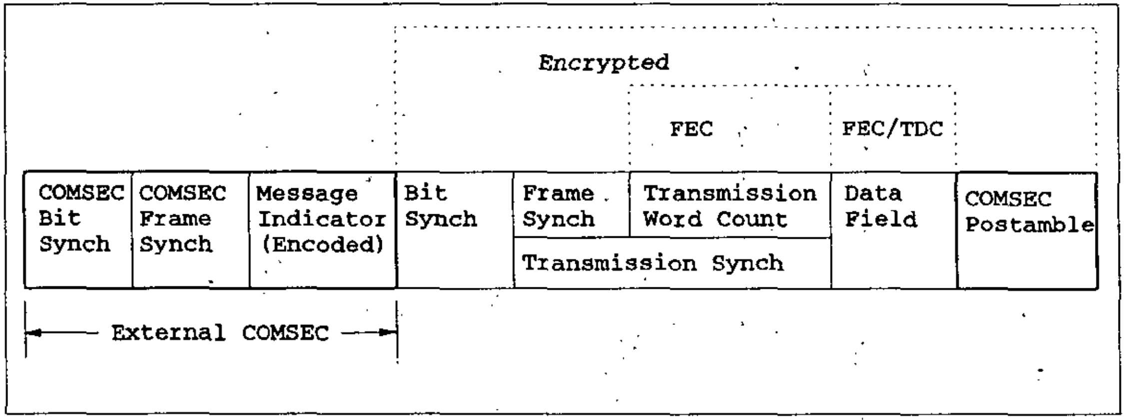


FIGURE D-1. Traditional COMSEC transmission frame structure.

50.1.1 COMSEC synchronization field. The COMSEC synchronization field shall consist of three components: a COMSEC bit synchronization subfield, a COMSEC frame synchronization subfield, and a Message Indicator (MI) subfield. This field is used to achieve cryptographic synchronization over the link.

50.1.1.1 COMSEC bit synchronization subfield. This subfield shall be used to provide a signal for achieving bit synchronization and for indicating activity on a data link to the receiver. The duration of the bit synchronization field shall be selectable from 200 milliseconds to 1.5 seconds. The bit synchronization subfield shall consist of the data-rate clock signal for the duration of the subfield.

50.1.1.2 COMSEC frame synchronization subfield. This subfield shall be used to provide a framing signal indicating the start of the encoded MI to the receiving station. This subfield shall be 465 bits long, consisting of 31 Phi-encoded bits, as shown in Figure D-2. The Phi patterns are a method of redundantly encoding data bits. A logical 1 data bit shall be encoded as a Phi(1)=111101011001000, and a logical 0 data bit shall be encoded as a Phi(0)=000010100110111. A simple majority voting process may be performed at the receiver to decode the Phi-encoded frame pattern to its original format.

50.1.1.3 Message Indicator subfield. This subfield shall contain the COMSEC-provided MI, a stream of random bits that are redundantly encoded using Phi patterns. Cryptographic synchronization is achieved when the receiver acquires the correct MI.

LSB MSB

1111111111111111111111111111110

FIGURE D-2. COMSEC frame synchronization pattern for Phi encoding.

50.1.2 Bit synchronization field. This field shall be as defined in 5.2.1.2.

50.1.3 Transmission synchronization field. This field, consisting of the frame synchronization subfield and the TWC subfield, shall be as defined in 5.2.1.3.

50.1.4 Data field. This field shall be as defined in 5.2.1.4.

50.1.5 COMSEC postamble field. This field shall be used to provide an end-of-transmission flag to the COMSEC at the receiving station. This will be automatically performed by the COMSEC key generator. Refer to ON431125, *WINDSTER Cryptographic Standards*, or DS-68, *INDICTOR Cryptographic Standards*, as appropriate.

50.1.6 COMSEC algorithm. The COMSEC algorithm shall be backward-compatible with VINSON and SINCGARS equipment. Refer to ON431125, *WINDSTER Cryptographic Standards*.

50.1.7 COMSEC modes of operation. The COMSEC shall be operated in Mode A. The rekey functions shall be performed through the use of KY-57 rekeys for backward compatibility. Refer to ON431125, *WINDSTER Cryptographic Standards*.

50.2 Embedded COMSEC transmission frame. The embedded COMSEC transmission frame shall be composed of the following components, as shown in Figure D-3.

a. Bit synchronization

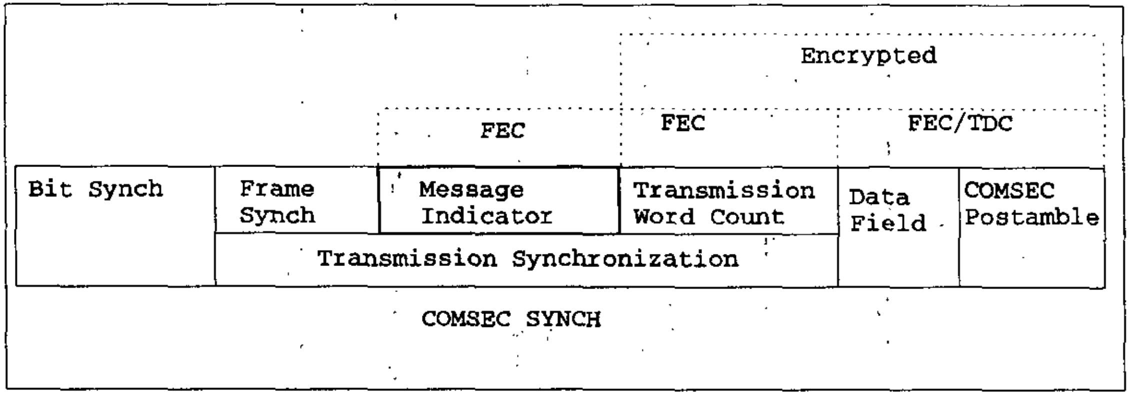


FIGURE D-3. Embedded COMSEC transmission frame structure.

b. Frame synchronization

c. Message indicator

d. Transmission word count

e. Data field

f. COMSEC postamble

50.2.1 Bit synchronization field. This field shall be used to provide a signal for achieving bit synchronization for the message as well as the COMSEC, and for indicating activity on a data link to the receiver. The duration of the bit synchronization field shall be as defined in 5.2.1.2.

50.2.2 Frame synchronization field. This field shall be as defined in 5.2.1.3.1. The frame synchronization is to be provided for both the message frame and the COMSEC.

50.2.3 Message Indicator field. This field shall contain the MI, a stream of random data that shall be encoded using half-rate Golay, as defined in 5.3.9. Cryptographic synchronization is achieved when the receiver acquires the correct MI. The COMSEC shall provide the MI bits. For backward compatibility, these MI bits must be redundantly encoded using Phi patterns, as described in 50.1.1.

50.2.4 Transmission word-count field. This field shall be as defined in 5.2.1.3.2.

50.2.5 Data field. This field shall be as defined in 5.2.1.4.

50.2.6 COMSEC postamble field. This field shall be used to provide an end-of-transmission flag to the COMSEC at the receiving station. The flag shall be a cryptographic function and may be used by the data terminal as an end-of-message flag as well.

50.2.7 COMSEC algorithm. Refer to 0N431125, *WINDSTER Cryptographic Standards.*

50.2.8 COMSEC modes of operation. COMSEC shall be operated in Mode A for all applications. The rekey functions will be performed through the use of KY-57 rekeys for backward-compatibility and will be performed through over-the-air-rekeying (OTAR) techniques for forward compatibility. Rekey signaling for OTAR must be supplied by the host equipment. Refer to 0N431125, *WINDSTER Cryptographic Standards.*

(This page intentionally left blank)

APPENDIX E

DATA-LINK MANAGEMENT PROCESSES

10. GENERAL

10.1 Scope. This appendix describes the management processes associated with the data-link layer.

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS. ISO 8885, General Purpose XID Frame Information Field Content and Format.

30. EXCHANGE IDENTIFICATION FRAME. The XID frame format of the high-level data-link control (HDLC) protocol is used to request or disseminate data-link-layer information. The XID format is in accordance with ISO 8885. At initialization time, a station can request link operating parameters that may be unknown. The XID user message types have been designed to provide management capabilities at the link layer. However, they are not required if all the stations on the net have been configured with link addresses and operating parameters prior to initialization.

30.1 XID format. The information field of the XID frame is comprised of up to three identifiers and a MIL-STD-188-220 defined message. A format identifier is in the first octet of the information field and indicates that the XID frame is in accordance with ISO 8885. A group identifier follows the format identifier. The first group identifier may either indicate a request for HDLC parameter negotiation or, if no HDLC negotiation is required, the group identifier shall indicate that a MIL-STD-188-220 defined message follows. The HDLC parameter negotiation group contains several optional parameters, as shown in Table E-1. Only those parameters that are being negotiated shall be present (as indicated by the parameter identifier) in the HDLC group field. Table E-2 shows the format that shall be used when HDLC negotiation is not required. All XID frames shall contain the MIL-STD-188-220 defined group, which is designated by the group value 255 (the value for user data in ISO 8885). One of the MIL-STD-188-220 messages, listed in Table E-3 and defined in Tables E-4 through E-7, shall follow the MIL-STD group identifier.

30.2 XID command/response messages. XID command messages (Join Request and Hello) shall have the C/R bit in the source address set to 1. The XID response messages (Join Accept and Join Reject) shall have the C/R bit set to 0.

30.3 XID poll/final bit. The Join Request message requires an immediate response from the receiving station (before any other station accesses the network) and, therefore, shall set the poll bit (bit 5 in the control field) to 1. The Hello message shall set the poll bit to 0 and requires no response. The Join Accepted and Join Rejected messages are contained in an XID response frame. These messages are responding to the Join Request frame whose poll bit was set to 1. Therefore, the final bit of the two Join responses shall be set to 1.

40. PARAMETERS TO NEGOTIATE. Two sets of parameters are contained in the XID messages. The first is parameter negotiations, defined by ISO 8885. The second is MIL-STD-188-220-specific and located in the user data subfield of the XID frame.

40.1 HDLC parameters. The ISO group identifier number 1 is used to encode the parameter negotiation function. Within that group, parameter identifiers 3, 5, 6, 7, and 8 are used. Parameter identifier 3 indicates that the HDLC options are to be negotiated. HDLC optional functions are represented in a 3-byte field to show which HDLC options are requested for use. Other HDLC parameters used for negotiation are parameter identifiers 5 and 6 that pass the length of the maximum transmit and receive information fields (up to 3500 bytes). HDLC parameter identifiers 7 and 8 are used to set the maximum transmit and receive window values, which are 0 for DMTDs.

40.2 MIL-STD-188-220 parameters. MIL-STD-188-220 specific initialization parameters are contained in the user data subfield of the XID Join messages (Request, Accept, and Reject). A new station's link address shall be assigned by NETCON. An originator of the Join Request may use a special net entry link address of 1, which has been reserved for temporary use by a station requesting link address assignment. To prohibit more than one station using that address at any one time, the join network message will set the acknowledge bit (P bit) to permit the Join Accept or Reject message to be returned before any other station can access the net. The reject or accept message will use the originator's link address contained in the source address field of the received Join Request message. The newly assigned link address is contained in the Join Accept or Reject message. To request information, a parameter field will contain all 1s, which will be interpreted as "empty."

