NOT MEASUREMENT SENSITIVE

MIL-STD-2045-47001E
1 February 2021
SUPERSEDING
MIL-STD-2045-47001D
w/CHANGE 1
23 June 2008

DEPARTMENT OF DEFENSE INTERFACE STANDARD

CONNECTIONLESS DATA TRANSFER APPLICATION LAYER STANDARD

AMSC N/A **AREA DCPS**

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

FOREWORD

This Military Standard (MIL-STD) is approved for use by all Departments and Agencies of the Department of Defense (DoD).

This MIL-STD is produced by the Combat Net Radio Working Group (CNRWG) under the auspices of the Radio Information Transfer Technical Working Group (RITTWG). The MIL-STD-2045 document series was established within the Data Communication Protocol Standards (DCPS) Standardization Area to allow for the enhancement of commercial standards or the development of standards that are unique to DoD.

Specific details and instructions for establishing a MIL-STD-2045 document, as well as profile development guidelines, are documented in the RITTWG Management Plan. RITTWG Working Groups (WGs) are responsible for standard development, formal service and agency coordination, and approval.

This MIL-STD does not supersede the scope of Allied Communication Publication (ACP) 123 with US SUPP-1. ACP 123 with US SUPP-1 addresses message handling communications protocol and procedures for the exchange of military messages.

The Preparing Activity (PA) and the primary Point of Contact (POC) for this standard is Headquarters, U.S. Army Communications-Electronics Command (CECOM), Life Cycle Management Command (LCMC), Software Engineering Center (SEC), ATTN: AMSEL-SEC-SAB (Chairman, CNRWG), 6002 Combat Drive, Aberdeen Proving Ground, MD 21005. The custodians for the document are identified in the Defense Standardization Program, "Standardization Directory (SD1)" under Standardization Area DCPS.

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this MIL-STD should be addressed to the POC at the above address by letter.

Comments, suggestions, or questions on this document should be addressed to Headquarters, U.S. Army Communications-Electronics Command (CECOM), Life Cycle Management Command (LCMC), Software Engineering Center (SEC), ATTN: ASEL-SEC-SAB (Chairman, CNRWG), 6002 Combat Drive, Aberdeen Proving Ground, MD 21005. Since contact information can change, you may want to verify the currency of this address information using the ASSIST Online database at https://assist.dla.mil/.

Notice: This version of MIL-STD-2045-47001 is to establish a new and manageable baseline from which to work. The following issues have been identified after initial submittal for publishing of MIL-STD-2045-47001E:

- MIL-STD-2045-47001E Control/Release Marking Data Field Indicator (DFI)/Data Unit Identifier (DUI) (6002/005) data elements are not consistent with MIL-STD-6017E DFI/DUI 4127/005 Nationality field.
- The current maximum iterations of Control/Release Marking field is 16. In view of the number of allies and partners (Northern Atlantic Treaty Organization (NATO) – 29 countries and Partners for Peace (PfP) – 20 countries) being able to list only 16 individual nations may be insufficient.
- User Data Message Version Field. In the case of Link 16 and VMF, the latest version of: MIL-STD-6016 is G and MIL-STD-6017 will soon be E. Many of the versions of the standards listed are no longer in use, i.e., MIL-STD-6016, 6016A, 6016B or Variable Message Format (VMF) Technical

Interface Design Plan (TIDP) - Test Edition (TE) Revision (R) R2, R3, R4 or MIL-STD-6040 Baseline 1993, 1995, 1997.

- Authentication and Encryption. The MIL-STD-2045-47001 built-in authentication and encryption capabilities require updating. The only authentication used in MIL-STD-2045-47001E, Group G20 is Secure Hash Algorithm (SHA) - 1. National Institute of Standards and Technology (NIST) formally deprecated use of SHA-1 in 2011 and disallowed its use for digital signatures in 2013.
- A requirement does not currently exist within MIL-STD-47001E Application Header Case 2 Receipt/Compliance response requirements section to always set the GPI for G20 User Data Message Security Group to 0 (NOT PRESENT). Implementers should note that G20 is not required for any Receipt/Compliance response (including CANTPRO) and therefore the GPI for G20 should always be set to 0 (NOT PRESENT) when a Case 2 response is generated.
- A Field was agreed for inclusion in MIL-STD-2045-47001E to facilitate the use of message versions in order to foster and promote backwards compatibility. However, during the rewrite effort that resulted in MIL-STD-2045-47001E, the emphasis on use for only VMF and MTF messages was lost and the field was incorrectly renamed to "USER DATA MESSAGE VERSION Field" (with the emphasis on the version of the User Data Message) rather than “USER DATA MESSAGE MESSAGE VERSION Field” (emphasis on the Message Version used within the User Data Message).
- Requirements in MIL-STD-2045-47001E convey that only a single received ALPDU will be used as the User Data when the UDMF Field is set to value 4 (REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT). However, rules in the Section for concatenating ALPDUs are contradictory.
- MIL-STD-2045-47001 B through D Ch1 had use of the FILE NAME Field specifically tied to processing when a binary file was in the User Data portion of an Application Layer Protocol Data Unit. However, this emphasis was lost during the re-write to MIL-STD-2045-47001E.
- The USER DATA MESSAGE SIZE Field is incapable of reflecting the maximum possible size of the User Data in a Redistributed ALPDU. The reason for this is that an Original ALPDU, which may have a maximum of 16 UDMs, is used as the Redistributed ALPDU User Data. Each UDM within the Original ALPDU may have a maximum size of 1,048,575 bytes giving a maximum Redistributed ALPDU User Data portion size of 16,777,200 bytes. The highest value that can currently be expressed by the USER DATA MESSAGE SIZE Field using the 20 allocated bits is 1,048,575 bytes.
- It is not made clear in MIL-STD-2045-47001E that the FPIs for all Unused FUGs should be set to 0 (Not PRESENT) to prevent uncontrolled use. Requirements to this effect existed in previous versions of the standard but were lost during the rewrite to MIL-STD-2045-47001E. An ICP is being raised to clarify use in a future version of the standard but implementers should not use unspecified FUGs. The use of FUGs is solely controlled and specified in MIL-STD-2045-47001.
- There are requirements in MIL-STD-2045-47001E that logically demand that various USER DATA MESSAGE HANDLING Group (R3) values are common. These are the OPERATION INDICATOR, USER DATA MESSAGE SECURITY CLASSIFICATION and CONTROL/RELEASE MARKING Fields. However, it is considered that the same commonality demand should be extended to the USER DATA MESSAGE PRECEDENCE Field. When concatenating User Data Messages, Implementers should ensure that the USER DATA MESSAGE PRECEDENCE Field values are common.
- There is a requirement in MIL-STD-2045-47001E that only those entities who are identified by inclusion in the RECIPIENT ADDRESS Group (G2) can generate a Receipt/Compliance response. It is however sensible that the only entities discretely identified, and not those that form part of a

multicast address, in the RECIPIENT ADDRESS Group (G2) should respond to an R/C request. Implementers should ensure that when an Acknowledgement is required from a unit, the unit is discretely addressed in G2.

- The direction in MIL-STD-2045-47001E as to what action to take on receipt of an R/C response (including a CANTPRO) is incomplete. There are a considerable number of rules with respect to an R/C receipt check, and what is processed and what is discarded but direction as to what action to take beyond the "process/discard" point is lacking. At a minimum, the operator should be advised that an R/C response has been received.
- There are known issues in MIL-STD-2045-47001E relating to CANTPRO processing relating to how a recipient that is part of a Multicast group or a Broadcast group responds with a CANTPRO. The MIL-STD currently specifies that the Multicast group/Broadcast group address is used as the Originator address for the CANTPRO R/C response. This is flawed as precise meaning cannot be ascribed to the response. An ICP will be raised to clarify the processing in a future version of the standard.
- Some of the optional CANTPRO REASON values in MIL-STD-2045-47001E require clarification and additional processing on reception needs amplification.

SUMMARY OF MODIFICATIONS

This document constitutes a complete re-write of MIL-STD-2045-47001. This includes format changes and restructuring of the original content, as well as the board approved ICPs listed below:

Date of Revision	**ICP Number**	**ICP Title**
11 December 2009	PA08-006R2	MIL-STD-2045-47001E Request for Exception Paragraphs
11 December 2009	PA08-008	Editorial Correction to MIL-STD-2045-47001 Case 9
11 December 2009	PA08-009R3	General Editorial Corrections to MIL-STD-2045-47001
29 April 2010	PA08-010R6	MIL-STD-2045-47001D Change 1, Table V Updates
29 April 2010	PA09-003R3	Clarification of MIL-STD-2045-47001 Header and Message Size Fields CANTPRO Processing; and Modifications to Cases 3, 4 and the Addition of a New Condition
29 April 2010	PA09-004R1	Amplify Reference to MIL-STD-188-220 Parameter Tables in MIL-STD-2045-47001
10 September 2010	PA09-002R4	Clarification of MIL-STD-2045-47001 Undefined, Illegal, and Disused Data Item Processing
17 November 2010	PA10-001R4	Segmentation/Reassembly Clarifications
17 November 2010	PA10-002R2	Receipt/Compliance Response Clarifications
17 November 2010	PA10-005R1	Non-Government Document Usage in MIL-STD-2045-47001
17 August 2011	PA10-007R5	Additional CANTPRO Reason Codes
08 June 2012	PA11-002R4	DSPICS Indices Corrections For Future Use Groups 6 Through 10
10 December 2012	PA12-004R1	S/R Example Correction
18 September 2013	PA12-001R8	VMF and USMTF Message Versioning
18 September 2013	PA13-001R6	Enhanced Segmentation/Reassembly
5 December 2013	PA13-006R2	Future Use Group Clarification
5 December 2013	PA13-013	MIL-STD-2045-47001E and DSPICS Corrections
23 August 2014	PA12-002R11	Numerous Editorial Corrections
02 November 2017	PA16-001R3	Proposed Modifications to MIL-STD-2045-47001D Ch1 Main Body
30 November 2017	PA16-002R3	Proposed Modifications to MIL-STD-2045-47001D Ch1 Appendix A, Segmentation/Reassembly Protocol
15 October 2017	PA16-003R3	Proposed Modifications to MIL-STD-2045-47001D Ch1 Appendix B, Data Element Dictionary
08 February 2018	PA18-001R1	Comment Resolution Matrix against Draft MS-2045-47001E

Contents

TABLE PAGE

FIGURE PAGE

PARAGRAPH PAGE

1 SCOPE

1.1 Purpose.

1.1.1 The purpose of MIL-STD-2045-47001 is to present the minimum essential technical parameters in the form of mandatory requirements and optional capabilities for interoperability and compatibility among digital message transfer devices (DMTDs), between DMTDs and applicable command, control, communications, computers, and intelligence (C4I) systems and among C4I systems using digital data for information transfer over limited bandwidth communication channels.

1.2 Scope.

1.2.1 This Military Standard (MIL-STD) addresses part of the communications protocol and procedures for the exchange of digital data among DMTDs, between DMTDs and C4I systems, and among C4I systems participating in inter- and intra-Service tactical networks. The material is presented in the context of ISO 7498-1 Open Systems Interconnection (OSI), as documented in national and international standards.

1.3 Application Guidance.

1.3.1 This MIL-STD applies to the design, construction, and development of new equipment and systems, and to the retrofit of existing equipment and systems.

1.3.2 Only approved versions of this MIL-STD may be implemented. Interface Change Proposals (ICPs) against a current version of this MIL-STD cannot be implemented before a new version of this standard is released. Refer to the Combat Net Radio Working Group (CNRWG) Management Plan for guidance.

1.4 Exceptions to Minimum Requirements.

1.4.1 There are minimum number of essential technical parameters that must be implemented by systems/platforms utilizing this standard to ensure interoperability and compatibility. These minimum requirements are identified in paragraph 5.4 and must be complied with to ensure the exchange of information on combat net radio networks.

1.4.2 Exceptions to the minimum requirements identified in this standard must be submitted by the Service/Agency having control of the system/platform in question to the CNRWG. The Request for Exception (RFE) must be specific as to the exact degree of the exception requested. The RFE will identify the specific systems/platforms, the item or items for which the exception is requested, the rationale for requesting the exception and any other information required by the CNRWG.