TABLE E-1. XID format with parameter negotiation.

BYTE NUMBER	FIELD NAME	LSB MSB	VALUE
1	ORIGINATOR ADDRESS	XXXXXXXX	3 to 95; 1 allowed with message 20; 2 also allowed with messages 21-22.
2	DESTINATION ADDRESS	XXXXXXXX	3 to 95; 1 allowed with messages 21-22; 2 allowed with message 20.
3	CONTROL FIELD	11111101	XID FRAME
4	FORMAT IDENTIFIER	01000001	130 General-Purpose XID Information
5	GROUP IDENTIFIER	00000001	128
6 7	GROUP LENGTH	00000000 11001000	19 (Number of bytes to follow)
8	PARAMETER IDENTIFIER	11000000	3
9	PARAMETER LENGTH	11000000	3 bytes
10 11 12	HDLC OPTION	0XX0000X 10XXX000 10000000	OPTIONS: Type 1: 8,10A,14B Type 1 and 2: 2, 3, 7B, 8, 10B, 11, 14B
13	PARAMETER IDENTIFIER	10100000	5
14	PARAMETER LENGTH	01000000	2 bytes
15 16	TRANSMIT INFORMATION FIELD LENGTH	XXXXXXXX XXXX0000	up to 3500 bytes
17	PARAMETER IDENTIFIER	01100000	6
18	PARAMETER LENGTH	01000000	2 bytes
19 20	RECEIVE INFORMATION FIELD LENGTH	XXXXXXXX XXXX0000	up to 3500 bytes
21	PARAMETER IDENTIFIER	11100000	7
22	PARAMETER LENGTH	10000000	1 byte
23	WINDOW SIZE	00000000	0-127; Type 2
24	PARAMETER IDENTIFIER	00010000	8
25	PARAMETER LENGTH	10000000	1 byte
26	WINDOW SIZE (k)	00000000	0-127; Type 2
27	GROUP IDENTIFIER	11111111	255 (User subfield follows)

TABLE E-2. XID format without HDLC parameter negotiation.

BYTE NUMBER	FIELD NAME	L S B M S B	VALUE
1	ORIGINATOR ADDRESS	XXXXXXXX	3 to 95; 1 may also be used for message 20; 2 may be used for messages 21-22
2	DESTINATION ADDRESS	XXXXXXXX	3 to 95; 1 allowed in messages 21-22; 2 allowed in message 20 global address for message 25
3	CONTROL FIELD	1111X101	XID FRAME
4	FORMAT IDENTIFIER	01000001	130 General-Purpose XID Information
5	GROUP IDENTIFIER	11111111	255

40.2.1 Link management messages. Table E-3 lists four XID link management messages. Three messages are used in the procedure for a station to request or verify the network operating parameters. At initialization, a station can send the Join Request message, and the NETCON station will either accept or reject the request to join. The Hello message allows an initiating station to announce its link address. Tables E-1 and E-2 show the XID frame formats that precede the user data subfield. The user data subfield of each message is presented in Tables E-4 through E-7.

40.2.2 Join the network messages. Three messages are used to convey network operating parameters. The initializing station sends the request to join message, and the NETCON replies with either an accept or reject message. Figure E-1 shows the message exchange when the link address is to be assigned.

40.2.2.1 Network control station. In a network that expects a station to request link operating parameters, one station must be designated the NETCON station. Only the NETCON will respond to those requests and therefore eliminate excessive response frames. The designation of the NETCON station will be done by a network authority. The data-link address 2 is a special address for the network control station. All stations can address the network control station by using that special address. The network control station may also be assigned an additional individual data-link address that it shall also recognize. All stations should be capable of performing the functions of NETCON. An operator command either at initialization or during normal operation times may inform the station of its NETCON responsibility.

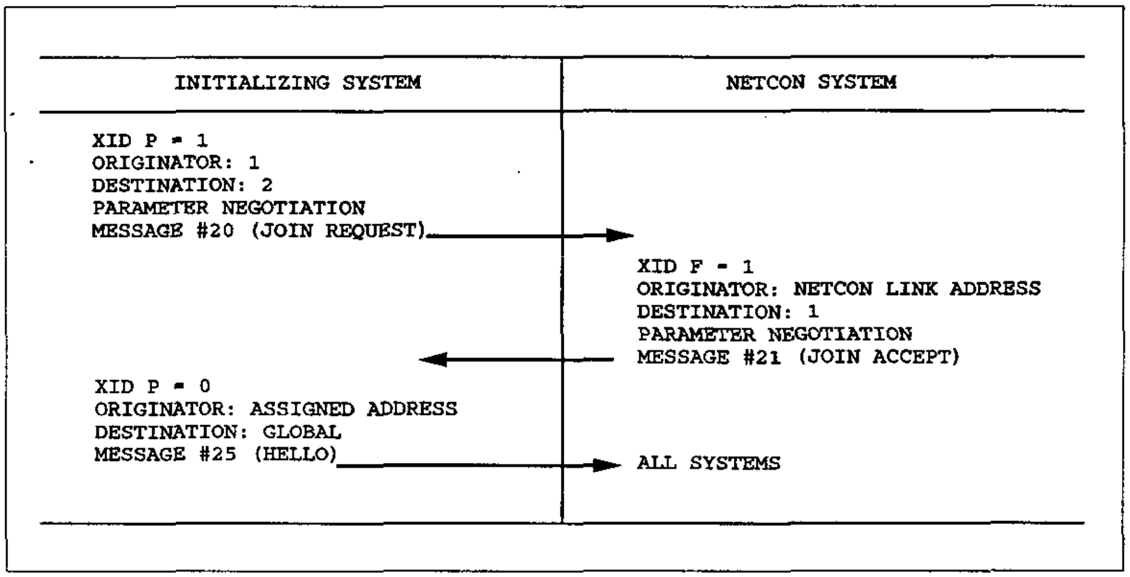


FIGURE E-1. Sample message exchange with successful link address assignment.

TABLE E-3. Link management messages.

MESSAGE NUMBER	TITLE	DESCRIPTION
20	Join Request	Request operating parameters assignment, validation, or both
21	Join Accepted	Accepts the Join Request
22	Join Rejected	Rejects the Join Request with errors indicated
25	Hello	Announces link address for an initiating station

NOTE: Messages 20-22 may be used with the XID formats with or without parameter negotiation (Tables E-1 and E-2). Message 25 may be used only with the XID format without negotiation.

40.2.2.2 Message exchange sequence. The initializing station sends to the NETCON station an XID Join Request message, which may contain the HDLC options it has implemented and known MIL-STD-188-220 parameters. MIL-STD-188-220 parameter fields that are left empty (a bit pattern of all 1s) indicate a request for NETCON to supply the parameters. The NETCON station compares the HDLC and MIL-STD-188-220 parameter fields with current network operating parameters. If an error is found in either portion, a Join Reject message is sent, entering all of the correct parameters into the frame and marking the error field to indicate the corrected parameters. Figure E-2 shows the error field indicators. If there is no error, a Join Accept message is sent after entering the parameters for any empty MIL-STD-188-220 parameter fields.

ERROR INDICATOR VALUES

HDLC OPTION	LINK ADDRESS	SYSTEM PRIORITY	KEYTIME DELAY	TOLERANCE TIME	NET ACCESS	NET BUSY DETECTION TIME	RESPONSE MODE	SYSTEM CLASS	NET ACCESS METHOD	NUMBER OF SUBSCRIBERS	INVALID MESSAGE	RESERVED	RESERVED	RESERVED	RESERVED

LSB MSB

Identifies the fields in error in a Join Request Message (#20)

Bit = 0 indicates no error in defined field
Bit = 1 indicates error in defined field

FIGURE E-2. Join Reject error indicators.

40.2.3 Hello Message. This message is sent after the link operating parameters are known and the station is ready to enter the network. The message contains the link address of the station entering the network. Address tables within the receiving station are updated, if necessary, with the new address information. The global destination link address is used in the address field so all stations will receive the message. Acknowledgments are not allowed for this message.

50. NET ACCESS. The set of join messages makes it possible for a station to know little about the network configuration when it is initializing. This flexibility requires some special handling of the frames. FEC usage cannot be learned because it encodes

the entire frame. The FEC state must be known before entry into the net.

50.1 Net-access delay method. MIL-STD-188-220 allows a network to choose among 3 net-access delay schemes. Each station that operates on the net must use the same scheme. If the station does not know this information before initialization, the join network request message allows a station to learn the net access scheme. To minimize the chance of collision, the random scheme will be assumed when this message is sent.

50.2 Use of forward error correction. The FCS will fail for every frame if FEC is not employed properly. The operator should be notified if the dropped-frame rate is high. A new station entering the net must know the current FEC usage state to be able to interoperate.

APPENDIX E

TABLE E-4. Join Request message.

BYTE NUMBER	FIELD IDENTIFICATION	FIELD SIZE (BITS)	VALUE
1	Message number: Identifies specific message content	8	20
2	Link address: Identifies the link address of the station to be initialized	8	255 = Requesting address be assigned. 3 to 95 actual link addresses.
3	Station priority: Identifies comparative ranking of stations on the net.	8	255 = Requesting priority be assigned. 0 = priority not used. 1 to 95 = actual priority value.
4	Keytime delay value: Equipment-dependent delay time (KT) used in net access delay time calculations.	8	255 = Requesting value be conveyed. 0.0 to 5.6 seconds in 0.1-second increments.
5	Tolerance Time: A factor *T* to compensate for the variance of other variables in the RHD formula.	8	0 to 0.5 seconds in increments of 0.1 seconds. Default is 0.5 seconds.
6	Net busy detection time: The time required to detect net busy. This is the variable B in the net-access delay formula.	8	255 = Requesting value be conveyed. 0 to 2.5 seconds in increments of 0.01 seconds.
7	Response mode: The state and capability of the station to send automatic acknowledgments.	8	0 = Always on; 1 = off; 2 = on, but can select off. Default = 2.
8	Station Type: The type of operations provided by the station.	8	1 = Type 1 2 = Type 1 and 2
9	Net access method: Net access method to be used on the net.	8	255 = Requesting access scheme be conveyed. 0 = random; 1 = priority; 2 = hybrid.
10	Number of stations: Specifies the maximum number of stations (NS) expected on the net. Used in all three NAD algorithms.	8	255 = Requesting NS. 2-32 = AFATDS actual number.
11	Percent of Urgent Frames: The percentage of urgent (%U) frames expected in an average 24-hour period. Used in the H-NAD algorithm.	8	255 = Requesting %U. 0 to 100 in multiples of 5. 25 = default
12	Percent of Priority Frames: The percentage of priority (%P) frames expected in an average 24-hour period. Used in the H-NAD algorithm.	8	255 = Requesting %P. 0 to 100 in multiples of 5. 25 = default
13	Traffic Load: Traffic load (TL) expected on the subnetwork. Used in the H-NAD algorithm.	8	255 = Requesting TL. 0 = Normal; 1 = Heavy; 2 = Light.

TABLE E-5. Join Accept message.

BYTE NUMBER	FIELD IDENTIFICATION	FIELD SIZE (BITS)	VALUE
1	Message number: Identifies specific message content	8	21
2	Link address: Identifies the link address of the station to be initialized	8	3 to 95 actual link address.
3	Station priority: Identifies comparative ranking of stations on the net.	8	0 = priority not used. 1 to 95 = actual priority value.
4	Keytime delay value: Equipment-dependent delay time (KT) used in net-access-delay time calculations.	8	0.0 to 5.6 seconds in 0.1 second increments.
5	Tolerance Time: A factor *T* to compensate for the variance of other variables in the RHD formula.	8	0 to 0.5 seconds in increments of 0.1 seconds. Default is 0.5 seconds.
6	Net busy detection time: The time required to detect net busy. This is the variable *B* in the net-access delay formula.	8	0 to 2.5 seconds in increments of 0.01 seconds.
7	Response mode: The state and capability of the station to send automatic acknowledgments.	8	0 = Always on; 1 = off; 2 = on, but can select off. Default = 2.
8	Station Type: The type of operations provided by the station.	8	1 = Type 1. 2 = Type 1 and 2.
9	Net access method: Net access method to be used on the net.	8	0 = random; 1 = priority; 2 = hybrid.
10	Number of stations: Specifies the maximum number of stations (NS) expected on the net. Used in all three NAD algorithms.	8	0 to 255 allowed. 2-32 = AFATDS actual number.
11	Percent of Urgent Frames: The percentage of urgent frames (%U) expected in an average 24-hour period. Used in the H-NAD algorithm.	8	0 to 100 in multiples of 5. 25 = default.
12	Percent of Priority Frames: The percentage of priority frames (%P) expected in an average 24-hour period. Used in the H-NAD algorithm.	8	0 to 100 in multiples of 5. 25 = default.
13	Traffic Load: Traffic load (TL) expected on the subnetwork. Used in the H-NAD algorithm.	8	0 = Normal; 1 = Heavy; 2 = Light. Default = 0.

TABLE E-6. Join Reject message.

BYTE NUMBER	FIELD IDENTIFICATION	FIELD SIZE (BITS)	VALUE
1	Message number: Identifies specific message content.	8	22
2	Link address: Identifies the link address of the station to be initialized.	8	3 to 95 actual link address.
3	Station priority: Identifies comparative ranking of stations on the net.	8	0 = priority not used. 1 to 95 = actual priority value.
4	Keytime delay value: Equipment-dependent delay time (KT) used in net-access-delay time calculations.	8	0.0 to 5.6 seconds in 0.1-second increments.
5	Tolerance Time: A factor *T* to compensate for the variance of other variables in the RHD formula.	8	0 to 0.5 seconds in increments of 0.1 seconds. Default is 0.5 seconds.
6	Net busy detection time: The time required to detect net busy. This is the variable *B* in the net-access delay formula.	8	0 to 2.5 seconds in increments of 0.01 seconds.
7	Response mode: The state and capability of the station to send automatic acknowledgments.	8	0 = Always on; 1 = off; 2 = on, but can select off. Default = 2.
8	Station Type: The type of operations provided by the station.	8	1 = Type 1. 2 = Type 1 and 2.
9	Net access method: Net access method to be used on the net.	8	0 = random; 1 = priority; 2 = hybrid.
10	Number of stations: Specifies the maximum number of stations (NS) expected on the net. Used in all three NAD algorithms.	8	0 to 255 allowed. 2-32 = AFATDS actual number.
11	Percent of Urgent Frames: The percentage of urgent Frames (%U) expected in an average 24-hour period. Used in the H-NAD algorithm.	8	0 to 100 in multiples of 5. 25 = default.
12	Percent of Priority Frames: The percentage of priority frames (%P) expected in an average 24-hour period. Used in the H-NAD algorithm.	8	0 to 100 in multiples of 5. 25 = default.
13	Traffic Load: Traffic load expected in the subnetwork. Used in the H-NAD algorithm.	8	0 = Normal; 1 = Heavy; 2 = Light. Default = 0.
14	Error Indicator: A bit map to identify the fields that contained errors. Appropriate values were substituted.	16	See Figure E-2 for bit meaning.

TABLE E-7. Hello message.

BYTE NUMBER	FIELD IDENTIFICATION	FIELD SIZE (BITS)	VALUE
1	Message Number: Identifies specific message content.	8	25
2	Link Address: Identifies the link address of the station to be initialized.	8	3 to 95 actual link addresses.

(This page intentionally left blank)

APPENDIX F

GOLAY CODING ALGORITHM

10. GENERAL

10.1 Scope. This appendix contains amplifying information in support of MIL-STD-188-220.

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS

30. FORWARD ERROR CORRECTION. The FEC method requires the receiver to detect and automatically correct errors in a received block of information. The number of errors the receiver can detect and correct depends on the coding method. The information bits (k) are separated into blocks that contain both information bits and code bits. The length of the block, including the information and code bits, is (n). The code is described as (n,k), where n is the length of the block and k is the number of information bits in the block.

40. GOLAY CODE. The Golay code is a linear, block, perfect, and cyclic (23,12) code capable of correcting any combination of three or fewer errors in a block of 23 digits. The generator polynomial for this code is

$$g(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

where

$$g(x) \text{ is a factor of } x^{23} + 1$$

40.1 Half-rate Golay code. The half-rate Golay code (24,12) is formed by adding a 0 fill-bit to the Golay (23,12) code. The (24,12) code is preferable to the (23,12) because it has a code rate of exactly one-half. This code rate simplifies system timing.

40.2 Golay code implementation. The Golay code may be implemented in either hardware or software. The hardware implementation uses shift-registers for encoding and decoding, as described in 40.2.1 and 40.2.2, respectively. The software implementation uses a generator matrix and conversion table, as described in 40.2.3.

40.2.1 Hardware implementation. Golay code encoding can be performed with an 11-stage feedback shift register with feedback connections selected according to the coefficients of $g(x)$. A shift register corresponding to the coefficients of $g(x)$ is shown in Figure F-1. The k information bits are located at the beginning of the *n* symbol block code. With the gate open, the information bits are loaded into the shift register stages and simultaneously into the output channel. At this time the shift register contains the check symbols. With the gate closed, register contents are then shifted onto the output channel. The last $n - k$ symbols are the check symbols that form the whole codeword.

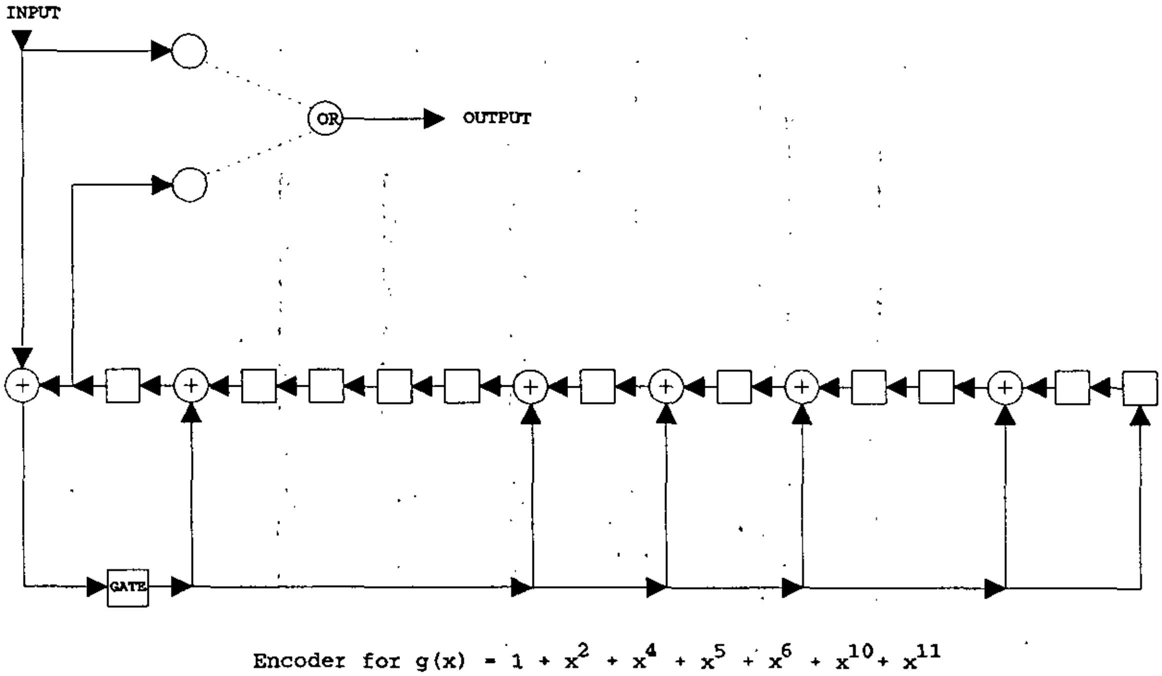


FIGURE F-1. Shift register encoder for the (23, 12) Golay code.

40.2.2 Hardware decoding. The Golay code is decoded using a number of techniques such as the error-trapping process developed by T. Kasami. The Kasami error-trapping decoder for the Golay code is shown in Figure F-2. It works as follows:

1. Gates 1, 3, and 5 are opened, and gates 2 and 4 are closed. The received codeword $r(x)$ is then shifted into both the 23-stage shift register and the syndrome register. At the same time, the previously corrected codeword is shifted out to the user. The syndrome

$$S(x) = S_0 + S_1x + . . . + S_{10}x_{10}$$

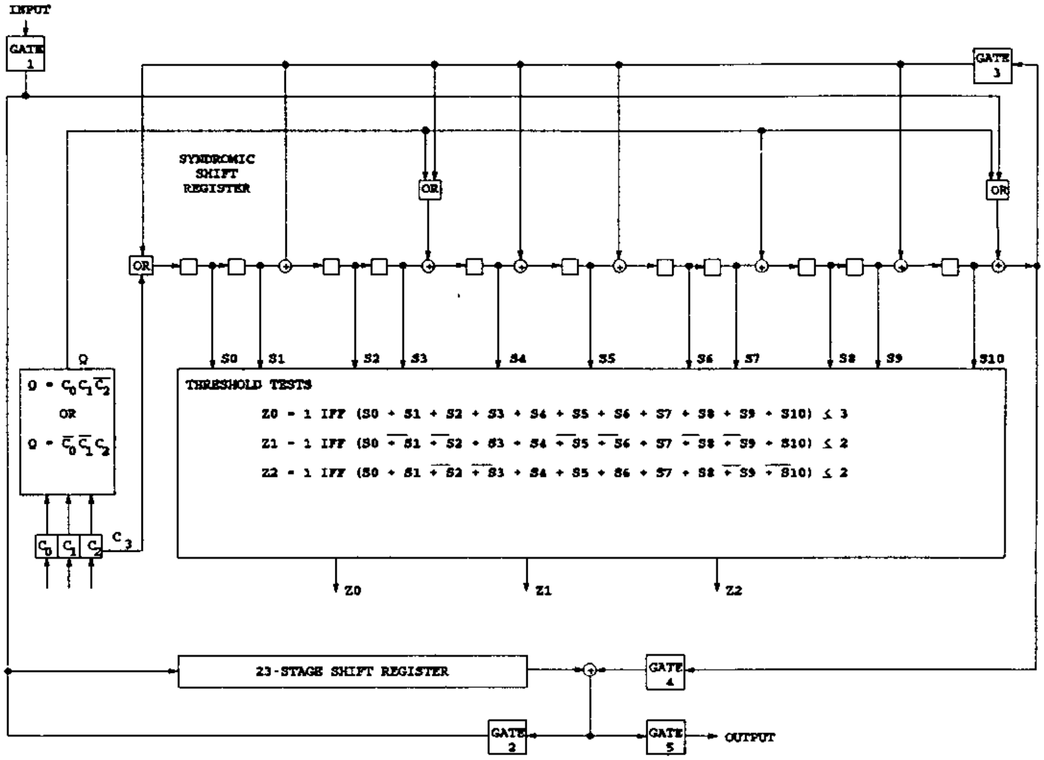


FIGURE F-2. Kasami error-trapping decoder for the (23, 12) Golay code.

is then formed and subjected to threshold tests.