1.4.3 RFEs will be submitted and processed in accordance with CNRWG Management Plan. The CNRWG will review, evaluate, and approve or deny each RFE on a case-by-case basis. The requesting Service/Agency may elevate the issue to the Radio Information Transfer Technical Working Group (RITTWG) Interoperability Panel (IP) if they have a substantive disagreement on an RFE.

2 APPLICABLE DOCUMENTS

2.1 General.

2.1.1 The documents listed in this section are referenced in sections 3, 4, and 5 of this standard. This section does not include documents cited in other sections of this standard or recommended for additional information as examples. While every effort has been made to ensure the completeness of this list, document users are cautioned that they will meet all specified requirements documents cited in sections 3, 4, and 5 of this standard, whether or not they are listed.

2.2 Government Documents.

2.2.1 Specifications, Standards, and Handbooks.

2.2.1.1 The following specifications, standards, and handbooks form a part of this MIL-STD to the extent specified herein.

2.2.1.2 Unless otherwise indicated, copies of federal and military standards are available from the Standardization Document Order Desk, 700 Robbins Avenue, Building 4D, Philadelphia, PA 19111-5094. Department of Defense Standards documents are available at the ASSIST website: https://assist.dla.mil/. MIL-STD-6016, MIL-STD-6017, MIL-STD-6040 can be obtained from Director, Defense Information System Agency (DISA), Business Development Center, Innovation (DBC), Systems Engineering, and Architecture Office (BDE), Tactical Data Link Standards Branch (BDE3), PO Box 549, Fort Meade, MD 20755-0549.

2.2.1.3 Referenced Standards:

2.2.1.3.1 Federal:

FED-STD-1037	Glossary of Telecommunication Terms

2.2.1.3.2 Military:

MIL-STD-188-220	DoD Interface Standard, Digital Message Transfer Device Subsystems
MIL-STD-2500	National Imagery Transmission Format (NITF) Version 2.1 for the National Imagery Transmission Format Standard (NITFS)
MIL-STD-6016	DoD Interface Standard, Tactical Data Link (TDL) 16 Message Standard
MIL-STD-6017	DoD Interface Standard, Variable Message Format (VMF) MIL-STD-6017
MIL-STD-6040	DoD Interface Standard U.S. Message Text Formatting Program Description of U.S. Message Text Formatting Program (USMTF) https://assist.dla.mil/

2.2.1.3.3 Federal Information Processing Standard:

FIPS 180-4	Secure Hash Standard (SHS) https://doi.org/10.6028/NIST.FIPS.180-4
FIPS 186-4	Digital Signature Standard (DSS) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

2.2.1.3.4 Joint Publications:

Joint Pub (JP) 1	DoD Dictionary http://www.jcs.mil/Doctrine/DOD-Terminology/

2.2.2 Other Government Documents, Drawings, and Publications.

2.2.2.1 None.

2.2.3 North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAG) Documents, Drawings, and Publications.

2.2.3.1 The following NATO STANAG documents, drawings, and publications form a part of this MIL-STD to the extent specified herein. Unless otherwise specified, the versions are those cited in the solicitation.

STANAG 4545	NATO Secondary Imagery Format (NSIF) https://assist.dla.mil/
NATO AEDP-4	NATO Allied Engineering Documentation Publication https://nso.nato.int/nso/zPublic/ap/aedp-4(2).pdf

2.3 Non-Government Publications.

2.3.1 General.

2.3.1.1 The following documents form a part of this MIL-STD to the extent specified herein. Unless otherwise specified, the versions of the documents that are DoD-adopted are those listed in the issue of the Department of Defense Index of Specifications and Standards (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.

2.3.1.2 Unless otherwise stated, only the specific version of any non-government documents (Request for Comments(RFC), International Organization for Standardization (ISO), International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers (IEEE) Standard, etc.) referenced in this MIL-STD must be used. Later versions of a referenced document or any other documents that may have superseded the listed document must not be used.

2.3.2 International Organization For Standardization (ISO).

ISO 7498-1	Information Processing Systems -- Open Systems Interconnection -- Basic Reference Model. American National Standards Institute (ANSI), Inc., 25 W 43rd St. 4th Fl., New York, NY 10018

2.3.3 Other.

RFC 1951	"DEFLATE Compressed Data Format Specification version 1.3", L. Peter Deutsch, May 1996. https://tools.ietf.org/html/rfc1951
RFC 1952	"GZIP file format specification, version 4.3", L. Peter Deutsch, May 1996

https://tools.ietf.org/html/rfc1952

2.4 Order of Precedence.

2.4.1 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.

3.1.1 This section defines the terms and definitions used in this MIL-STD. Additional definitions of terms found in this document can be located in FED-STD-1037, Glossary of Telecommunication Terms.

Acknowledge	The act of notifying a unit transmitting data that the data has been received as valid data.
Addressee	An entity identified in either the RECIPIENT ADDRESSEE Group or the INFORMATION ADDRESSEE Group of an Application Header.
Are	"Are" is used to introduce background information provided to enhance understanding of requirements. "Are" is not a directive.
Binary File	A sequence of Bits (0 or 1).
Bit	A binary digit. In the binary system of numbering, each digit can only have one of two values (0 or 1). (Derived from ACP 167E)
Can	The word "can" in the text expresses a permissible practice or action, not a mandatory requirement.
CANTPRO	A response generated to indicate that a User Data Message (UDM) cannot be successfully processed at the ultimate destination.
Compatibility	The capability of two or more items or components of equipment or materiel to exist or function in the same system or environment without mutual interference. (Joint Pub 1-02)
Conditional	A field which may be used, but which is not designated as a mandatory field. A conditional field will be preceded by an FPI or in a group preceded by a GPI.
Data Element	A basic unit (class) of information having a unique meaning and subcategories (data items) of distinct units or values. Examples of data elements are military personnel grade, sex, race, geographic location, and military unit. (Joint Pub 1-02) The Variable Message Format (VMF) data element is the Data Use Identifier (DUI).

Data Field Identifier (DFI)	A category of data whose specification includes one or more Data Use Identifier (DUI) specifications. Each DUI's class of data must fall within the bounds of the DFI category.
Data Item (DI)	A subunit of descriptive information or value classified under a data element. For example, the data element "military personnel grade" contains data items such as Sergeant, Captain, and Colonel.
Data Item (DI), Disused	A Data Item (DI) value that was previously named but is no longer valid. A Disused value cannot be renamed without determining if coordinated implementation is required.
Data Item (DI), Illegal	A term used to describe a bit code that is not a permissible entry into the tactical data system(s) supporting interface. (For example, a 9-bit DUI called HEADING that has legal values of 0-359 that represents degrees has illegal values of 360-511.)
Data Item (DI), No Statement	A data item to describe no information on this DUI is being transmitted. (This does not necessarily indicate that the Originator does not have the information.) If the Originator of the Application Layer Protocol Data Unit (ALPDU) has actual data but chooses not to transmit the data, then they may select the NO STATEMENT data item, when available. The data item is an explicit transmission value to designate the absence of process-able information by the receiver.
Data Item (DI), Reserved	A DI that is intended for future use.
Data Item (DI), To Be Determined	This indicates that the DI design is incomplete. (DI names and bit codes will be specified at a later time.)
Data Item (DI), Undefined	A term used to describe a DI that has no currently assigned value but may have a value assigned in the future. (This occurs in logically coded items (DUIs) in which all the DIs in the DUI do not have assigned values.)
Data Item (DI), Unknown	A DI that indicates that other values available for this DUI have not been determined by the Originator.

Data Link	The means of connecting one location to another for the purpose of transmitting and receiving data. (Joint Pub 1-02)
Data Use Identifier (DUI)	A data element (class of data). The DUI specification determines the name and permitted contents of each Application Header field to which the DUI is assigned, as explained below. A DFI specification includes a specification for each DUI under that DFI. Each DUI specification identifies the DUI name, and the data items and associated bit codes employed by the DUI. When a DUI is designated as the contents of a VMF message field, the DUI name is the field name, and the data items employed by the DUI are (subject to any implementation or VMF message restrictions) the data items which may be conveyed in that field.
Default Condition	The state automatically assumed by a terminal's hardware or software in the absence of an input directing otherwise.
Digital Message Transfer Device (DMTD)	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, relay and broadcast transfer of information over data communications links. (MIL-STD-188-220)
Directive	(1) A military communication in which policy is established or a specific action is ordered. (Joint Pub 1-02) (2) A plan issued with a view to putting it in effect when so directed, or in the event that a stated contingency arises. (Joint Pub 1-02) (3) Broadly speaking, any communication that initiates or governs action, conduct, or procedure. (Joint Pub 1-02)
Field Presence Indicator (FPI)	A one bit field used to indicate the presence or absence of the following field.
Field Recurrence Indicator (FRI)	A one bit field used to indicate the repeatability of a field.
Field Value	A decimal number assigned to an Application Header Field that represents a Data Item as specified by the Data Element Dictionary.

Future Use Group (FUG)	Future Use Groups take into consideration future Application Header expansion while retaining backward compatibility between MIL-STD-2045-47001 versions from D onwards. New fields will be added to the Application Header only within the FUGs; this will preserve the basic structure of the Application Header thus facilitating backward compatibility.
Future Use Group Sub Group	FUG Sub Groups are groups within a FUG.
Group Presence Indicator (GPI)	A one bit field used to indicate the presence or absence of the following group.
Group Recurrence Indicator (GRI)	A one bit field used to indicate the repeatability of a group.
Information Addressee	An entity identified in the INFORMATION ADDRESSEE Group of an Application Header. An Information Addressee does not respond to the Originator of an ALPDU.
Interoperability	(1) The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together. (Joint Pub 1-02) (2) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (Joint Pub 1-02) (3) The ability to exchange data in a prescribed manner and the processing of such data to extract intelligible information which can be used to control/coordinate operations.
Is	"Is" is used to introduce background information provided to enhance understanding of requirements. "Is" is not a directive.
Joint	Connotes activities, operations, organization, etc., in which elements of more than one Service of the same nation participate. (Joint Pub 1-02)

Link 16	A secure, jam-resistant, node-less data link which utilizes the Joint Tactical Information Distribution System or Multifunctional Information Distribution System, and the protocols, conventions and fixed word message formats defined by the MIL-STD-6016.
Mandatory	Identifies a field which must be present on each transmission and must be processed as received. Mandatory fields are not discarded. Mandatory fields are marked with an "M" in TABLE I. "M" is also used to indicate a mandatory capability in tables listing Cases, Conditions, Expected Responses and Special Considerations.
May	The word "may" in the text expresses a permissible practice or action, not a mandatory requirement.
Message	Any thought or idea expressed briefly in a plain, coded, or secret language, prepared in a form suitable for transmission by any means of communications. (Joint Pub 1-02)
Message Standard	A set of protocols consisting of rules, procedures, formats, data element definitions, or other conventions for information exchange and related interactions agreed upon between cooperating systems to ensure interoperability.
Minimum Implementation	Any MIL-STD-2045-47001 Field, Case, Condition, Expected Response and Special Consideration that is required to be implemented by all systems.
Multicast	Multicast is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split.
Must	The word "must" in the text is used in legislative or regulatory requirements with which both the customer and the vendor shall comply.
Nested Group	Any group within a group.
Network	In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

NITFS	The National Imagery Transmission Format Standard (NITFS) is a U.S. Department of Defense (DoD) and Federal Intelligence Community suite of standards for the exchange, storage, and transmission of digital-imagery products and image-related products.
Operator	"Operator" is a user or person entering and receiving tactical information within a Tactical Data System (TDS), as appropriate to the capability to which a particular requirement applies. No attempt is made to specify the operator position or title expected to carry out specified actions or use specified capabilities, because these vary among systems and platforms.
Optional	Identifies a capability which is optional for implementation. "O" is used to indicate an optional capability in tables listing Cases, Expected Responses and Special Considerations.
Originator	The sender of the ALPDU. This includes the sender of a retransmitted UDM within an ALPDU.
Receipt/Compliance	The acknowledgment of a UDM and/or an indication of intent to respond to a UDM, either by Machine Acknowledgment or Operator Response.
Recipient	An entity identified in the RECIPIENT ADDRESS Field of an ALPDU.
Shall	"Shall" is directive, indicating a mandatory capability or requirement that must be implemented, and that is subject to testing.
Should	The word "should" in the text expresses a recommendation or advice on implementing such a requirement, not a mandatory requirement.
Streaming/Undelimited	Streaming/undelimited as used in this document defines a service provided by a transport layer (e.g., Transmission Control Protocol) that does not have an end-of –packet indication, but instead it provides a stream of data bytes. When using streaming/undelimited transport layer it is for the application to define the end of the packet by breaking the transport connection on each packet or by specifying the end-of-packet in the application data (e.g., MIL-STD-2045-47001).