2. Gates 1, 4, and 5 are closed and gate 2 is opened. Gate 3 remains open. The threshold tests occur in the following order:

   a. If Z_0 is unity, then all the errors are confined to the 11 high-order positions of $r(x)$, and $S(x)$ matches the errors. Z_0 opens gate 4 and closes gate 3. Contents of both the 23-stage shift register and the syndrome shift register are then shifted 11 times, and the errors are corrected. Then gate 4 is closed and the contents of the 23-stage shift register are shifted until the received codeword is in its original position. The decoder then goes to step 3 below.

   b. If Z_1 is unity, the error pattern in $S(x)$ is the same as the errors in the 11 high-order bits of the codeword $r(x)$, and a single error exists at location x^5. Gate 4 is opened and gate 3 is closed. The counter is preloaded with a count of

2, and both the syndrome shift register and the 23-stage shift register are shifted until the error in x^5 is corrected. Then gate 4 is closed, and the contents of the 23-stage shift register are shifted until the received codeword is in its original position. The decoder then goes to step 3.

c. If Z_2 is unity, the error pattern in $S(x)$ is the same as the errors in the 11 high-order bits of the codeword $r(x)$, and there is a single error in location x^6. The same steps are followed as in b (above) except that the counter is preloaded with a count of 3. The decoder then goes to step 3.

d. If neither of the three thresholds is unity, the decoder goes directly to step 3.

3. Gates 1, 4, and 5 are closed, and gates 2 and 3 are opened. Contents of both the 23-stage shift register and the syndrome shift register are then shifted once to the right. The decoder then goes to step 2.

4. This action continues until step 3 has been executed 46 times. Then the decoder returns to step 1 to process the next received codeword.

The decoder always yields an output. The output is correct if there were 3 or fewer errors in the received codeword, and erroneous if there were more than 3 errors in the codeword.

40.2.3 Software implementation. The transmitting DMTD shall generate the check bits using the following generator polynomial:

$$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

Note that using modulo 2 addition,

$$x^{23}+1 = (x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)\ (x^{11}+x^9+x^7+x^6+x^5+x+1)\ (x+1)$$

The 11 check bits shall be as derived from the following generator matrix G:

$$\begin{array}{r|ccccccccccccccccccccccc|l}
 & X^{22} & ^{21} & ^{20} & ^{19} & ^{18} & ^{17} & ^{16} & ^{15} & ^{14} & ^{13} & ^{12} & ^{11} & ^{10} & ^{9} & ^{8} & ^{7} & ^{6} & ^{5} & ^{4} & ^{3} & ^{2} & ^{1} & X^{0} & \\
\hline
x^{11} \;.\; g(x) = & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
x^{10} \;.\; g(x) = & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
x^{9} \;.\; g(x) + x^{11} \;.\; g(x) = & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
x^{8} \;.\; g(x) + x^{10} \;.\; g(x) = & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
x^{7} \;.\; g(x) + x^{9} \;.\; g(x) = & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
(x^{6} + x^{8} + x^{11}) \;.\; g(x) = & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & = G \\
(x^{5} + x^{7} + x^{10}) \;.\; g(x) = & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \\
(x^{4} + x^{6} + x^{8}) \;.\; g(x) = & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \\
(x^{3} + x^{5} + x^{8} + x^{11}) \;.\; g(x) = & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \\
(x^{2} + x^{4} + x^{7} + x^{10} + x^{11}) \;.\; g(x) = & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \\
(x + x^{3} + x^{5} + x^{9} + x^{10} + x^{11}) \;.\; g(x) = & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \\
(1 + x^{2} + x^{5} + x^{8} + x^{9} + x^{10} + x^{11}) \;.\; g(x) = & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \\
\hline
 & \multicolumn{11}{c}{\text{Parity}} & \multicolumn{12}{c}{\text{Identity}} & \\
\end{array}$$

where

the matrix contains the coefficients of the polynomials on the left. By interchanging the I and P columns to obtain matrix *T*, that is,

$$G = [P, I]_{(12 \times 23)} \;=\; > [I, P]_{(12 \times 23)} \;=\; T$$

$$T = \left[\begin{array}{ccccccccccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1\\
0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&1&1&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&1&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1
\end{array}\right]$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{I}\quad\underbrace{\qquad\qquad\qquad\qquad}_{P}$$

the transmission order and value of the code word bits can be obtained by matrix multiplication (modulo 2 addition without carry) as follows:

$$\underset{\substack{\uparrow\\ \text{FIRST BIT TRANSMITTED}}}{\left[\text{Ib}_1\ \text{INFO BITS Ib}_{12}\right]_{(1\text{x}12)}} \cdot \left[\text{I, P}\right]_{(12\text{x}23)} = \underset{\substack{\uparrow\\ \text{FIRST BIT TRANSMITTED}}}{\left[\text{INFO BITS, CHECK BITS}\right]_{(1\text{x}23)}}$$

APPENDIX G

VARIABLE MESSAGE FORMAT SYNTAX AND STRUCTURE

10. GENERAL

10.1 Scope. This appendix contains a sample message, which was constructed using the syntax of the variable message format (VMF) related to MIL-STD-188-220. The VMF is fully defined in the *Variable Message Format, Technical Interface Design Plan* (test edition).

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220.

20. APPLICABLE DOCUMENTS

30. VMF MESSAGE ENCODING. The DMTD will process a message similar to the sample message presented in Figure G-1. The message structure in Figure G-2 will be supported. Messages in this format will contain all mandatory fields, selected optional fields, and repeated fields arranged in the order specified by the applicable message specifications. FPIs and GPIs will be used to indicate the specific optional fields that are selected. FRIs and GRIs will be used to indicate repetition.

30.1 Repeat codes. The repeat codes, shown in Figure G-1, denote group appearance, nesting of groups, and maximum repetitions. The following notations are used:

R = Indicates this field is repeatable.

RN = Indicates this field is part of a group that can be repeated, with *n* specifying the group number (that is, R1 indicates the first repeatable group in the message).

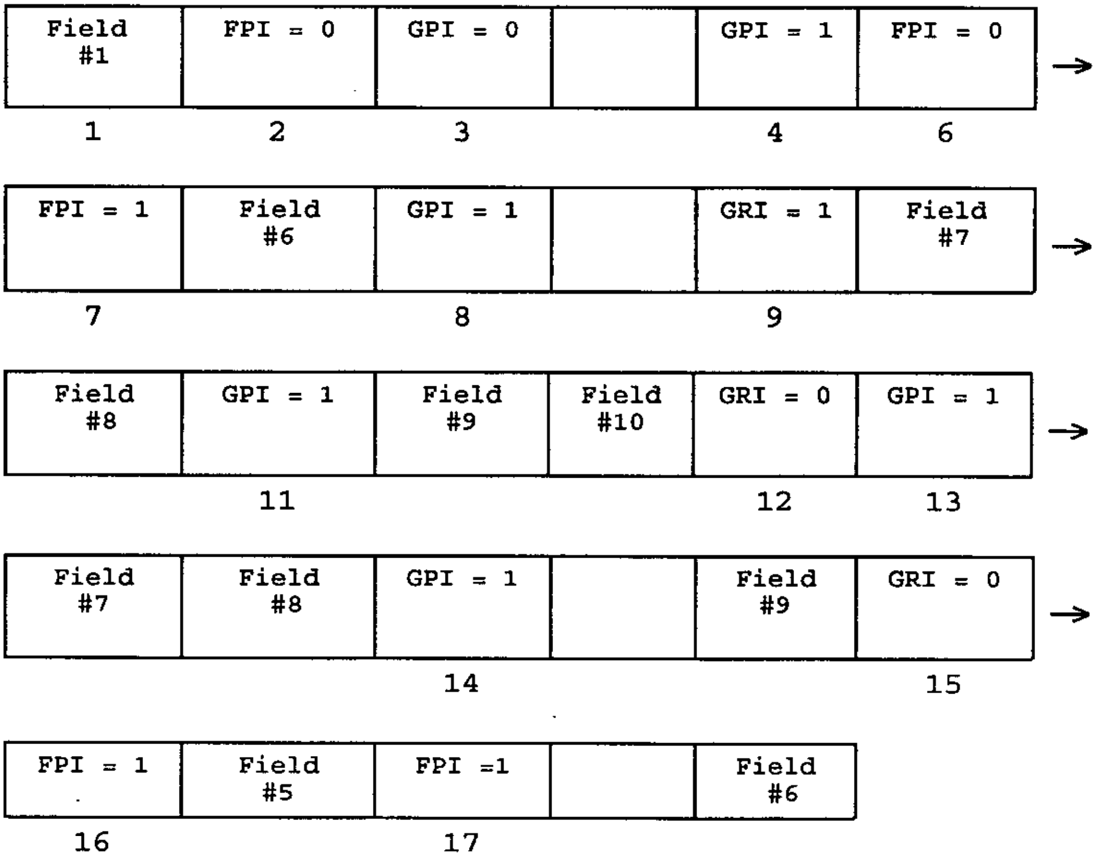
C = Consecutive repeatability indicator specifies that the individual repeatable field or repeatable group of fields may be repeated only in a consecutive manner (for example, fields 3 and 4, followed immediately by fields 3 and 4). Consecutive repeating of a group of fields can occur only when the group is a single group (no nested groups) or the group is the innermost of several nested groups.

I = Iterative repeatability indicator specifies that the repeatable group may be repeated only after consideration has been given to all embedded iterative and consecutive repeatables.

INDEX NUMBER	FIELD INDICATOR	DFI/DUI	DATA FIELD DESCRIPTOR	CATEGORY	GROUP CODE	REPEAT CODE	FIELD LENGTH
1			Field Argument #1	M			1
2	FPI	4014/002					1
2.1			Field Argument #2				1
3	GPI	4014/001	(GPI for G1)				7
3.1			Field Argument #3		G1		4
3.2			Field Argument #4		G1		4
4	GPI	4014/001	(GPI for R1)				1
4.1	GRI	4045/002	(GRI for R1)			R1I(2)	1
4.2	FPI	4014/002				R1	1
4.2.1			Field Argument #5			R1	15
4.3	FPI	4014/002				R1	1
4.3.1			Field Argument #6			R1	1
4.4	GPI	4014/001	(GPI for R2)			R1	1
4.4.1	GRI	4045/001	(GRI for R2)			R1/R2C(3)	1
4.4.2	GPI	4014/001	(GPI for G2)			R1/R2	1
4.4.2.1			Field Argument #7		G2	R1/R2	1
4.4.2.2			Field Argument #8		G2	R1/R2	4
4.4.3	GPI	4014/001	(GPI for G3)			R1/R2	8
4.4.3.1			Field Argument #9		G3	R1/R2	1
4.4.3.2			Field Argument #10		G3	R1/R2	5

FIGURE G-1. Example message summary.

(N) = Appears with the first field of a repeatable group, that is, R3C(3), and indicates the maximum number of appearances of the group in the message. The example, R3C(3), indicates the third repeatable group of the message that will be repeated consecutively and can appear a maximum of three times.



KEY:

FPI = field presence indicator
GPI = group presence indicator
GRI = group recurrence indicator

FIGURE G-2. Example of a message format.

Notes to Figure G-2:

1. Field 1 is a mandatory entry; thus, it is present in every transmission. No FPI is required.

2. Field 2 is omitted; thus, the FPI = 0.

3. Group fields 3 and 4 were omitted; thus, the GPI = 0.

4. One or more fields of the repeatable group R1 are present in this transmission; thus, the GPI = 1.

5. Repeatable group R1 repeats; thus, its GRI = 1.

6. Field 5 is omitted in this iteration; thus, FPI = 0.

7. Field 6 is present; thus, FPI = 1.

8. At least one of the fields within repeatable group R2 is present; thus, the GPI = 1.

9. Repeatable group R2 is repeated; thus, the GRI = 1.

10. The fields within group G2 (fields 7 and 8) are present in this iteration; thus, their GPI = 1.

11. The fields within group G3 (field 9 and 10) are present; thus, GPI = 1.

12. Prior to the appearance of repeatable group R2, the GRI field was set to 1, indicating that it would be repeated (see note 9). Since group R2 is a consecutive recurring group and does not contain any embedded repeatable groups, a repeat of R2 is now appropriate. The first field of repeatable group R2 is the GRI field. In this particular use of the example message, the third permitted appearance of group R2 is not required; thus, the GRI = 0.

13. The fields within group G2 (fields 7 and 8) are present; thus, the GPI = 1.

14. The fields within group G3 (fields 9 and 10) are present; thus, the GPI = 1.

15. With the inclusion of field 10 in the format, repeatable group R2 is completed. Previously, in item 12, it was indicated that group R2 would not be repeated. Since there are no more embedded repeatable groups within group R2 to consider, logic returns to consideration of group R1 to repeat. Item 5 previously indicated R1 would be repeated after its first appearance; therefore, repeatable group R1 is considered. The first field of repeatable group R1 is the GRI field. Since the example message format indicates group R1 can appear only twice in the message, further repeats of R1 are illegal; thus, the GRI = 0.

16. The first field (field 5) of group R1 is present; thus, the FPI = 1.

17. The next field (field 6) of group R1 is present; thus, the FPI = 1.

18. Group field R2 is omitted on this iteration of R1; thus, the GRI = 0. Note that the setting of GPI = 0 for a repeatable group upon its first consideration for appearance deletes that repeatable group from consideration for repeat; thus, the absence of repeatable group R2, in this example, ends the message.

APPENDIX H

DFI/DUI MESSAGE ELEMENT DEFINITIONS

10. GENERAL

10.1 Scope. This appendix provides the message element definitions applicable to MIL-STD-188-220. These definitions have been extracted from the VMF Data Element Dictionary cited in 20.

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS. VMF TIDP (TE) Volume II - Data Element Dictionary

30. DFI/DUI DEFINITIONS. The following DFI/DUI descriptions apply to the message elements specified in this MIL-STD.

	DFI	NAME	DEFINITION
(U)	4014	PRESENCE INDICATOR	INDICATES PRESENCE OR ABSENCE OF THE ASSOCIATED INFORMATION.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** FSSG PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	GROUP PRESENCE INDICATOR [1 BIT] [GPI]	INDICATES PRESENCE OR ABSENCE OF THE ASSOCIATED INFORMATION GROUP FOLLOWING THE GPI.	- K02.2 K02.4 K02.5 K02.7 K02.8 K02.9 K02.11 K02.14 K02.15 K02.16 K02.17 K02.18 K02.19 K02.20 K02.21 K02.22 K02.24
(U)	002	FIELD PRESENCE INDICATOR [1 BIT] [FPI]	INDICATES PRESENCE OR ABSENCE OF THE ASSOCIATED INFORMATION FIELD FOLLOWING THE FPI.	- K02.1 K02.2 K02.4 K02.5 K02.6 K02.7 K02.8 K02.9 K02.10 K02.12 K02.14 K02.15 K02.16 K02.17 K02.18 K02.19 K02.20 K02.21 K02.22 K02.24 K02.25

DATA ITEMS AND CODES

	DATA ITEM	BIT CODE		EXPLANATION
(U)	.....FOR DUI 001-002.....			
(U)	ABSENT	0	[OCTAL]	INFORMATION ASSOCIATED WITH THE INDICATOR IS OMITTED.
(U)	PRESENT	1	[OCTAL]	INFORMATION ASSOCIATED WITH THE INDICATOR IS PRESENT.

	DFI	NAME	DEFINITION
(U)	4019	DAY	A 24-HOUR PERIOD RESERVED FOR A CERTAIN ACTIVITY.

(U) **DATA STANDARD USAGE:** K SERIES VMF

STATUS: FSSG PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	DAY OF MONTH [5 BITS]	ONE OF 24-HOUR PERIODS OF A MONTH AS DEFINED BY THE GREGORIAN CALENDAR.	PROTOCOL HEADER VMF TIDP-TE VOL IV
(U)	002	DAY ON TARGET [5 BITS]	THE DAY AN AIRCRAFT PREPARED TO PERFORM ITS ASSIGNED MISSION SHOULD REACH A SPECIFIC TARGET, OR IMPACT OR HAVE IMPACTED.	- K02.4 K02.14 K02.22
(U)	003	DAY SHELLING BEGAN [5 BIT]	THE DAY OF THE MONTH THAT SHELLING BEGAN.	- K02.5
(U)	004	EFFECTIVE DAY [5 BIT]	THE EFFECTIVE DAY ON AN EVENT.	- K02.9 K02.11 K02.15 K02.23
(U)	005	MET VALIDITY START DAY [5 BIT]	THE FIRST DAY OF A VALID TIME PERIOD.	- K02.3
(U)	006	DEACTIVE DAY [5 BIT]	THE DEACTIVATION DAY OF AN EVENT.	- K02.15
(U)	007	MISSION STOP DAY [5 BIT]	THE MISSION STOP DAY.	- K02.16 K02.17
(U)	008	ACTIVATION DAY [5 BIT]	THE DAY OF THE MONTH THAT A FIRE UNIT IS EXPECTED TO BE OPERATIONAL.	- K02.18
(U)	009	START SEARCH DAY [5 BIT]	INDICATES THAT RECORDS DATED BEFORE THIS DAY ARE NOT TO BE RETRIEVED.	- K02.19

DATA ITEM AND CODES

	DATA ITEM	BIT CODE		EXPLANATION
(U)	.....FOR DUI 001-009.....			
(U)	[ILLEGAL]	0		[OCTAL]
(U)	(NUMERIC)	(1-37)	[OCTAL]	THE SPECIFIC DAY OF THE MONTH

DFI 4019 DAY

	DFI	NAME	DEFINITION
(U)	4035	TIME ZONE DESIGNATOR	THE DIFFERENCE IN HOURS BETWEEN THE ASSOCIATED TIME IN THIS MESSAGE AND GREENWICH MEAN TIME.

(U) DATA STANDARD USAGE: K SERIES VMF

STATUS: FSSG PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	TIME ZONE DESIGNATOR [7 BIT]	THE DIFFERENCE IN HOURS BETWEEN THE ASSOCIATED TIME IN THIS MESSAGE AND GREENWICH MEAN TIME.	- K02.4 K02.5 K02.9 K02.11 K02.14 K02.15 K02.16 K02.17 K02.18 K02.19 K02.22 K02.23

DATA ITEMS AND CODES

	DATA ITEM	BIT CODE		EXPLANATION
(U)	.....FOR DUI 001.....			
(U)	ILLEGAL	(0-100)	[OCTAL]	
(U)	A	101	[OCTAL]	GMT PLUS 1 HOUR.
(U)	B	102	[OCTAL]	GMT PLUS 2 HOURS.
(U)	C	103	[OCTAL]	GMT PLUS 3 HOURS.
(U)	D	104	[OCTAL]	GMT PLUS 4 HOURS.
(U)	E	105	[OCTAL]	GMT PLUS 5 HOURS.
(U)	F	106	[OCTAL]	GMT PLUS 6 HOURS.
(U)	G	107	[OCTAL]	GMT PLUS 7 HOURS.

	DATA ITEM			
(U)	H	110	[OCTAL]	GMT PLUS 8 HOURS.
(U)	I	111	[OCTAL]	GMT PLUS 9 HOURS.
(U)	[ILLEGAL]	112	[OCTAL]	NOT USED.
(U)	K	113	[OCTAL]	GMT PLUS 10 HOURS.
(U)	L	114	[OCTAL]	GMT PLUS 11 HOURS.
(U)	M	115	[OCTAL]	GMT PLUS 12 HOURS.
(U)	N	116	[OCTAL]	GMT MINUS 1 HOUR.
(U)	O	117	[OCTAL]	GMT MINUS 2 HOURS.
(U)	P	120	[OCTAL]	GMT MINUS 3 HOURS.
(U)	Q	121	[OCTAL]	GMT MINUS 4 HOURS.
(U)	R	122	[OCTAL]	GMT MINUS 5 HOURS.
(U)	S	123	[OCTAL]	GMT MINUS 6 HOURS.
(U)	T	124	[OCTAL]	GMT MINUS 7 HOURS.
(U)	U	125	[OCTAL]	GMT MINUS 8 HOURS.
(U)	V	126	[OCTAL]	GMT MINUS 9 HOURS.
(U)	W	127	[OCTAL]	GMT MINUS 10 HOURS.
(U)	X	130	[OCTAL]	GMT MINUS 11 HOURS.
(U)	Y	131	[OCTAL]	GMT MINUS 12 HOURS.