Subnetwork	A subnetwork is a separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.
Tactical Data Link (TDL)	A Joint Chiefs of Staff (JCS) approved standardized communications link suitable for transmission of digital information. A TDL is characterized by its standardized message formats and transmission characteristics.
Technical Interface Design Plan (TIDP)	An engineering implementation plan that specifies the technical standards required to achieve compatibility and interoperability. The plan includes a comprehensive technical description of the operational interface, message implementation, methods, and rules for processing data between operational facilities and a final list of effective Service/Agency facilities/systems.
User	A User is a person entering and receiving tactical information within a Tactical Data System (TDS), as appropriate to the capability to which a particular requirement applies.
User Data	This portion of the Application Layer Protocol Data Unit (ALPDU) will contain the application process messages or data. The User Data is individually encoded and zero padded before it is passed to the Application Layer to have the Application Header added. User Data passed to the Application Layer should be a multiple of 8 bits.
USMTF	United States Message Text Format (USMTF) is a MIL-STD collection of information exchanges.
VMF	Variable Message Format (VMF) is a bit oriented digital information standard consisting of variable length messages suitable for near real time data exchange in a bandwidth constrained combat environment.
VML	Variable Message Format Markup Language. An XML compliant representation of a given VMF message format.
Will	"Will" is used to introduce background information provided to enhance understanding of requirements. "Will" is not a directive.
XML-MTF	An eXtensible Markup Language (XML) compliant representation of a given MTF message format.

3.2 Abbreviations and Acronyms.

3.2.1 Abbreviations and acronyms used in this MIL-STD are defined below. In addition, those listed in the current edition of FED-STD-1037 that are pertinent to standards referenced by this document have been included for the convenience of the reader.

ACP	Allied Communication Publication
AEDP	Allied Engineering Documentation Publication
ALP	Application Layer Protocol
ALPDU	Application Layer Protocol Data Unit
ASCII	American Standard Code for Information Interchange
C	Conditional
C4I	Command, Control, Communications, Computers, and Intelligence
CANTCO	Cannot Comply
CANTPRO	Cannot Process
CAT	Category
CECOM	Communications-Electronics Command
CNR	Combat Network Radio
CNRWG	Combat Net Radio Working Group
DARPA	Defense Advanced Research Projects Agency
DCPS	Data Communication Protocol Standards
DED	Data Element Dictionary
DFI	Data Field Identifier
DI	Data Item
DISA	Defense Information Systems Agency
DMTD	Digital Message Transfer Device
DoD	Department of Defense
DoDISS	Department of Defense Index of Specifications and Standards
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DSSCS	Defense Special Security Communications System
DTG	Date-Time Group
DUI	Data Use Identifier
EOLF	End Of Literal Field Marker
EXI	Efficient XML Interchange
FAD	Functional Area Designator
FED-STD	Federal Standard
FIPS	Federal Information Processing Standard
FPI	Field Presence Indicator
FRI	Field Recurrence Indicator
GPI	Group Presence Indicator
GRI	Group Recurrence Indicator
HLEN	Header Length
HAVCO	Have Complied
ICP	Interface Change Proposal
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
IPHS	Internet Protocol Header Size
ISO	International Organization for Standardization
JCS	Joint Chiefs of Staff
JTF	Joint Task Force
LCMC	Life Cycle Management Command
LRA	Least Recently Active
LSB	Least Significant Bit
LZ	Lempel-Ziv
LZW	Lempel-Ziv-Welch

M	Mandatory
MAC	Media Access Control
MIL-STD	Military Standard
MIN IMP	Minimum Implementation
MSB	Most Significant Bit
MTF	Message Text Format
NA	Not Applicable
NATO	North Atlantic Treaty Organization
ND	Not Determined
NITF	National Imagery Transmission Format
NITFS	National Imagery Transmission Format System
NLPT	Network Layer Pass Through (MIL-STD-188-220)
NSIF	NATO Secondary Imagery Format
OSI	Open Systems Interconnection
PA	Preparing Activity
PDU	Protocol Data Unit
QOS	Quality of Service
QSO	Queue Size in Octets
RFC	Request for Comments
RFE	Request For Exception
S/R	Segmentation/Reassembly
SD1	Standardization Directory
SHA-1	Secure Hash Algorithm
SHS	Secure Hash Standard
SINCGARS	Single Channel Ground and Airborne Radio System
SPI	Security Parameters Information
STANAG	NATO Standard Agreement
TCP	Transmission Control Protocol
TDL	Tactical Data Link
TE	Test Edition
TIDP-TE	Technical Interface Design Plan-Test Edition
UDM	User Data Message
UDMF	User Data Message Format
UDP	User Datagram Protocol
ULP	Upper Layer Protocols
URN	Unit Reference Number
USMTF	United States Message Text Format
VML	Variable Message Format Markup Language
VHF	Very High Frequency
VMF	Variable Message Format
W3C	World Wide Web Consortium
WG	Working Group
WILCO	Will Comply
XML	eXtensible Markup Language
XOR	Exclusive OR

4 GENERAL REQUIREMENTS

4.1 Application Layer Users.

4.1.1 In the context of this MIL-STD, the user of the Application Layer Protocol (ALP) is the application process that requires the communications services provided by the protocol.

4.2 Interoperability.

4.2.1 Interoperability between end systems may be enabled by implementing the ALP specified in this MIL-STD. This standard defines the data communications parameters and protocol conventions that are necessary to support the handling and exchange of single or concatenated UDMs over subnetworks, point-to-point links, and broadcast networks.

4.3 Application Layer Services Provided.

4.3.1 The ALP provides the following services to the application process in order to facilitate the exchange of data between end user systems:

a. Identification of intended communications partners.

b. Identification of privacy/security mechanisms required.

c. Passing of quality-of-service parameters (performance and non-performance parameters).

d. Synchronization of cooperating application processes.

e. ALPDU and UDM handling (distribution, receipting, and monitoring).

f. Identification of constraints on data syntax (character sets, data structure).

g. Data transfer via connectionless operation.

h. Optional security services.

5 DETAILED REQUIREMENTS

5.1 Application Layer.

5.1.1 The Application Layer provides the simplified message-handling protocol.

5.2 Application Layer Protocol Data Unit (ALPDU).

5.2.1 The ALPDU is normally composed of an Application Header and User Data, as shown in FIGURE 1. User Data can take the form of a message or other types of data or messages. However, in certain circumstances, the Application Header can be transmitted without User Data, such as when sending a CANTPRO reply.

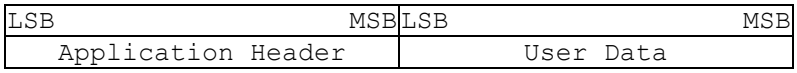

FIGURE 1 Application Layer Protocol Data Unit Structure

5.3 Application Header.

5.3.1 Application Header, General Description.

5.3.1.1 The Application Header precedes the User Data. The Application Header consists of a subset of Application Header Fields from TABLE I – Application Header Map as dictated by its purpose.

5.3.2 Application Header, General Requirements.

5.3.2.1 The Application Header shall be created using Application Header Fields from TABLE I.

5.3.2.2 The order of the Fields in an Application Header shall follow the order shown in TABLE I.

5.3.2.3 A complete Application Header shall have a length which is a multiple of 8 bits.

5.3.2.4 If an Application Header is created and is not a multiple of 8 bits, the HEADER ZERO PADDING Field shall be implemented.

5.3.3 Application Header Map, Description.

5.3.3.1 Application Header Map, General Description.

5.3.3.1.1 TABLE I is an Application Header map which contains:

a. Index Numbers.
b. DFI/DUI numbers.
c. Application Header Field names.
d. Field Length in bits.
e. Categories.
f. Group Codes.
g. Repeat Codes.
h. Resolution Data.

5.3.3.2 Application Header Map, Index Number, Description.

5.3.3.2.1 The index number indicates the numerical position of each field within the Application Header and provides a visual representation of the field structure within an Application Header based on the syntax and repeatability criteria required by presence and recurrence indicators that are discussed below.

5.3.3.2.2 When a presence indicator (as explained in paragraph 5.5) is encountered, the associated field, indicators, or group of indicators and fields will retain the index number of the parent presence indicator and will be further identified by additional numbers beginning with a numerical 1 separated from the presence indicator index by a decimal point (i.e., if the presence indicator is 6, then the first field or indicator following will be 6.1). When a recurring field or group is encountered and does not have a presence indicator, the recurrence indicator will be numbered as though it were following a presence indicator. When a recurring field or group is encountered and is following a group presence indicator, an additional index number will be added beginning with a numerical 1 separated by a decimal point (i.e., if the group presence indicator is 6, then the field recurrence indicator following will be 6.1.1 or if the group presence indicator is 6, then the group recurrence indicator following will be 6.1.1).

5.3.3.3 Application Header Map, DFI/DUI, Description.

5.3.3.3.1 DFI/DUI identifies data elements by DFI and DUI numbers. These numbers provide a reference to the Data Element Dictionary (DED) at Appendix B.

5.3.3.4 Application Header Map, Application Header Field Name, Description.

5.3.3.4.1 The Application Header Field name takes the DUI NAME and is a unique, singular representation of the DFI concept. Presence and recurrence indicators will be displayed as "FPI" (Field Presence Indicator), or "FRI" (Field Recurrence Indicator), "GPI" (Group Presence Indicator), or "GRI" (Group Recurrence Indicator).

5.3.3.5 Application Header Map, Field Length, Description.

5.3.3.5.1 The Field Length identifies the Application Header Field length in binary digits.

5.3.3.6 Application Header Map, Category, Description.

5.3.3.6.1 The Category column is used to mark the field type for each Field within the Application Header. Field types are defined in Section 3 DEFINITIONS. Category column markings are as follows:

a. Mandatory - M.
b. Optional - O.
c. Conditional - C.

5.3.3.7 Application Header Map, Group Code, Description.

5.3.3.7.1 The Group Code column identifies the groups within an Application Header. Group Code column markings are provided in paragraph 5.5.9.2.

5.3.3.8 Application Header Map, Repeat Code, Description.

5.3.3.8.1 The Repeat Code column identifies the fields or groups that are repeatable within an Application Header. Repeat Code column markings are provided in paragraph 5.5.9.3.

5.3.3.9 Application Header Map, Resolution Data, Description.

5.3.3.9.1 The Resolution data will contain explanatory information indicating the group with which the indicator is associated, i.e., GRI for R3. The Resolution data also contains explanatory information about repeatability of fields and groups.

5.4 Implementation.

5.4.1 Minimum Implementation (MIN IMP).

5.4.1.1 Minimum Implementation (MIN IMP), Description.

5.4.1.1.1 This section describes the Minimum Implementation (MIN IMP) of MIL-STD-2045-47001. MIN IMP occurs at several levels and includes:

a. All fields marked "M" in TABLE I Application Header CAT column.

b. All Cases marked "M" in TABLE II Case Level MIN IMP.

c. All Conditions in TABLE III.

d. All Expected Responses marked "M" in TABLE IV Expected Response Level MIN IMP.

e. All Special Considerations marked "M" in TABLE V Special Consideration Level MIN IMP.

5.4.1.1.2 Fields indicated by a "C" in TABLE I Application Header CAT column are conditional fields.

5.4.1.1.3 An "O" in TABLE II, IV or V indicates that the item is optional for implementation.

5.4.1.2 Minimum Implementation (MIN IMP), Requirements.

5.4.1.2.1 All fields marked "M" in TABLE I shall be implemented for transmission.

5.4.1.2.2 All fields marked "M" in TABLE I shall be implemented for reception.

5.4.1.2.3 Cases marked "M" in TABLE II shall be implemented.

5.4.1.2.4 Conditions marked "M" in TABLE III shall be implemented.

5.4.1.2.5 Expected Responses marked "M" in TABLE IV shall be implemented.

5.4.1.2.6 Special Considerations marked "M" in TABLE V shall be implemented.

5.4.2 Field Level Implementation.

5.4.2.1 Field Level Implementation, Description.

5.4.2.1.1 This section describes and sets the requirements for the fields in TABLE I that are determined by the dependence on the setting of certain FPIs, FRIs, GPIs and GRIs.