	DATA ITEM			
(U)	Z	132	[OCTAL]	GREENWICH MEAN TIME.
(U)	[ILLEGAL]	(133-177)	[OCTAL]	

THE TIME ZONE CONTAINING THE INTERNATIONAL DATE LINE MAY BE DESIGNATED EITHER BY "M" OR "Y." AN EAST-TO-WEST MOVEMENT ACROSS THE INTERNATIONAL DATE LINE PROJECTS THE TIME RELATIONSHIP INTO THE NEXT OR FOLLOWING DAY. A WEST-TO-EAST MOVEMENT ACROSS THE INTERNATIONAL DATE LINE PROJECTS THE TIME RELATIONSHIP INTO THE PREVIOUS DAY. EACH TIME ZONE IS 15 DEGREES WIDE, EXCEPT WHERE BOUNDARY VARIATIONS HAVE BEEN NECESSARY TO MAINTAIN NATIONAL OR REGIONAL GEOPOLITICAL INTEGRITY. TIME ZONES ARE DEPICTED GRAPHICALLY ON U.S. NAVAL OCEANOGRAPHIC OFFICE CHART NO. 5192, STANDARD TIME ZONE CHART OF THE WORLD.

	DFI	NAME	DEFINITION
(U)	4045	RECURRENCE INDICATOR	

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** FSSG PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	GROUP RECURRENCE INDICATOR [1 BIT] [GRI]	INDICATES THE ASSOCIATED INFORMATION GROUP FOLLOWING THE GRI IS REPEATED.	- K02.3 K02.4 K02.5 K02.6 K02.7 K02.8 K02.9 K02.10 K02.11 K02.14 K02.15 K02.17
(U)	002	FIELD RECURRENCE INDICATOR [1 BIT]	INDICATES THE ASSOCIATED INFORMATION FIELD FOLLOWING THE FRI IS REPEATED.	- K02.2 K02.5 K02.6 K02.10 K02.12 K02.15 K02.18 K02.20 K02.21 K02.25 K02.26

DATA ITEMS AND CODES

	DATA ITEM	BIT CODE		EXPLANATION
(U)	.....FOR DUI 001-002.....			
(U)	NOT REPEATED	0	[OCTAL]	INDICATES THIS IS THE LAST RECURRENCE OF INFORMATION ASSOCIATED WITH THE INDICATOR.
(U)	REPEATED	1	[OCTAL]	INDICATES THAT AT LEAST 1 MORE RECURRENCE OF INFORMATION IS ASSOCIATED WITH THE INDICATOR.

	DFI	NAME	DEFINITION
(U)	4076	CANNOT PROCESS (CANTPRO) REASON CODE	A CODE INDICATING WHY A PARTICULAR MESSAGE CANNOT BE PROCESSED.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** VMF PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	CANTPRO CODE [6 BITS]	A CODE INDICATING WHY A PARTICULAR MESSAGE CANNOT BE PROCESSED.	PROTOCOL HEADER VMF TIDP-TE

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	**.....FOR DUI 001.....**		
(U)	CANTPRO CODE	1	FIELD CONTENT INVALID.
(U)	CANTPRO CODE	2	MESSAGE INCORRECTLY ROUTED.
(U)	CANTPRO CODE	3	ADDRESS INACTIVE.
(U)	CANTPRO CODE	4	REFERENCE POINT UNKNOWN TO RECEIVING AGENCY.
(U)	CANTPRO CODE	5	FIRE UNITS MUST BE CONTROLLED BY RECEIVING AGENCY.
(U)	CANTPRO CODE	6	MISSION MUST BE CONTROLLED BY RECEIVING AGENCY.
(U)	CANTPRO CODE	7	MISSION NUMBER UNKNOWN BY RECEIVING AGENCY.
(U)	CANTPRO CODE	8	TARGET NUMBER UNKNOWN BY RECEIVING AGENCY.
(U)	CANTPRO CODE	9	SCHEDULE NUMBER UNKNOWN BY RECEIVING AGENCY.
(U)	CANTPRO CODE	10	INCORRECT CONTROLLING ADDRESS FOR A GIVEN TRACK NUMBER.
(U)	CANTPRO CODE	11	TRACK NUMBER NOT IN OWN TRACK FILE.
(U)	CANTPRO CODE	12	INVALID ACCORDING TO GIVEN FIELD.
(U)	CANTPRO CODE	13	MESSAGE CANNOT BE CONVERTED.
(U)	CANTPRO CODE	14	AGENCY FILE FULL.

	DATA ITEM		
(U)	CANTPRO CODE	15	AGENCY DOES NOT RECOGNIZE THIS MESSAGE NUMBER.
(U)	CANTPRO CODE	16	AGENCY CANNOT CORRELATE MESSAGE TO CURRENT FILE CONTENT.
(U)	CANTPRO CODE	17	AGENCY LIMIT EXCEEDED ON REPEATED FIELDS OR GROUPS.
(U)	CANTPRO CODE	18	AGENCY COMPUTER SYSTEM INACTIVE.
(U)	CANTPRO CODE	19	ADDRESSEE UNKNOWN.
(U)	CANTPRO CODE	20	CAN'T FORWARD (AGENCY FAILURE).
(U)	CANTPRO CODE	21	CAN'T FORWARD (LINK FAILURE).
(U)	CANTPRO CODE	54	ILLOGICAL JUXTAPOSITION OF HEADER FIELDS.
(U)	SPARE	0, 22-53, 55-63	SPARE CODE(S).

DFI	NAME	DEFINITION	
(U)	4081	FUNCTIONAL AREA DESIGNATOR	PROVIDES THE NUMBERING CONVENTION FOR VARIABLE MESSAGE FORMAT.

(U) DATA STANDARD USAGE: K SERIES VMF

STATUS: FSSG PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	FUNCTIONAL AREA DESIGNATOR [7 BITS]	IDENTIFIES THE FUNCTIONAL AREA OF A SPECIFIC MESSAGE.	PROTOCOL HEADER VMF TIDP-TE VOL IV

DATA ITEMS AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	.....FOR DUI 001.....		
(U)	NETWORK CONTROL	0	
(U)	[UNDEFINED]	1	
(U)	FIRE SUPPORT	2	
(U)	[UNDEFINED]	3	
(U)	[UNDEFINED]	4	
(U)	[UNDEFINED]	5	
(U)	[UNDEFINED]	6	
(U)	[UNDEFINED]	7	

	DFI	NAME	DEFINITION
(U)	4085	NUMBER	AN IDENTIFIER OF AN ENTITY, COMMONLY CONSIDERED TO BE, OR REFERRED TO AS A "NUMBER".

(U) **DATA STANDARD USAGE:** K SERIES VMF

STATUS: FSSG PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	002	BLOCK COUNT DESIGNATOR [3 BITS] [BCD]	PROVIDES MULTI-BLOCK ACCOUNTABILITY IN MESSAGES OF THREE OR MORE BLOCKS. NOT USED FOR MESSAGES OF LESS THAN THREE BLOCKS SINCE BCD ACCOUNTS ONLY FOR THE INTERMEDIATE BLOCKS (THE BLOCKS BETWEEN THE START AND END BLOCKS).	TBD
(U)	003	COUNT DESIGNATOR [3 BITS]	PROVIDES MULTI-BLOCK ACCOUNTABILITY.	USED IN JTIDS ONLY
(U)	004	BLOCK NUMBER NOT ACKNOWLEDGED [3 BITS]	IDENTIFIES BLOCK NOT ACKNOWLEDGED.	
(U)	005	CONTINUATION COUNT DESIGNATOR [3 BITS] [CCD]	PROVIDES MULTI-BLOCK ACCOUNTABILITY.	USED IN JTIDS ONLY.
(U)	006	COUNTER, INITIAL [4 BITS]	PROVIDES INITIAL VALUE OF COUNTER.	TBD
(U)	007	FLOODING REQUEST [7 BITS]	A SERIAL NUMBER ASSIGNED BY A SOURCE.	TBD
(U)	008	FLOODING COUNTER [4 BITS]	NUMBER DESIGNATION, DECREMENTED BY EACH RELAY.	TBD
(U)	009	LAST BLOCK NUMBER ACKNOWLEDGED [3 BITS]	IDENTIFIES THE LAST BLOCK NUMBER ACKNOWLEDGED.	TBD

(U)	010	MESSAGE SEQUENCE NUMBER *[16 BITS]*	MESSAGE IDENTIFICATION NUMBER ASSIGNED BY THE MESSAGE ORIGINATOR.	TBD
(U)	011	MESSAGE TRANSMISSION COUNTER [12 BITS]	SERIAL NUMBER OF THE ORIGINAL TRANSMITTED MESSAGE.	USED IN JTIDS ONLY
(U)	012	MESSAGE RECEPTION COUNTER [12 BITS]	SERIAL NUMBER OF THE RECEIVED ORIGINAL MESSAGE.	USED IN JTIDS ONLY.
(U)	013	NETWORK SELECTION [3 BITS]	IDENTIFIES COMMUNICATIONS NETWORK OVER WHICH MESSAGE WILL BE TRANSMITTED.	TBD.
(U)	014	REFERENCE MESSAGE SEQUENCE NUMBER [16 BITS]	CONTAINS THE MESSAGE SEQUENCE NUMBER OF THE VMF CONNECTION REQUEST CONTROL MESSAGE TO WHICH THE MESSAGE CONTAINING THIS REFERENCE RESPONDS.	TBD.
(U)	015	ROUTE SEGMENT NUMBER [4 BITS]	THE NUMBER OF THE ROUTE SEGMENT OVER WHICH THE DATA PACKET/MESSAGE IS TO BE RELAYED.	TBD.
(U)	016	*WINDOW SIZE* [3 BITS]	*NUMBER OF BLOCKS ALLOWED TO BE OUTSTANDING WITHOUT* ACKNOWLEDGEMENT.	TBD.
(U)	017	MESSAGE FRAME NUMBER [8 BITS] [BCD]	USED TO SEQUENTIALLY NUMBER MESSAGE FRAMES, ALSO USED AS START OF MESSAGE/END OF MESSAGE INDICATOR.	PROTOCOL HEADER VMF TIDP-TE VOL IV.
(U)	018	STATION SERIAL NUMBER [12 BITS] [BCD]	SEQUENTIAL NUMBER INCLUDED IN EACH MESSAGE TRANSMITTED BY AN AGENCY. AN AGENCY SHALL INCREMENT (BY ONE) ITS STATION SERIAL NUMBER EACH TIME A MESSAGE IS TRANSMITTED.	PROTOCOL HEADER VMF TIDP-TE VOL IV.
(U)	019	*MESSAGE NUMBER* [10 BITS]	A NUMBER WHICH IDENTIFIES A SPECIFIC MESSAGE WITHIN A FUNCTIONAL AREA.	PROTOCOL HEADER VMF TIDP-TE VOL 1V.