5.4.2.2 Field Level Implementation, Requirements.

5.4.2.2.1 It shall be mandatory to implement all FPIs for transmission.

5.4.2.2.2 It shall be mandatory to implement all FRIs for transmission.

5.4.2.2.3 It shall be mandatory to implement all GPIs for transmission.

5.4.2.2.4 It shall be mandatory to implement all GRIs for transmission.

5.4.2.2.5 It shall be mandatory to implement all FPIs for reception.

5.4.2.2.6 It shall be mandatory to implement all FRIs for reception.

5.4.2.2.7 It shall be mandatory to implement all GPIs for reception.

5.4.2.2.8 It shall be mandatory to implement all GRIs for reception.

5.4.2.2.9 All fields without an FPI but within a Group that has its GPI set to value 1 (PRESENT) shall be implemented for transmission.

5.4.2.2.10 All fields without an FPI but within a Group that has its GPI set to value 1 (PRESENT) shall be implemented for reception.

5.4.2.2.11 All fields that have their FPI set to value 1 (PRESENT) shall be implemented for transmission.

5.4.2.2.12 All fields that have their FPI set to value 1 (PRESENT) shall be implemented for reception.

5.4.2.2.13 When a system implements a field, it shall implement all field values for that field.

5.4.2.2.14 A system shall implement processing logic for all field values relating to each Field implemented for transmission.

5.4.2.2.15 A system shall implement processing logic for all Field values relating to each Field implemented for reception.

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
1.	6001	006	HEADER VERSION	4	M			MIL-STD-2045-47001 VERSION NUMBER.
2.	4014	002	FPI	1	M			
2.1	6001	010	DATA COMPRESSION TYPE	2	C			
3.	4014	001	GPI	1	M			GPI FOR G1. ORIGINATOR ADDRESS GROUP.
3.1	4014	002	FPI	1	C	G1		
3.1.1	4004	012	URN	24	C	G1		ORIGINATOR.
3.2	4014	002	FPI	1	C	G1		
3.2.1	6010	013	UNIT NAME	448	C	G1		ORIGINATOR.
4.	4014	001	GPI	1	M			GPI FOR G2. RECIPIENT ADDRESS GROUP.
4.1.1	4045	001	GRI	1	C	G2	R1(16)	GRI FOR R1. R1(N): 0 < N <= 16.
4.1.2	4014	002	FPI	1	C	G2	R1	
4.1.2.1	4004	012	URN	24	C	G2	R1	RECIPIENT.
4.1.3	4014	002	FPI	1	C	G2	R1	
4.1.3.1	6010	013	UNIT NAME	448	C	G2	R1	RECIPIENT.
5.	4014	001	GPI	1	M			GPI FOR G3. INFORMATION ADDRESS GROUP.
5.1.1	4045	001	GRI	1	C	G3	R2(16)	GRI FOR R2. 0 < R2 <= (16 – N).
5.1.2	4014	002	FPI	1	C	G3	R2	
5.1.2.1	4004	012	URN	24	C	G3	R2	INFORMATION ADDRESSEE.
5.1.3	4014	002	FPI	1	C	G3	R2	
5.1.3.1	6010	013	UNIT NAME	448	C	G3	R2	INFORMATION ADDRESSEE.
6.	4014	002	FPI	1	M			
6.1	6005	003	HEADER SIZE	16	C			
7.	4014	001	GPI	1	M			GPI FOR G4. FUTURE USE 1.

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
7.1	6005	004	GROUP SIZE	12	C	G4		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G4		
8.	4014	001	GPI	1	M			GPI FOR G5. FUTURE USE 2.
8.1	6005	004	GROUP SIZE	12	C	G5		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G5		
9.	4014	001	GPI	1	M			GPI FOR G6. FUTURE USE 3.
9.1	6005	004	GROUP SIZE	12	C	G6		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G6		
10.	4014	001	GPI	1	M			GPI FOR G7. FUTURE USE 4.
10.1	6005	004	GROUP SIZE	12	C	G7		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G7		
11.	4014	001	GPI	1	M			GPI FOR G8. FUTURE USE 5.
11.1	6005	004	GROUP SIZE	12	C	G8		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G8		
12.1	4045	001	GRI	1	M		R3(16)	GRI FOR R3. USER DATA MESSAGE HANDLING GROUP. R3(N): 0 < N <= 16.
12.2	6001	012	USER DATA MESSAGE FORMAT	4	M		R3	
12.3	4014	002	FPI	1	M		R3	
12.3.1	6001	011	USER DATA MESSAGE STANDARD VERSION	4	C		R3	

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
12.4	4014	001	GPI	1	M		R3	GPI FOR G9. VMF MESSAGE IDENTIFICATION GROUP.
12.4.1	4081	001	FUNCTIONAL AREA DESIGNATOR	4	C	G9	R3	
12.4.2	4085	019	MESSAGE NUMBER	7	C	G9	R3	
12.4.3	4014	002	FPI	1	C	G9	R3	
12.4.3.1	6001	013	VMF MESSAGE SUBTYPE	7	C	G9	R3	
12.5	4014	002	FPI	1	M		R3	
12.5.1	6006	001	FILE NAME	448	C		R3	
12.6	4014	002	FPI	1	M		R3	
12.6.1	6005	001	USER DATA MESSAGE SIZE	20	C		R3	
12.7	6001	005	OPERATION INDICATOR	2	M		R3	
12.8	6007	004	RETRANSMIT INDICATOR	1	M		R3	
12.9	6002	006	USER DATA MESSAGE PRECEDENCE	3	M		R3	
12.10	6002	002	USER DATA MESSAGE SECURITY CLASSIFICATION	2	M		R3	
12.11	4014	002	FPI	1	M		R3	
12.11.1	4045	002	FRI	1	C		R3/R4 (16)	FRI FOR R4. CONTROL/RELEASE MARKING. R4(N): 0 < N <= 16.
12.11.2	6002	005	CONTROL/RELEASE MARKING	9	C		R3/R4	
12.12	4014	001	GPI	1	M		R3	GPI FOR G10. ORIGINATOR DATE TIME GROUP GROUP.
12.12.1	4098	001	YEAR	7	C	G10	R3	
12.12.2	4099	001	MONTH	4	C	G10	R3	
12.12.3	4019	001	DAY OF MONTH	5	C	G10	R3	
12.12.4	792	001	HOUR	5	C	G10	R3	
12.12.5	797	004	MINUTE	6	C	G10	R3	

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
12.12.6	380	001	SECOND	6	C	G10	R3	
12.12.7	4014	002	FPI	1	C	G10	R3	
12.12.7.1	6005	002	DTG EXTENSION	12	C	G10	R3	
12.13	4014	001	GPI	1	M		R3	GPI FOR G11. PERISHABILITY DATE TIME GROUP GROUP.
12.13.1	4098	001	YEAR	7	C	G11	R3	
12.13.2	4099	001	MONTH	4	C	G11	R3	
12.13.3	4019	001	DAY OF MONTH	5	C	G11	R3	
12.13.4	792	001	HOUR	5	C	G11	R3	
12.13.5	797	004	MINUTE	6	C	G11	R3	
12.13.6	380	001	SECOND	6	C	G11	R3	
12.14	4014	001	GPI		M		R3	GPI FOR G12. ACKNOWLEDGMENT REQUEST GROUP.
12.14.1	6007	001	MACHINE ACKNOWLEDGE REQUEST INDICATOR	1	C	G12	R3	
12.14.2	6007	002	OPERATOR ACKNOWLEDGE REQUEST INDICATOR	1	C	G12	R3	
12.14.3	6007	003	OPERATOR REPLY REQUEST INDICATOR	1	C	G12	R3	
12.15	4014	001	GPI	1	M		R3	GPI FOR G13. RESPONSE DATA GROUP.
12.15.1	4098	001	YEAR	7	C	G13	R3	
12.15.2	4099	001	MONTH	4	C	G13	R3	
12.15.3	4019	001	DAY OF MONTH	5	C	G13	R3	
12.15.4	792	001	HOUR	5	C	G13	R3	
12.15.5	797	004	MINUTE	6	C	G13	R3	
12.15.6	380	001	SECOND	6	C	G13	R3	
12.15.7	4014	002	FPI	1	C	G13	R3	
12.15.7.1	6005	002	DTG EXTENSION	12	C	G13	R3	

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
12.15.8	6003	001	USER DATA MESSAGE RECEIPT/COMPLIANCE	3	C	G13	R3	
12.15.9	4014	002	FPI	1	C	G13	R3	
12.15.9.1	6003	002	CANTCO REASON	3	C	G13	R3	
12.15.10	4014	002	FPI	1	C	G13	R3	
12.15.10.1	6003	005	CANTPRO REASON	6	C	G13	R3	
12.15.11	4014	002	FPI	1	C	G13	R3	
12.15.11.1	6004	001	REPLY AMPLIFICATION	350	C	G13	R3	
12.16	4014	001	GPI	1	M		R3	GPI FOR G14. REFERENCE USER DATA MESSAGE DATA GROUP.
12.16.1.1	4045	001	GRI	1	C	G14	R3/R5 (4)	GRI FOR R5. R5(N): 0 < N <= 4.
12.16.1.2	4014	002	FPI	1	C	G14	R3/R5	
12.16.1.2.1	4004	012	URN	24	C	G14	R3/R5	REFERENCE USER DATA MESSAGE ORIGINATOR.
12.16.1.3	4014	002	FPI	1	C	G14	R3/R5	
12.16.1.3.1	6010	013	UNIT NAME	448	C	G14	R3/R5	REFERENCE USER DATA MESSAGE ORIGINATOR.
12.16.1.4	4098	001	YEAR	7	C	G14	R3/R5	
12.16.1.5	4099	001	MONTH	4	C	G14	R3/R5	
12.16.1.6	4019	001	DAY OF MONTH	5	C	G14	R3/R5	
12.16.1.7	792	001	HOUR	5	C	G14	R3/R5	
12.16.1.8	797	004	MINUTE	6	C	G14	R3/R5	
12.16.1.9	380	001	SECOND	6	C	G14	R3/R5	
12.16.1.10	4014	002	FPI	1	C	G14	R3/R5	
12.16.1.10.1	6005	002	DTG EXTENSION	12	C	G14	R3/R5	
12.17	4014	001	GPI	1	M		R3	GPI FOR G15. FUTURE USE 6, VERSION 1.
12.17.1	6005	004	GROUP SIZE	12	C	G15	R3	

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
12.17.2	4014	001	GPI	1	M	G15	R3	GPI FOR G15.1. USER DATA MESSAGE VERSION GROUP.
12.17.2.1	6005	004	GROUP SIZE	12	C	G15/G15.1	R3	
12.17.2.2	6001	014	USER DATA MESSAGE VERSION	10	C	G15/G15.1	R3	
			<Future Use Group Sub-Group(s) will be present here>	0-4072	C	G15		
12.18	4014	001	GPI	1	M		R3	GPI FOR G16. FUTURE USE 7.
12.18.1	6005	004	GROUP SIZE	12	C	G16	R3	
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G16		
12.19	4014	001	GPI	1	M		R3	GPI FOR G17. FUTURE USE 8.
12.19.1	6005	004	GROUP SIZE	12	C	G17	R3	
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G17		
12.20	4014	001	GPI	1	M		R3	GPI FOR G18. FUTURE USE 9.
12.20.1	6005	004	GROUP SIZE	12	C	G18	R3	
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G18		
12.21	4014	001	GPI	1	M		R3	GPI FOR G19. FUTURE USE 10.
12.21.1	6005	004	GROUP SIZE	12	C	G19	R3	
			<Future information group(s) and/or field(s) will be present here>	0-4095	C	G19		
12.22	4014	001	GPI	1	M		R3	GPI FOR G20. USER DATA MESSAGE SECURITY GROUP.

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
12.22.1	6008	001	SECURITY PARAMETERS INFORMATION	4	C	G20	R3	
12.22.2	4014	001	GPI	1	C	G20	R3	GPI FOR G21. KEYING MATERIAL GROUP.
12.22.2.1	6009	001	KEYING MATERIAL ID LENGTH	3	C	G20/G21	R3	
12.22.2.2	6008	002	KEYING MATERIAL ID	64	C	G20/G21	R3	
12.22.3	4014	001	GPI	1	C	G20	R3	GPI FOR G22. CRYPTOGRAPHIC INITIALIZATION GROUP.
12.22.3.1	6009	002	CRYPTOGRAPHIC INITIALIZATION LENGTH	4	C	G20/G22	R3	
12.22.3.2	6008	003	CRYPTOGRAPHIC INITIALIZATION	1024	C	G20/G22	R3	
12.22.4	4014	001	GPI	1	C	G20	R3	GPI FOR G23. KEY TOKEN GROUP.
12.22.4.1	6009	003	KEY TOKEN LENGTH	8	C	G20/G23	R3	
12.22.4.2.1	4045	002	FRI	1	C	G20/G23	R3/R6 (16)	R6(N): 0 < N <= 16.
12.22.4.2.2	6008	004	KEY TOKEN	16384	C	G20/G23	R3/R6	
12.22.5	4014	001	GPI	1	C	G20	R3	GPI FOR G24. AUTHENTICATION (A) GROUP.
12.22.5.1	6009	004	AUTHENTICATION DATA (A) LENGTH	7	C	G20/G24	R3	
12.22.5.2	6008	005	AUTHENTICATION DATA (A)	8192	C	G20/G24	R3	
12.22.6	4014	001	GPI	1	C	G20	R3	GPI FOR G25. AUTHENTICATION (B) GROUP.
12.22.6.1	6009	005	AUTHENTICATION DATA (B) LENGTH	7	C	G20/G25	R3	
12.22.6.2	6008	006	AUTHENTICATION DATA (B)	8192	C	G20/G25	R3	
12.22.7	6008	007	SIGNED ACKNOWLEDGE REQUEST INDICATOR	1	C	G20	R3	

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
12.22.8	4014	001	GPI	1	C	G20	R3	GPI FOR G26. USER DATA MESSAGE SECURITY PADDING GROUP.
12.22.8.1	6009	006	USER DATA MESSAGE SECURITY PADDING LENGTH	8	C	G20/G26	R3	
12.22.8.2	4014	002	FPI	1	C	G20/G26	R3	
12.22.8.2.1	6008	008	USER DATA MESSAGE SECURITY PADDING	2040	C	G20/G26	R3	
13.	4014	001	GPI	1	M			GPI FOR G27. FUTURE USE 11.
13.1	6005	004	GROUP SIZE	12	C	G27		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G27		
14.	4014	001	GPI	1	M			GPI FOR G28. FUTURE USE 12.
14.1	6005	004	GROUP SIZE	12	C	G28		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G28		
15.	4014	001	GPI	1	M			GPI FOR G29. FUTURE USE 13.
15.1	6005	004	GROUP SIZE	12	C	G29		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G29		
16.	4014	001	GPI	1	M			GPI FOR G30. FUTURE USE 14.
16.1	6005	004	GROUP SIZE	12	C	G30		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G30		
17.	4014	001	GPI	1	M			GPI FOR G31. FUTURE USE 15.

TABLE I Application Header Map

Index no	DFI	DUI	Field Name	Field Length	CAT	Group Code	Repeat Code	Resolution Data
17.1	6005	004	GROUP SIZE	12	C	G31		
			<Future Use Group Sub-Group(s) will be present here>	0-4095	C	G31		
18.	6011	001	HEADER ZERO PADDING	0-7	C			

TABLE II Case Level MIN IMP.

Case	Title	Transmit	Receive
1	Original Application Layer Protocol Data Unit	M	M
2	Receipt/Compliance Response	M	M
3	Signed Acknowledgment Response	O	O

TABLE III Conditions Level MIN IMP.

Condition	Title	Transmit	Receive
1	URN and UNIT NAME Mutual Exclusivity	M	M
2	ORIGINATOR DATE TIME GROUP Group Presence in Original User Data Message Requiring a Receipt/Compliance Response	M	M
3	SPI is Value 0 (Authentication/No Encryption)	M	M
4	SIGNED ACKNOWLEDGE REQUEST INDICATOR and ACKNOWLEDGMENT REQUEST Group (G12) Relationship	M	M
5	Retransmitted User Data Message ORIGINATOR DTG Setting	M	M

TABLE IV Expected Response Level MIN IMP.

Expected Response	Title	Transmit	Receive
1	Machine Acknowledge Requested	M	M
2	Operator Acknowledge Requested	M	M
3	Operator Reply Requested	M	M
4	Cannot Process a Signed Acknowledgment Request	O	O
5	Incorrect Header Size	O	O
6	Incorrect User Data Message Size	O	O
7	Non Zero Value in HEADER ZERO PADDING Field	O	O
8	Data Has Perished	M	M

TABLE V Special Consideration Level MIN IMP.

Special Consideration	Title	Transmit	Receive
1	Response to Header Version Non-Interoperability	M	M
2	User Data Message Concatenation	O	M
3	Decompression of User Data Prior to Parsing	M	M
4	UNIT NAME Usage in a Receipt/Compliance Response	M	M
5	URN Usage in a Receipt/Compliance Response	M	M
6	Use of Segmentation/Reassembly Protocol	M	M
7	Use of MIL-STD-188-220 Network Layer Pass Through (NLPT)	O	O

5.5 Application Header Formatting and Syntax.

5.5.1 Application Header Formatting and Syntax, General Description.

5.5.1.1 Application Header syntax is implemented in the Host System software and is transparent to the user. The Application Header facilitates adaptive and efficient construction, uses a variable format syntax and format structure, and consists of an ordered collection of bits (ones and zeroes). A group is a combination of two or more related fields designated as a group. There are two types of groups, "G" groups and "R" groups. A "G" group is a combination of related fields. An "R" group is a repeatable combination of related fields. The presence and recurrence indicator syntax fields used in the selection of fields to be transmitted are defined in the subsequent paragraphs and are allowed in groups.

5.5.2 Field Presence Indicator (FPI).

5.5.2.1 Field Presence Indicator (FPI), Description.

5.5.2.1.1 FPIs are 1-bit fields that are used to indicate the presence or absence of the field following the FPI as indicated in TABLE I. FPIs are not used for single bit fields.

5.5.2.2 Field Presence Indicator (FPI), Requirements.

5.5.2.2.1 If a field is to be used and TABLE I indicates that it is controlled by an FPI, that FPI shall be set to value 1 (PRESENT).

5.5.2.2.2 If a field is not to be used and TABLE I indicates that it is controlled by an FPI, that FPI shall be set to value 0 (NOT PRESENT).

5.5.2.2.3 If a repeatable field controlled by an FPI is not to be transmitted then its associated FRI shall be omitted.

5.5.2.2.4 If a repeatable field controlled by a FPI is to be transmitted, only one iteration of the FPI shall be transmitted whether or not the Field is repeated.

5.5.3 Field Recurrence Indicator (FRI).

5.5.3.1 Field Recurrence Indicator (FRI), Description.

5.5.3.1.1 FRIs are 1-bit fields that are used to designate whether a field is repeated again (FRI=1) after the current iteration or not (FRI=0). The maximum number of appearances, including the first appearance, for a repeated field is indicated in parentheses in the repeat code column in TABLE I as described in paragraph 5.5.9.3.1.b.

5.5.3.2 Field Recurrence Indicator (FRI), Requirements.

5.5.3.2.1 When an FRI is set to value 0 (NOT REPEATED), the field controlled by the FRI shall not be repeated in the USER DATA MESSAGE HANDLING Group (R3) in which the FRI and the controlled field are present.

5.5.3.2.2 When an FRI is set to value 1 (REPEATED), the field controlled by the FRI shall be repeated in the USER DATA MESSAGE HANDLING Group (R3) in which the FRI and the controlled field are present.

5.5.4 Group Presence Indicator (GPI).

5.5.4.1 Group Presence Indicator (GPI), Description.

5.5.4.1.1 GPIs are 1-bit fields that are used to indicate the presence (GPI=1) or absence (GPI=0) of a group.

5.5.4.2 Group Presence Indicator (GPI), Requirements.

5.5.4.2.1 If a group is to be transmitted and TABLE I indicates that it is controlled by a GPI, that GPI shall be set to value 1 (PRESENT).

5.5.4.2.2 If a group is not to be transmitted and TABLE I indicates that it is controlled by a GPI, that GPI shall be set to value 0 (NOT PRESENT).

5.5.4.2.3 If a repeatable field or group controlled by a GPI is to be transmitted, only one iteration of the GPI shall be transmitted whether or not the field or group is repeated.

5.5.5 Group Recurrence Indicator (GRI).

5.5.5.1 Group Recurrence Indicator (GRI), Description.

5.5.5.1.1 GRIs are 1-bit fields that are used to indicate whether a group is to be repeated (GRI=1) after the current iteration or not (GRI=0). A group that is repeatable is referred to as an "R" group. The maximum number of appearances, including the first appearance, for a repeated group is indicated in parentheses in the repeat code column in TABLE I as describe in paragraph 5.5.9.3. "R" groups are often but not always controlled by a GPI and therefore an "R" group without a GPI will be transmitted at least once.

5.5.5.2 Group Recurrence Indicator (GRI), Requirements.

5.5.5.2.1 A GRI shall be set to value 0 (NOT REPEATED) to indicate that the controlled group does not occur after this iteration.

5.5.5.2.2 A GRI shall be set to value 1 (REPEATED) to indicate the recurrence of the controlled group after this iteration.

5.5.6 End-Of-Literal Field Marker.

5.5.6.1 End-Of-Literal Field Marker, Description.

5.5.6.1.1 The End-Of-Literal Field Marker (EOLF) is the ASCII value 127 (ASCII DELETE) and is used to indicate the end of the field for free text, variable length, character-based, literal fields only. The end of a literal field may be indicated by using all the bits in the field.

5.5.6.2 End-Of-Literal Field Marker, Requirements.

5.5.6.2.1 The End-Of-Literal Field (EOLF) marker shall be the 7-bit ASCII DELETE character (1111111).

5.5.6.2.2 Systems shall recognize when the End-Of-Literal Field (EOLF) marker is being used to indicate the end of a field.

5.5.6.2.3 Systems shall be able to signify the end of a free-text, character-based, literal field by using the maximum number of bits for the field as specified in TABLE I.

5.5.6.2.4 Systems shall recognize when the maximum number of bits indicates the end of a field.

5.5.6.2.5 Systems shall use the End-Of-Literal Field (EOLF) marker to indicate the end of a field when the maximum number of bits is not used in the construction of that free-text, character-based, literal field.

5.5.6.2.6 Free text, variable length, character-based literal fields shall have at least one character other than the End-Of-Literal Field (EOLF) marker when the field is transmitted.

5.5.7 Data-Field Construction.

5.5.7.1 Data-Field Construction, Description.

5.5.7.1.1 Application Header fields are linearly joined before being passed to the next lower protocol layer. The Least Significant Bit (LSB) of each successive Application Header field is concatenated to the Most Significant Bit (MSB) of the preceding Application Header field. The following construction procedures prescribe the sequence in which the Application Header fields are linearly joined. The two representations for data elements are:

a. 7-bit ASCII characters.

b. Binary numbers.

5.5.7.2 Data-Field Construction, Requirements.

5.5.7.2.1 All Application Header fields shall be least significant bit LSB-justified.

5.5.7.2.2 All Application Header fields shall be joined LSB first.

5.5.7.2.3 The first ASCII character in a literal field shall be LSB-justified.

5.5.7.2.4 When joining ASCII characters within a literal field, the LSB of each character shall immediately follow the MSB of the previous character.

5.5.8 Binary Data Element.

5.5.8.1 Binary Data Element, Description.

5.5.8.1.1 A binary data element is a number expressed in the base-2 numeral system.

5.5.8.2 Binary Data Element, Requirements.

5.5.8.2.1 An Application Header element composed of binary code shall be interpreted as a single value.

5.5.9 Application Header Format Notations.

5.5.9.1 Category, Description.

5.5.9.1.1 Fields that are mandatory are indicated by an "M" in the category (CAT) column. Those fields indicated by a "C" in the category (CAT) column are conditional fields.