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	.....FOR DUI 002.....		
(U)	DESIGNATOR	0-7	
(U)	.....FOR DUI 003.....		
(U)	ILLEGAL	0	
(U)	NUMERIC	1-7	
(U)	.....FOR DUI 004.....		
(U)	NUMERIC	1-7	
(U)	.....FOR DUI 005.....		
(U)	DESIGNATOR	1-7	
(U)	.....FOR DUI 006.....		
(U)	COUNTER	1-15	
(U)	.....FOR DUI 007.....		
(U)	NUMERIC	1-99	
(U)	.....FOR DUI 008.....		
(U)	NUMERIC	0-15	
(U)	.....FOR DUI 009.....		
(U)	NUMERIC	0-7	

	DATA ITEM		
(U)	.....FOR DUI 010.....		
(U)	NUMBER	0-65, 535	
(U)	.....FOR DUI 011.....		
(U)	COUNTER	0-4, 095	
(U)	.....FOR DUI 012.....		
(U)	COUNTER	0-4, 095	
(U)	.....FOR DUI 013.....		
(U)	NUMERIC	0-7	
(U)	.....FOR DUI 014.....		
(U)	NUMBER	0-65, 535	
(U)	.....FOR DUI 015.....		
(U)	NUMBER	0-15	
(U)	.....FOR DUI 016.....		
(U)	NUMERIC	0-7	
(U)	.....FOR DUI 017.....		
(U)	NUMERIC	01-40	THE BIT CODE SHALL BE A FOUR BIT BINARY CODED DECIMAL.
(U)	.....FOR DUI 018.....		
(U)	NUMERIC	000-999	THE BIT CODE SHALL BE A FOUR BIT BINARY CODED DECIMAL.

	DATA ITEM	
(U)	.....FOR DUI 019.....	
(U)	NUMERIC	1-999

	DFI	NAME	DEFINITION
(U)	4097	RECEIPT/COMPLIANCE	CONVEYS THE UNIT'S ACKNOWLEDGEMENT AND/OR INTENTIONS.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** VMF PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	RECEIPT/COMPLIANCE [4 BITS]	CONVEYS THE UNIT'S ACKNOWLEDGEMENT AND/OR INTENTIONS.	PROTOCOL HEADER VMF TIDP-TE VOL IV
(U)	002	OPERATOR'S ACKNOWLEDGEMENT/REPLY [4 BITS]	CONVEYS THE OPERATOR'S ACKNOWLEDGEMENT AND INTENTIONS.	PROTOCOL HEADER VMF TIDP-TE VOL IV

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	.....FOR DUI 001.....		
(U)	OPERATOR RESPONSE REQUIRED	0	THE INDICATION IN ORIGINAL MESSAGE THAT AN OPERATOR RESPONSE IS EXPECTED.
(U)	NO REPLY/RESPONSE REQUIRED	1	THE ORIGINATOR IS NOT EXPECTING A REPLY/RESPONSE.
(U)	MACHINE RECEIPT REQUIRED	2	AN INDICATION THAT A MACHINE ACKNOWLEDGEMENT FROM ULTIMATE DESTINATION STATION COMPUTER IS EXPECTED.

	DATA ITEM		
(U)	MACHINE RECEIPT	3	AN INDICATION AUTOMATICALLY GENERATED BY THE ULTIMATE DESTINATION STATION COMPUTER THAT AN ORIGINAL MESSAGE CAN BE SUCCESSFULLY PROCESSED.
(U)	CANNOT PROCESS	4	AN INDICATION AUTOMATICALLY GENERATED BY THE ULTIMATE DESTINATION STATION COMPUTER THAT AN ORIGINAL MESSAGE CANNOT BE SUCCESSFULLY PROCESSED.
(U)	.....FOR DUI 001-002.....		
(U)	OPERATOR ACKNOWLEDGE	5	A POSITIVE ACKNOWLEDGEMENT BY THE OPERATOR OF A MESSAGE AT THE ULTIMATE DESTINATION.
(U)	WILL COMPLY	6	RECEIVED MESSAGE UNDERSTOOD AND WILL COMPLY.
(U)	HAVE COMPLIED	7	RECEIVED MESSAGE UNDERSTOOD AND COMPLIANCE HAS BEEN ACCOMPLISHED.
(U)	CANNOT COMPLY	8	ORIGINATOR OF THIS RESPONSE CANNOT COMPLY WITHIN THIS MESSAGE. THIS IS A MANUALLY GENERATED RESPONSE BY AN OPERATOR WHO HAS RECEIVED THE MESSAGE AND HAS DETERMINED THAT THE MESSAGE CANNOT/WILL NOT BE CARRIED OUT.
(U)	.....FOR DUI 001.....	9-15	SPARE CODE(S)
(U)	.....FOR DUI 002.....	0-4, 9-15	SPARE CODE(S)

	DFI	NAME	DEFINITION
(U)	4098	YEAR	A PERIOD OF EITHER 365 OR 366 DAYS OF A CENTURY AS DEFINED BY THE GREGORIAN CALENDAR.

(U) DATA STANDARD USAGE: K SERIES VMF

STATUS: VMF PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	YEAR [7 BITS]	A PERIOD OF EITHER 365 OR 366 DAYS OF A CENTURY AS DEFINED BY THE GREGORIAN CALENDAR	PROTOCOL HEADER VMF TIDP-TE VOL IV

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	.....FOR DUI 001.....		
(U)	YEAR	0-99	

	DFI	NAME	DEFINITION
(U)	4099	MONTH	ONE OF TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY THE GREGORIAN CALENDAR.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** VMF PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	MONTH [4 BITS]	ONE OF TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY THE GREGORIAN CALENDAR	PROTOCOL HEADER VMF TIDP-TE VOL IV

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	.....FOR DUI 001.....		
(U)	MONTH	1-12	

	DFI	NAME	DEFINITION
(U)	4100	CALL SIGN	ANY COMBINATION OF CHARACTERS OR WORDS WHICH IDENTIFIES ONE OR MORE COMMUNICATIONS FACILITIES, COMMANDS, AUTHORITIES, ACTIVITIES OR UNITS.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** VMF PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)		.....**FOR DUI 001**.....		
(U)		CALL SIGN (FROM) [56 BITS]	THE CALL SIGN OF THE ORIGINATING UNIT.	PROTOCOL HEADER VMF TIDP-TE VOL IV
(U)		.....**FOR DUI 002**.....		
(U)		CALL SIGN (TO) [56 BITS]	THE CALL SIGN OF THE ACTION ADDRESSEE.	PROTOCOL HEADER VMF TIDP-TE VOL IV
(U)		.....**FOR DUI 002**.....		
(U)		CALL SIGN (INFO) [56 BITS]	THE CALL SIGN OF AN INFORMATION ADDRESSEE.	PROTOCOL HEADER VMF TIDP-TE VOL IV

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	CALL SIGN	7 ASCII	INFO BITS/CHARACTER CURRENT CALL SIGN ASSIGNED WILL BE USED AS THE CHARACTER CODE. THE 56 BITS OF THE CALL SIGN ARE MADE UP OF 8 ASCII CHARACTERS.

	DFI	NAME	DEFINITION
(U)	4101	CONTROL AND RELEASE MARKING	THE SPECIAL NOTATIONS (CAVEATS) THAT INDICATE THE SPECIAL HANDLING (ACCESS) AND/OR RELEASABILITY RESTRICTIONS OR REQUIREMENTS THAT HAVE BEEN ASSIGNED TO INFORMATION OR MATERIAL.

(U) **DATA STANDARD USAGE:** K SERIES VMF

STATUS: VMF PROPOSED

DATA USE IDENTIFIER

	DUI	NAME	EXPLANATION	APPLICABILITY
(U)	001	CONTROL AND RELEASE MARKING [14 BITS]	THE SPECIAL NOTATIONS (CAVEATS) THAT INDICATE THE SPECIAL HANDLING (ACCESS) AND/OR RELEASABILITY RESTRICTIONS OR REQUIREMENTS THAT HAVE BEEN ASSIGNED TO INFORMATION OR MATERIAL.	

DATA ITEM AND CODES

	DATA ITEM	BIT CODE	EXPLANATION
(U)	**......FOR DUI 001.....**		
(U)	SPECIAL NOTATION	7	ASCII INFO BITS/CHAR THE COMPLETE LISTING OF DATA ITEMS OF THIS DUI IS CONTAINED IN DEFENSE INTELLIGENCE AGENCY MANUAL 65-19 STANDARD SECURITY MARKINGS (U), AS AMENDED, CONFIDENTIAL. DATA ITEMS ARE CLASSIFIED. THIS IS A TWO CHARACTER GROUP.

	DFI	NAME	DEFINITION
(U)	792	HOUR	EXPRESSES TIME OF DAY OR A PERIOD OF TIME IN HOURS.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** VMF PROPOSED

DATA USE IDENTIFIER

DUI	NAME	EXPLANATION	APPLICABILITY

(U) THE DATA USE IDENTIFIER AND DATA ITEMS AND CODES INFORMATION FOR THIS DFI ARE CLASSIFIED AND CAN BE FOUND IN THE JTIDS TIDP-TE, VOLUME V, REISSUE 2.

	DFI	NAME	DEFINITION
(U)	797	MINUTE	EXPRESSES THE MINUTE OF THE HOUR.

(U) **DATA STANDARD USAGE:** K SERIES VMF **STATUS:** VMF PROPOSED

DATA USE IDENTIFIER

DUI	NAME	EXPLANATION	APPLICABILITY

(U) THE DATA USE IDENTIFIER AND DATA ITEMS AND CODES INFORMATION FOR THIS DFI ARE CLASSIFIED AND CAN BE FOUND IN THE JTIDS TIDP-TE, VOLUME V, REISSUE 2.

APPENDIX I

ROUTING AND RELAY FOR MULTIPLE DESTINATION ADDRESSING

10. GENERAL

10.1 Scope. This appendix contains an example that illustrates routing and relay procedures for multiple destination addressing, as described in 5.4.2.9.1.

10.2 Application. This appendix is not a mandatory part of MIL-STD-188-220. The information contained herein is intended for guidance only.

20. APPLICABLE DOCUMENTS. This section is not applicable to this appendix.

30. SCENARIO. Given the network topology shown in Figure I-1, the procedures for routing information to multiple destination addresses are described below in an example. The interpretation of the address subfields (that is, area, subnet, and system codes) of the ORI and DRI depends on the network configuration chosen by the network authority.