5.5.9.2 Group Code, Description.

5.5.9.2.1 The Groups in TABLE I represent a logical grouping of information. Each field belonging to a Group is indicated in the group column of TABLE I and the format described as follows:

a. GN - Indicates the field is part of a group, with G identifying "Group" and where N identifies the group number (that is, G1 indicates the first group in the ALPDU).

b. GN/GN - Nested groups are indicated by "GN/GN" notation. The right-most Group is the nested group. The left-most Group is the group within which the nested group is nested; e.g. G1/G2 where G2 is nested in G1.

c. The notation G*X.Y* shall be used to identify FUG sub groups. *X* is the Group number of the FUG and *Y* is the sub group number.

5.5.9.3 Repeat Group Code, Description.

5.5.9.3.1 The Repeat Groups in TABLE I represent a logical grouping of information that may be repeated. Each field belonging to a Repeat Group is indicated in the Repeat Code column of TABLE I and the format described as follows:

a. RN - Indicates the field is part of a group, with R identifying "Repeat Group" and where N identifies the Repeat Group number (that is, R1 indicates the first Repeat Group in the ALPDU).

b. (N) – Indicates the maximum number of appearances of the group in an Application Header. The notation is appended to the first field of a Repeat Group. R3(16) indicates that the third Repeat Group can appear a maximum of 16 times for each Group occurrence.

c. RN/RN - Nested Repeat Groups are indicated by "RN/RN" notation. The right-most Repeat Group is the nested group. The left-most Repeat Group is the group within which the nested group is nested; e.g. R3/R6 where R6 is nested in R3.

5.6 Application Header Fields.

5.6.1 HEADER VERSION Field.

5.6.1.1 HEADER VERSION Field, Description.

5.6.1.1.1 The HEADER VERSION Field is a mandatory 4-bit binary field used to represent the MIL-STD-2045-47001 Application Header Version being used for the ALPDU. FUG application allows systems to process ALPDUs from systems implementing MIL-STD-2045-47001 versions which are currently not defined i.e. future versions. Value 15 (VERSION SENT NOT IMPLEMENTED) is used to indicate to an Originator that the Recipient does not implement MIL-STD-2045-47001C. If an Application Header is received with a HEADER VERSION Field indicating MIL-STD-2045-47001B or earlier, the only way to indicate that the ALPDU cannot be processed is to respond with a CANTPRO Receipt/Compliance response.

5.6.1.2 HEADER VERSION Field, Requirements.

5.6.1.2.1 On transmission of an ALPDU, the HEADER VERSION Field shall be set to value 5 (MIL-STD-2045-47001E) as specified by the Data Element Dictionary at Appendix B to indicate the version of the Application Header being used.

5.6.1.2.2 If a Recipient receives an ALPDU with the HEADER VERSION Field set to value 0 (MIL-STD-2045-47001), a Receipt/Compliance response shall be transmitted with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO).

5.6.1.2.3 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 0 (MIL-STD-2045-47001), the ALPDU shall be discarded without further processing.

5.6.1.2.4 If a Recipient receives an ALPDU with the HEADER VERSION Field set to value 1 (MIL-STD-2045-47001B), a Receipt/Compliance response shall be transmitted with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO).

5.6.1.2.5 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 1 (MIL-STD-2045-47001B), the ALPDU shall be discarded without further processing.

5.6.1.2.6 If a Recipient receives an ALPDU with the HEADER VERSION Field set to value 2 (MIL-STD-2045-47001C), a version non-interoperability response shall be transmitted with the HEADER VERSION Field set to value 15 (VERSION SENT NOT IMPLEMENTED).

5.6.1.2.7 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 2 (MIL-STD-2045-47001C), the ALPDU shall be discarded without further processing.

5.6.1.2.8 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 3 (MIL-STD-2045-47001D), the ALPDU shall be processed.

5.6.1.2.9 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 4 (MIL-STD-2045-47001D Change 1), the ALPDU shall be processed.

5.6.1.2.10 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 5 (MIL-STD-2045-47001E), the ALPDU shall be processed.

5.6.1.2.11 It shall be a system option to alert the operator on receipt of an ALPDU with the HEADER VERSION Field set to value 15 (VERSION SENT NOT IMPLEMENTED).

5.6.1.2.12 If an Addressee receives an ALPDU with the HEADER VERSION Field set to value 6 through 14 (UNDEFINED), the ALPDU shall be processed.

5.6.2 DATA COMPRESSION TYPE Field.

5.6.2.1 DATA COMPRESSION TYPE Field, Description.

5.6.2.1.1 The DATA COMPRESSION TYPE Field is a 2-bit binary field used to indicate what data compression algorithm has been applied to the UDMs in the User Data portion of the ALPDU, refer to RFC 1951 and RFC 1952. The absence of this field therefore signifies that data compression is not used. Data compression is not applied to the Application Header.

5.6.2.2 DATA COMPRESSION TYPE Field, Requirements.

5.6.2.2.1 Data compression shall only be applied to the User Data portion of an ALPDU.

5.6.2.2.2 The FPI of the DATA COMPRESSION TYPE Field shall be set to value 0 (NOT PRESENT) when data compression is not applied to the User Data portion of an ALPDU.

5.6.2.2.3 The FPI of the DATA COMPRESSION TYPE Field shall be set to value 1 (PRESENT) when data compression is applied to User Data portion of an ALPDU.

5.6.2.2.3 The DATA COMPRESSION TYPE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the type of data compression applied to the User Data portion of an Application Layer Protocol Data Unit.

5.6.2.2.4 When data compression is applied to the User Data portion of an ALPDU, all UDMs in the User Data shall be independently compressed.

5.6.3 URN Field.

5.6.3.1 URN Field, Description.

5.6.3.1.1 The Unit Reference Number (URN) Field is used to uniquely identify friendly military units, broadcast networks and multicast groups. The URN can also identify an ALPDU to be broadcast and would be used to send an ALPDU to the local subnetwork without routing (e.g., radio subnetwork, data link address of 127, IP broadcast without routing, or Local Area Network subnetwork broadcast without routing). Within the Application Header, the URN Field and the UNIT NAME Field are mutually exclusive within the ORIGINATOR ADDRESS Group (G1), within the RECIPIENT ADDRESS Group (G2) and within the INFORMATION ADDRESS Group (G3).

5.6.3.2 URN Field, Requirements.

5.6.3.2.1 The URN Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the reference number of the unit being referred to as assigned in accordance with interface operating procedures.

5.6.3.2.2 No acknowledgment shall be transmitted in response to an ALPDU addressed to the Broadcast URN.

5.6.3.2.3 No acknowledgment shall be transmitted in response to an ALPDU addressed to the UNIT NAME "Broadcast URN".

5.6.4 UNIT NAME Field.

5.6.4.1 UNIT NAME Field, Description.

5.6.4.1.1 The UNIT NAME field is used to uniquely identify a friendly military individual, unit, broadcast group or multicast group. The field is divided into 64 groups of 7 bits each representing an ASCII character. Special characters are legal. Within the Application Header, the URN Field and the UNIT NAME Field are mutually exclusive within the same address group.

5.6.4.2 UNIT NAME Field, Requirements.

5.6.4.2.1 The UNIT NAME Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the literal name for the unit being referred.

5.6.5 HEADER SIZE Field.

5.6.5.1 HEADER SIZE Field, Description.

5.6.5.1.1 The HEADER SIZE Field is a 16-bit field used to indicate the size, in octets, of the Application Header. The octet count includes all Application Header fields including the HEADER SIZE Field itself.

5.6.5.2 HEADER SIZE Field, Requirements.

5.6.5.2.1 The HEADER SIZE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the size of the Application Header in octets.

5.6.5.2.2 The HEADER SIZE Field shall be present when sending ALPDUs over a streaming transport mechanism, e.g. a persistent Transmission Control Protocol (TCP) connection.

5.6.5.2.3 An ALPDU with the USER DATA MESSAGE HANDLING Group (R3) GRI set to value 1 (REPEATED) shall have the HEADER SIZE Field FPI set to value 1 (PRESENT).

5.6.6 GROUP SIZE Field.

5.6.6.1 GROUP SIZE Field, Description.

5.6.6.1.1 The GROUP SIZE Field is used in two places; within a primary FUG and within a sub-group nested in a primary FUG. The GROUP SIZE Field allows system knowledge of the number of bits in a FUG or FUG sub-group. The GROUP SIZE Field is a 12-bit binary number indicating the size of a FUG, including all nested sub-groups.

5.6.6.1.2 Implementations compliant with MIL-STD-2045-47001D and D w/CHANGE 1 will use the GROUP SIZE Field value to determine how many bits to account for and disregard before resuming full processing of the received data. Implementations compliant with MIL-STD-2045-47001E and later versions may use the GROUP SIZE Field to similarly process optional FUGs, the contents of which are not implemented.

5.6.6.2 GROUP SIZE Field, Requirements.

5.6.6.2.1 The GROUP SIZE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the size of the FUG in bits.

5.6.7 USER DATA MESSAGE FORMAT Field.

5.6.7.1 USER DATA MESSAGE FORMAT Field, Description.

5.6.7.1.1 The mandatory USER DATA MESSAGE FORMAT (UDMF) Field indicates the format of the data that is contained in the User Data portion of the ALPDU as described in paragraph 5.9. The format and type of the data for each UDMF is not defined in this MIL-STD. The use of a mix of different UDMFs is allowed within iterations of the USER DATA MESSAGE HANDLING Group (R3).

5.6.7.2 USER DATA MESSAGE FORMAT Field, Requirements.

5.6.7.2.1 The UDMF Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the format of the data in a UDM.

5.6.7.2.2 When sending a Receipt/Compliance Response the UDMF Field shall be set to the same value as the UDMF Field value in the received UDM being acknowledged.

5.6.8 USER DATA MESSAGE STANDARD VERSION Field.

5.6.8.1 USER DATA MESSAGE STANDARD VERSION Field, Description.

5.6.8.1.1 The USER DATA MESSAGE STANDARD VERSION Field is used to identify the document or publication defining the data format for the UDMF used in the User Data portion of the ALPDU. The field also indicates the version of the document or publication. Not all UDMFs have an associated standard. For some UDMFs, the facility exists to identify the UDM message version as opposed to the UDM standard version.

5.6.8.2 USER DATA MESSAGE STANDARD VERSION Field, Requirements.

5.6.8.2.1 The USER DATA MESSAGE STANDARD VERSION Field FPI shall be set to value 0 (NOT PRESENT) when the UDMF for the User Data being referred to is set to value 1 (BINARY FILE).

5.6.8.2.2 The USER DATA MESSAGE STANDARD VERSION Field FPI shall be set to value 0 (NOT PRESENT) when the UDMF for the User Data being referred to is set to value 4 (REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT).

5.6.8.2.3 For UDMFs other than value 1 (BINARY FILE) and value 4 (REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT), the USER DATA MESSAGE STANDARD VERSION Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the version of the message standard used by the UDM contained in the User Data portion of the ALPDU.

5.6.9 FUNCTIONAL AREA DESIGNATOR (FAD) Field.

5.6.9.1 FUNCTIONAL AREA DESIGNATOR (FAD) Field, Description.

5.6.9.1.1 The FUNCTIONAL AREA DESIGNATOR (FAD) Field is composed of a 4-bit binary value used to identify the functional area of a VMF message being transferred. The VMF Functional Areas are described in MIL-STD-6017.

5.6.9.2 FUNCTIONAL AREA DESIGNATOR (FAD) Field, Requirements.

5.6.9.2.1 The FUNCTIONAL AREA DESIGNATOR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the functional area of a specific VMF message.

5.6.10 MESSAGE NUMBER Field.

5.6.10.1 MESSAGE NUMBER Field, Description.

5.6.10.1.1 The MESSAGE NUMBER Field is composed of a 7-bit binary value used with the FAD value to identify a VMF message. The MESSAGE NUMBER Field value matches the VMF K Series message number. A list of VMF messages will be found in MIL-STD-6017.

5.6.10.2 MESSAGE NUMBER Field, Requirements.

5.6.10.2.1 The MESSAGE NUMBER Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the specific message number within a VMF Functional Area Designator.

5.6.11 VMF MESSAGE SUBTYPE Field.

5.6.11.1 VMF MESSAGE SUBTYPE Field, Description.

5.6.11.1.1 The VMF MESSAGE SUBTYPE Field is used with the FUNCTIONAL AREA DESIGNATOR Field and MESSAGE NUMBER Field values to identify a message case within a VMF K Series message. Case statements exist for some VMF messages in order to define specific rules for the preparation of the message for transmission, and/or reception. These statements include the specific function of a VMF message, its purpose(s), and the conditions for the use of data groups and data elements within that VMF message.

5.6.11.1.2 The VMF MESSAGE SUBTYPE Field value matches the VMF K Series Message Case number. A list of VMF messages will be found in MIL-STD-6017.

5.6.11.2 VMF MESSAGE SUBTYPE Field, Requirements.

5.6.11.2.1 When a particular Case of the VMF message identified in the MESSAGE NUMBER Field forms the User Data being identified, the VMF MESSAGE SUBTYPE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the specific Case.

5.6.12 FILE NAME Field.

5.6.12.1 FILE NAME Field, Description.

5.6.12.1.1 The FILE NAME Field is a variable size (up to a maximum of 448 bits) character-coded field. The FILE NAME Field indicates the name of a file or data block contained in a UDM. The field is divided into 64 groups of 7 bits each representing an ASCII character. The last four characters of the field may consist of a period followed by a three-character ending, indicative of the file type (e.g., .txt, .doc, .exe, .bin). Special characters are legal.

5.6.12.2 FILE NAME Field, Requirements.

5.6.12.2.1 The FILE NAME Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the name of a computer file or data block in a UDM.

5.6.13 USER DATA MESSAGE SIZE Field.

5.6.13.1 USER DATA MESSAGE SIZE Field, Description.

5.6.13.1.1 The USER DATA MESSAGE SIZE Field is a binary number used to indicate the size, in bytes, of the associated UDM.

5.6.13.2 USER DATA MESSAGE SIZE Field, Requirements.

5.6.13.2.1 The USER DATA MESSAGE SIZE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the size of the UDM in bytes.

5.6.13.2.2 If the system option for User Data compression is implemented, the USER DATA MESSAGE SIZE Field shall reflect the size of the UDM after it has been compressed.

5.6.13.2.3 The USER DATA MESSAGE SIZE Field FPI shall be set to value 0 (NOT PRESENT) when a delimited transport protocol is being used.

5.6.13.2.4 If the ALPDU is being sent via a streaming/undelimited transport protocol such as Transmission Control Protocol (TCP) and the USER DATA MESSAGE HANDLING Group (R3) GRI is set to value 0 (NOT REPEATED), the USER DATA MESSAGE SIZE Field FPI shall be set to value 1 (PRESENT).

5.6.13.2.5 An ALPDU with the USER DATA MESSAGE HANDLING Group (R3) GRI set to value 1 (REPEATED) shall have each iteration of the USER DATA MESSAGE SIZE Field FPI set to value 1 (PRESENT).

5.6.13.2.6 The USER DATA MESSAGE SIZE Field shall be present if the transport protocol is unknown.

5.6.13.2.7 If a UDM is not a multiple of 8 bits, zeroes shall be added to the end of the UDM until the resultant UDM is a multiple of 8 bits.

5.6.14 OPERATION INDICATOR Field.

5.6.14.1 OPERATION INDICATOR Field, Description.

5.6.14.1.1 The mandatory OPERATION INDICATOR Field is a 2-bit binary codeword used to indicate the operational function of the UDM. The available settings are:

a. Operation. A sequence of tactical actions with a common purpose or unifying theme; A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. (JP 1-02).

b. Exercise. A military maneuver or simulated wartime operation involving planning, preparation, and execution that is carried out for the purpose of training and evaluation. (JP 1-02).

c. Simulation. Bogus message(s) initiated from simulated video, computer-generated or other input such as a scenario generator for training purposes.

d. Test. Message(s) are inserted for the purpose of validating connectivity and interoperability of communications components and Command, Control, Communications, Computers and Intelligence (C4I) system(s).

5.6.14.2 OPERATION INDICATOR Field, Requirements.

5.6.14.2.1 The OPERATION INDICATOR Field value shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the operational use of the UDM.

5.6.15 RETRANSMIT INDICATOR Field.

5.6.15.1 RETRANSMIT INDICATOR Field, Description.

5.6.15.1.1 The mandatory RETRANSMIT INDICATOR Field is a 1-bit field indicating whether a UDM is a retransmission.

5.6.15.2 RETRANSMIT INDICATOR Field, Requirements.

5.6.15.2.1 The RETRANSMIT INDICATOR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate whether the UDM is a retransmission.

5.6.16 USER DATA MESSAGE PRECEDENCE Field.

5.6.16.1 USER DATA MESSAGE PRECEDENCE Field, Description.

5.6.16.1.1 The mandatory USER DATA MESSAGE PRECEDENCE Field is used to indicate the precedence of a UDM. The available settings are:

a. ROUTINE. Used for all types of messages that justify transmission by rapid means unless of sufficient urgency to require a higher precedence.

b. PRIORITY. Used for messages that require expeditious action by the addressee(s) and/or furnishes essential information for the conduct of operations in progress when routine precedence will not suffice.

c. IMMEDIATE. Used for messages relating to situations that gravely affect the security of national/allied forces or populace and that require immediate delivery to the addressee(s).

d. FLASH. Used for initial enemy contact messages or operational combat messages of extreme urgency.

e. FLASH OVERRIDE. Used for messages of higher precedence than FLASH.

5.6.16.2 USER DATA MESSAGE PRECEDENCE Field, Requirements.

5.6.16.2.1 The USER DATA MESSAGE PRECEDENCE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the precedence of the UDM.

5.6.17 USER DATA MESSAGE SECURITY CLASSIFICATION Field.

5.6.17.1 USER DATA MESSAGE SECURITY CLASSIFICATION Field, Description.

5.6.17.1.1 The mandatory USER DATA MESSAGE SECURITY CLASSIFICATION Field is used to indicate the security classification of the UDM.

5.6.17.2 USER DATA MESSAGE SECURITY CLASSIFICATION Field, Requirements.

5.6.17.2.1 The USER DATA MESSAGE SECURITY CLASSIFICATION Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the security classification applied to the UDM.

5.6.18 CONTROL/RELEASE MARKING Field.

5.6.18.1 CONTROL/RELEASE MARKING Field, Description.

5.6.18.1.1 The CONTROL/RELEASE MARKING Field is an optional field that supports the exchange of up to 16 country codes. This field may be repeated up to 16 times. The countries listed are those to whom the UDM may be released.

5.6.18.2 CONTROL/RELEASE MARKING Field, Requirements.

5.6.18.2.1 The CONTROL/RELEASE MARKING Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to identify an entity or Country to which the UDM may be released.

5.6.19 YEAR Field.

5.6.19.1 YEAR Field, Description.

5.6.19.1.1 The YEAR Field is used to indicate a year in the Gregorian calendar. Years 1995 to 2094 can be indicated using values 0 to 99 in the YEAR Field. Values 95 to 99 indicate a 20th century year and 0 to 94 indicate a 21st century year.

5.6.19.2 YEAR Field, Requirements.

5.6.19.2.1 The YEAR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate a Gregorian Calendar year number.

5.6.20 MONTH Field.

5.6.20.1 MONTH Field, Description.

5.6.20.1.1 The MONTH Field is used to indicate a month in the Gregorian calendar.

5.6.20.2 MONTH Field, Requirements.

5.6.20.2.1 The MONTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate a month of the Gregorian calendar year.

5.6.21 DAY OF MONTH Field.

5.6.21.1 DAY OF MONTH Field, Description.

5.6.21.1.1 The DAY OF MONTH Field is used to indicate a day of the month in the Gregorian calendar.

5.6.21.2 DAY OF MONTH Field, Requirements.

5.6.21.2.1 The DAY OF MONTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate a day of the month of the Gregorian calendar.

5.6.22 HOUR Field.

5.6.22.1 HOUR Field, Description.

5.6.22.1.1 The HOUR Field is used to indicate an hour of the day. 24 hour clock notation is used.

5.6.22.2 HOUR Field, Requirements.

5.6.22.2.1 The HOUR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate an hour of the day.

5.6.23 MINUTE Field.

5.6.23.1 MINUTE Field, Description.

5.6.23.1.1 The MINUTE Field is used to indicate a minute in the hour.

5.6.23.2 MINUTE Field, Requirements.

5.6.23.2.1 The MINUTE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate a minute of the hour.

5.6.24 SECOND Field.

5.6.24.1 SECOND Field, Description.

5.6.24.1.1 The SECOND Field is used to indicate a second within the minute.

5.6.24.2 SECOND Field, Requirements.

5.6.24.2.1 The SECOND Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate a second of the minute.

5.6.25 DTG EXTENSION Field.

5.6.25.1 DTG EXTENSION Field, Description.

5.6.25.1.1 The DTG EXTENSION Field uses a binary field to uniquely identify UDMs prepared for transmission which have the same ORIGINATOR DATE TIME GROUP Group (G10) date and time values.

5.6.25.2 DTG EXTENSION Field, Requirements.

5.6.25.2.1 The DTG EXTENSION Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to disambiguate between UDMs with the same DTG.

5.6.25.2.2 The DTG EXTENSION Field shall be mandatory when more than one UDM prepared for transmission has the same ORIGINATOR DTG Group (G10) date and time values.

5.6.26 MACHINE ACKNOWLEDGE REQUEST INDICATOR Field.

5.6.26.1 MACHINE ACKNOWLEDGE REQUEST INDICATOR Field, Description.

5.6.26.1.1 The MACHINE ACKNOWLEDGE REQUEST INDICATOR Field is a 1-bit field used to indicate whether the Originator of a UDM requires a Receipt/Compliance Response value 1 (MACHINE RECEIPT) from the Recipient(s), confirming receipt of the UDM.

5.6.26.2 MACHINE ACKNOWLEDGE REQUEST INDICATOR Field, Requirements.

5.6.26.2.1 The MACHINE ACKNOWLEDGE REQUEST INDICATOR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate whether the Originator requires a Receipt/Compliance Response value 2 (MACHINE RECEIPT) confirming receipt of the UDM.

5.6.27 OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field.

5.6.27.1 OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field, Description.

5.6.27.1.1 The OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field is a 1-bit field used to indicate whether the Originator of an UDM requires a Receipt/Compliance Response value 3 (OPERATOR ACKNOWLEDGE) from the Recipient(s), confirming receipt of the UDM.

5.6.27.2 OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field, Requirements.

5.6.27.2.1 The OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate whether the Originator requires a Receipt/Compliance Response value 3 (OPERATOR ACKNOWLEDGE) of UDM receipt.

5.6.28 OPERATOR REPLY REQUEST INDICATOR Field.

5.6.28.1 OPERATOR REPLY REQUEST INDICATOR Field, Description.

5.6.28.1.1 The OPERATOR REPLY REQUEST INDICATOR Field is a 1-bit field used to indicate whether the Originator of an UDM requires a Receipt/Compliance Response from the Recipient(s) indicating the Operator Reply to a UDM.

5.6.28.2 OPERATOR REPLY REQUEST INDICATOR Field, Requirements.

5.6.28.2.1 The OPERATOR REPLY REQUEST INDICATOR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate whether the Originator requires a Receipt/Compliance Response Operator Reply to a UDM.