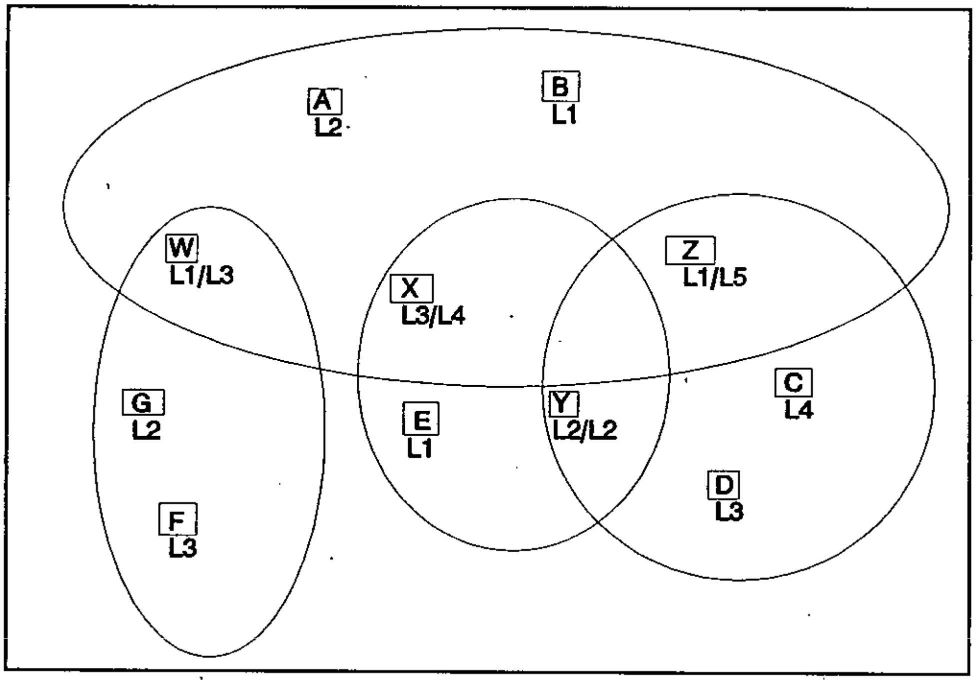


Figure I-1. Example of scenario topology.

30.1 Assumptions. A prerequisite to successful routing and relay capabilities is the apriori connectivity information each node acquires on its nearest neighbors, nearest neighbors + 1, nearest neighbors + 2, and so on. It is assumed that connectivity information can be gained from system initialization data, either manually or automatically. Furthermore, the information on connectivity tables can be updated during operations from network header information. For this example, minimal information is known regarding connectivity.

30.2 Example. In this example, node F will generate a single message and address it to nodes A, B, C, D, E, G, and Z as final destinations. The example will follow the network header through to the final destinations.

30.2.1 Source F (ORI). To transmit information to multiple destinations, the source shall set the L bit of its own ORI (field 8) to 0. It is assumed that source F has connectivity information on nodes A, B, G, and W. Furthermore, it is assumed that source F has no connectivity information on nodes C, D, E, and Z. However, the source assumes that node W (an intermediate) may have connectivity information on nodes C, D, E, and Z. Since F is the originator of information, it must set the D-bit of each address to 0. Source F must also correctly set J-bits to flag the addresses as intermediates or finals. The J-bits of nodes A, B, C, D, E, G, and Z shall be set to 0, and all intermediate addresses (that is, W) shall be set to 1. Figure I-2 represents the ORI of the network header built by node F.

			SOURCE NETWORK ADDRESS																				
L	R	R	X	X	X	X	X	R	R	R	X	X	X	X	X	R	R	R	X	X	X	X	X
0	R	R	SOURCE ADDRESS (F)																				

FIGURE I-2. Example Source F's ORI.

30.2.2 Source F (DRI). In building field 9 (DRI), source F has a direct connection with nodes G and W. System W performs all routing and relaying for F and G. Using this method, it is not necessary for source F to know the exact path to any of the final destinations. All source F is required to know is that W is designated as its routing focal point to those addresses with which it does not have direct connectivity. For this example, it is assumed that source F has some information on nodes A, B, G, and W. Node F knows it can reach all final destinations through W. A worst-case scenario for this example is that source F has no knowledge of connectivity (other than W). This would require an intermediate destination for each final destination. Figure I-3 depicts the DRI of source F's network header. The Y of each destination indicates that source F has direct connectivity with nodes W and G. Therefore, the network header shall be mapped to the link address.

MAP LINK ADDRESS	FINAL OR INTERMEDIATE NETWORK ADDRESS																							
	D	R	J	X	X	X	X	X	R	R	R	X	X	X	X	X	R	R	R	X	X	X	X	X
Y	0	R	0	FINAL DESTINATION (G)																				
Y	0	R	1	INTERMEDIATE DESTINATION (W)																				
	0	R	0	FINAL DESTINATION (A)																				
	0	R	0	FINAL DESTINATION (B)																				
	0	R	1	INTERMEDIATE DESTINATION (W)																				
	0	R	0	FINAL DESTINATION (C)																				
	0	R	1	INTERMEDIATE DESTINATION (W)																				
	0	R	0	FINAL DESTINATION (D)																				
	0	R	1	INTERMEDIATE DESTINATION (W)																				
	0	R	0	FINAL DESTINATION (Z)																				
	0	R	1	INTERMEDIATE DESTINATION (W)																				
	0	R	0	FINAL DESTINATION (E)																				

FIGURE I-3. Example of Source F's DRI.

30.2.3 Node G. On reception of the network header, each node will examine the L bit and determine that the DRI to follow is for multiple destinations and proceed to analyze the destination list for their network address. Since the D-bit is set to 0, all information is new. Node G will read its address and continue to process the message. The entire destination list is analyzed by node G. Since G is not an intermediate address, the remainder of the network header will be discarded.

30.2.4 Node W. Node W will examine the destination list for redundant information and its own address. Subsequently, node W will determine that it is an intermediate address for five final destinations. Node W has direct connectivity with nodes A, B, and Z. Node W also has responsibility for routing information to nodes C, D, and E. A search through its connectivity table reveals that nodes C and D can be reached through node Z and node E through X. Node W will set the D-bit of its own intermediate address to 1, preceding the addresses of final destinations to which it will directly route information. Node W shall map the network addresses to those link addresses with which it has direct connectivity. Node W shall replace its own intermediate address with the network addresses of nodes Z and X for routing information to nodes C, D, and E respectively. Figure I-4 depicts the changes node W makes to the DRI of the network header.

MAP LINK ADDRESS	FINAL OR INTERMEDIATE NETWORK ADDRESS			
	D	R	J	X X X X X R R R X X X X X R R R X X X X X
	0	R	0	FINAL DESTINATION (G)
	1	R	1	INTERMEDIATE DESTINATION (W)
Y	0	R	0	FINAL DESTINATION (A)
Y	0	R	0	FINAL DESTINATION (B)
Y	0	R	1	INTERMEDIATE DESTINATION (Z)
	0	R	0	FINAL DESTINATION (C)
Y	0	R	1	INTERMEDIATE DESTINATION (Z)
	0	R	0	FINAL DESTINATION (D)
Y	1	R	1	INTERMEDIATE DESTINATION (W)
	0	R	0	FINAL DESTINATION (Z)
Y	0	R	1	INTERMEDIATE DESTINATION (X)
	0	R	0	FINAL DESTINATION (E)

FIGURE I-4. Example of Node W's DRI.

30.2.5 Node Z. Node Z will examine the destination list for redundant information and its own address. Subsequently, node Z will determine that it is an intermediate address for two final destinations. Node Z has direct connectivity with nodes C and D. Node Z will set the D-bit of its own intermediate address to 1, preceding the addresses of final destinations to which it will directly route information. Node Z shall map the network addresses to those link addresses with which it has direct connectivity. Node Z is also a final destination and will process the information it received through node W from source F. Figure I-5 depicts the changes node Z makes to the DRI of the network header.

MAP LINK ADDRESS				FINAL OR INTERMEDIATE NETWORK ADDRESS
	D	R	J	X X X X X R R R X X X X X R R R X X X X X
	0	R	0	FINAL DESTINATION (G)
	1	R	1	INTERMEDIATE DESTINATION (W)
	0	R	0	FINAL DESTINATION (A)
	0	R	0	FINAL DESTINATION (B)
	1	R	1	INTERMEDIATE DESTINATION (Z)
Y	0	R	0	FINAL DESTINATION (C)
	1	R	1	INTERMEDIATE DESTINATION (Z)
Y	0	R	0	FINAL DESTINATION (D)
	1	R	1	INTERMEDIATE DESTINATION (W)
	0	R	0	FINAL DESTINATION (Z)
	0	R	1	INTERMEDIATE DESTINATION (X)
	0	R	0	FINAL DESTINATION (E)

FIGURE I-5. Example of Node Z's DRI.

30.2.6 Node X. Node X will examine the destination list for redundant information and its own address. Subsequently, node X will determine that it is an intermediate address for one final destination. Node X has direct connectivity with node E. Node X will set the D-bit of its own intermediate address to 1, preceding the addresses of final destinations to which it will directly route information. Node X shall map the network address to the link addresses with which it has direct connectivity. Figure I-6 depicts the changes node X makes to the DRI of the network header.

MAP LINK ADDRESS	FINAL OR INTERMEDIATE NETWORK ADDRESS			
	D	R	J	X X X X X R R R X X X X X R R R X X X X X
	0	R	0	FINAL DESTINATION (G)
	1	R	1	INTERMEDIATE DESTINATION (W)
	0	R	0	FINAL DESTINATION (A)
	0	R	0	FINAL DESTINATION (B)
	0	R	1	INTERMEDIATE DESTINATION (Z)
	0	R	0	FINAL DESTINATION (C)
	0	R	1	INTERMEDIATE DESTINATION (Z)
	0	R	0	FINAL DESTINATION (D)
	1	R	1	INTERMEDIATE DESTINATION (W)
	0	R	0	FINAL DESTINATION (Z)
	1	R	1	INTERMEDIATE DESTINATION (X)
Y	0	R	0	FINAL DESTINATION (E)

FIGURE I-6. Example of Node X's DRI.

CONCLUDING MATERIAL

Custodians:

Army - CR
Navy - EC
Air Force - 90

Preparing Activity:

DISA - DC

Review activities:

Army - AM, SC, PT
Navy - MC, NC, TD
Air Force - 02, 13, 17, 19,
29, 89, 90, 93
DLA - DH
NSA - NS
ECAC - --
DMA - MP
DOT - OST
DIA - DIA

Agent:

N/A

(Project TCSS - 2200)

User Activities:

Army - AC, MI
Navy - OM
Air Force - 11, 18

International Interest:

NATO

(This page intentionally left blank.)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.

2. The submitter of this form must complete blocks 4, 5, 6, and 7.

3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to requrest waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER: MIL-STD-188-220	2. DOCUMENT DATE (YYMMDD) 93-05-07

3. DOCUMENT TITLE: **Interoperability Standard for Digital Message Transfer Device Subsystems**

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME *(Last, First, Middle Initial)*

b. ORGANIZATION

c. ADDRESS *(Include Zip Code)*

d. TELEPHONE *(Include Area Code)*
(1) Commercial
(2) AUTOVON
(If applicable)

7. DATE SUBMITTED (YYMMDD)

8. PREPARING ACTIVITY

a. NAME:
Director, Joint Interoperability
and Engineering Organization

b. TELEPHONE *(Include Area Code)*
(1) Commercial (908) 532-7715 (2) AUTOVON: 992-7715

c. ADDRESS *(Include Zip Code)*
ATTN: TBBC
Ft. Monmouth, NJ 07703-5613

IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:
Defense Quality and Standardization Office
5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466
Telephone (703) 756-2340 AUTOVON 289-2340

DD Form 1426, OCT.89 Previous editions are obsolete. 108-290