5.6.29 USER DATA MESSAGE RECEIPT/COMPLIANCE Field.

5.6.29.1 USER DATA MESSAGE RECEIPT/COMPLIANCE Field, Description.

5.6.29.1.1 The USER DATA MESSAGE RECEIPT/COMPLIANCE Field is a 3-bit field that indicates the Recipients ability to receive or comply with a UDM. The available settings are: MACHINE RECEIPT, CANTPRO, OPERATOR ACKNOWLEDGE, WILCO, HAVCO and CANTCO. A MACHINE RECEIPT is automatically generated by a Recipient in response to a Machine Acknowledge request from the Originator to indicate that the Original UDM can be successfully processed at the ultimate destination. A CANTPRO is automatically generated by a Recipient to indicate that an ALPDU or UDM cannot be successfully processed at the ultimate destination. An OPERATOR ACKNOWLEDGE is derived from a positive operator-generated acknowledgment to indicate receipt of a UDM at the ultimate Recipient destination; an OPERATOR ACKNOWLEDGE is only sent by a Recipient. A WILCO is derived from an operator reply that is generated to indicate that a received UDM is understood and that the ultimate Recipient destination will comply with the requirements in or demands of the received UDM. A HAVCO is an operator reply generated to indicate that a received UDM is understood and that the ultimate destination has complied with the requirements in or demands of the received UDM; a HAVCO is only sent by a Recipient. A CANTCO is an operator reply generated to indicate that the requirements in or demands of a received UDM cannot or will not be carried out; a CANTCO is only sent by a Recipient.

5.6.29.2 USER DATA MESSAGE RECEIPT/COMPLIANCE Field, Requirements.

5.6.29.2.1 The USER DATA MESSAGE RECEIPT/COMPLIANCE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the Recipient's ability to comply with the requirements in or demands of a received UDM.

5.6.29.2.2 When the GPI for the ACKNOWLEDGMENT REQUEST Group (G12) in an iteration of the USER DATA MESSAGE HANDLING Group (R3) stimulating a Receipt/Compliance response for a particular UDM is set to value 0 (NOT PRESENT), the only allowable USER DATA MESSAGE RECEIPT/COMPLIANCE Field value for that UDM shall be 2 (CANTPRO).

5.6.30 CANTCO REASON Field.

5.6.30.1 CANTCO REASON Field, Description.

5.6.30.1.1 The CANTCO REASON Field is an optional 3-bit field used to indicate the reason that a Recipient cannot comply with a particular UDM. The field is only used when the USER DATA MESSAGE RECEIPT/COMPLIANCE Field is set to value 6 (CANTCO) by Operator action. When the Operator has selected CANTCO and the optional capability to transmit a CANTCO Reason has been adopted, the Recipient system allows the Operator to select a reason why from those listed in the Data Element Dictionary at Appendix B.

5.6.30.2 CANTCO REASON Field, Requirements.

5.6.30.2.1 If the optional capability to transmit a CANTCO Reason has been adopted, and the system is a Recipient, the Operator shall only be provided with the capability to select a CANTCO Reason with a RECEIPT/COMPLIANCE Response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 6 (CANTCO).

5.6.31 CANTPRO REASON Field.

5.6.31.1 CANTPRO REASON Field, Description.

5.6.31.1.1 The CANTPRO REASON Field is a 6-bit machine-generated field used to indicate the reason that a Recipient cannot process a particular ALPDU or UDM. The field is only used when the system has automatically generated a CANTPRO.

5.6.31.2 CANTPRO REASON Field, Requirements.

5.6.31.2.1 If the optional capability to transmit a CANTPRO Reason has been adopted, and the system is a Recipient, the system shall only invoke the capability when the USER DATA MESSAGE RECEIPT/COMPLIANCE Field is set to value 2 (CANTPRO).

5.6.31.2.2 If the optional capability to transmit a CANTPRO Reason has been adopted, and the system is a Recipient, the CANTPRO REASON Field shall be automatically set to a value as specified by the Data Element Dictionary at Appendix B.

5.6.32 REPLY AMPLIFICATION Field.

5.6.32.1 REPLY AMPLIFICATION Field, Description.

5.6.32.1.1 The REPLY AMPLIFICATION Field is a variable size (up to a maximum of 350 bits) character-coded field. It is used by Recipients to provide amplification of a Receipt/Compliance response with the exception of a CANTPRO or MACHINE RECEIPT (as these are machine-generated responses). The field is divided into 50 7-bit ASCII characters. Special characters are legal.

5.6.32.2 REPLY AMPLIFICATION Field, Requirements.

5.6.32.2.1 When the RECEIPT/COMPLIANCE response value is anything other than value 2 (CANTPRO), the Recipient's Operator shall be provided with the option to amplify the response as specified by the Data Element Dictionary at Appendix B.

5.6.33 USER DATA MESSAGE VERSION Field.

5.6.33.1 USER DATA MESSAGE VERSION Field, Description.

5.6.33.1.1 The USER DATA MESSAGE VERSION Field is a 10-bit binary field that indicates the version of the UDM being transmitted in the User Data portion of the ALPDU. The USER DATA MESSAGE VERSION Field is part of FUTURE USE 6 USER DATA MESSAGE VERSION Group (G15).

5.6.33.2 USER DATA MESSAGE VERSION Field, Requirements.

5.6.33.2.1 The USER DATA MESSAGE VERSION Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the version of the UDM being transmitted in the User Data portion of the ALPDU.

5.6.34 SECURITY PARAMETERS INFORMATION (SPI) Field.

5.6.34.1 SECURITY PARAMETERS INFORMATION (SPI) Field, Description.

5.6.34.1.1 The SECURITY PARAMETER INFORMATION Field is a 4-bit field used to indicate the identities of the parameters and algorithms that enable unambiguous security processing. The field provides for 16 unique security implementations. Security implementations will differ in that all implementation may not provide the same security services or use the same algorithms and parameters. The maximum field sizes are quite large in order to support newer and future cryptographic algorithms and very large key sizes.

5.6.34.2 SECURITY PARAMETERS INFORMATION (SPI) Field, Requirements.

5.6.34.2.1 The SECURITY PARAMETERS INFORMATION Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the parameters and algorithms used to enable unambiguous security processing.

5.6.35 KEYING MATERIAL ID LENGTH Field.

5.6.35.1 KEYING MATERIAL ID LENGTH Field, Description.

5.6.35.1.1 The KEYING MATERIAL ID LENGTH Field is a 3-bit field that defines the size, in octets, of the KEYING MATERIAL ID Field. The KEYING MATERIAL ID LENGTH Field value represents the number of octets in the range of 1 to 8. The KEYING MATERIAL ID LENGTH Field is set to a value equal to the number of octets in the KEYING MATERIAL ID Field minus 1. e.g. a length of 1 octet is represented by value 0 and 2 octets are represented by a value of 1, etc.

5.6.35.2 KEYING MATERIAL ID LENGTH Field, Requirements.

5.6.35.2.1 The KEYING MATERIAL ID LENGTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the length of the KEYING MATERIAL ID Field.

5.6.36 KEYING MATERIAL ID Field.

5.6.36.1 KEYING MATERIAL ID Field, Description.

5.6.36.1.1 The KEYING MATERIAL ID Field is a variable size up to a maximum of 8 octets as specified by the KEYING MATERIAL ID LENGTH Field. The binary field identifies the key, a unique value, which was used for encryption. The use of this field is determined by the value set in the SECURITY PARAMETER INFORMATION Field. It should be noted that the maximum field size is quite large in order to support newer and future cryptographic algorithms and very large key sizes.

5.6.36.2 KEYING MATERIAL ID Field, Requirements.

5.6.36.2.1 The KEYING MATERIAL ID Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the unique key used for encryption.

5.6.37 CRYPTOGRAPHIC INITIALIZATION LENGTH Field.

5.6.37.1 CRYPTOGRAPHIC INITIALIZATION LENGTH Field, Description.

5.6.37.1.1 The CRYPTOGRAPHIC INITIALIZATION LENGTH Field is a 4-bit field that defines the size in 64-bit blocks of the CRYPTOGRAPHIC INITIALIZATION Field.

5.6.37.2 CRYPTOGRAPHIC INITIALIZATION LENGTH Field, Requirements.

5.6.37.2.1 The CRYPTOGRAPHIC INITIALIZATION LENGTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the length of the CRYPTOGRAPHIC INITIALIZATION ID Field.

5.6.38 CRYPTOGRAPHIC INITIALIZATION Field.

5.6.38.1 CRYPTOGRAPHIC INITIALIZATION Field, Description.

5.6.38.1.1 The CRYPTOGRAPHIC INITIALIZATION Field is a variable size up to a maximum of 1024 bits (16 64-bit blocks) as specified by the CRYPTOGRAPHIC INITIALIZATION LENGTH Field. The binary field identifies a sequence of bits used by the Originator and Recipient to initialize the encryption and decryption process. The mechanism that describes how Cryptographic Initialization is achieved, the format of initialization data and the use of this field is determined by the value set in the SECURITY PARAMETER INFORMATION Field.

5.6.38.2 CRYPTOGRAPHIC INITIALIZATION Field, Requirements.

5.6.38.2.1 The CRYPTOGRAPHIC INITIALIZATION Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the sequence of bits used to initialize the encryption and decryption process.

5.6.39 KEY TOKEN LENGTH Field.

5.6.39.1 KEY TOKEN LENGTH Field, Description.

5.6.39.1.1 The KEY TOKEN LENGTH Field is an 8-bit field that defines the size in 64-bit blocks of the KEY TOKEN Field. The KEY TOKEN LENGTH Field value represents the number of 64-bit blocks in the range of 1 to 256 in increments of 1. A key token maybe required for each Originator, Recipient and Information Addressee. The FRI field allows for up to 16 key tokens per UDM.

5.6.39.2 KEY TOKEN LENGTH Field, Requirements.

5.6.39.2.1 The KEY TOKEN LENGTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the length of the KEY TOKEN Field.

5.6.40 KEY TOKEN Field.

5.6.40.1 KEY TOKEN Field, Description.

5.6.40.1.1 The KEY TOKEN Field is a variable size up to a maximum of 16,384 bits (256 64-bit blocks) as specified by the KEY TOKEN LENGTH Field. The binary field contains information which enables the decryption of the User Data associated with the iteration of the USER DATA MESSAGE HANDLING Group (R3) in which the field occurs. The mechanism that describes how Key Tokens are generated, validated, and processed is determined by the value set in the SECURITY PARAMETER INFORMATION Field.

5.6.40.2 KEY TOKEN Field, Requirements.

5.6.40.2.1 The KEY TOKEN Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to enable the Recipient to decrypt the User Data.

5.6.41 AUTHENTICATION DATA (A) LENGTH Field.

5.6.41.1 AUTHENTICATION DATA (A) LENGTH Field, Description.

5.6.41.1.1 The AUTHENTICATION DATA (A) LENGTH Field is a 7-bit field that gives the size in 64-bit blocks of the AUTHENTICATION DATA (A) Field which is used when the SECURITY PARAMETERS INFORMATION Field is set to a value which requires authentication using the Secure Hashing Algorithm Version 1 and the Digital Signature Algorithm (as specified in FIPS 186-4). The AUTHENTICATION DATA (A) LENGTH Field represents the number of 64-bit blocks in the range of 0 to 127 in increments of 1.

5.6.41.2 AUTHENTICATION DATA (A) LENGTH Field, Requirements.

5.6.41.2.1 The AUTHENTICATION DATA (A) LENGTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the length of the AUTHENTICATION DATA (A) Field in 64-Bit blocks.

5.6.42 AUTHENTICATION DATA (A) Field.

5.6.42.1 AUTHENTICATION DATA (A) Field, Description.

5.6.42.1.1 The AUTHENTICATION DATA (A) Field is used when the SECURITY PARAMETERS INFORMATION Field is set to a value which requires authentication using the Secure Hashing Algorithm Version 1 and the Digital Signature Algorithm (as specified in SHA 186-4). The AUTHENTICATION DATA (A) Field is created by the Originator of the UDM. An AUTHENTICATION DATA (A) Field is also generated by the recipient when creating a Signed Acknowledgment Response. It is a variable size up to a maximum of 8,192 bits (128 64-bit blocks) which is reflected in the AUTHENTICATION DATA (A) LENGTH Field. The mechanism that describes how AUTHENTICATION DATA (A) is generated, validated, and processed is determined by the value set in the SECURITY PARAMETERS INFORMATION Field.

5.6.42.1.2 The AUTHENTICATION DATA (A) field provides for data origin authentication, connectionless integrity and non-repudiation with proof of origin. It is generated by digitally signing the hash of both the Application Header and User Data in accordance with FIPS 180-4.

5.6.42.2 AUTHENTICATION DATA (A) Field, Requirements.

5.6.42.2.1 The AUTHENTICATION DATA (A) Field shall be set to a value as specified by the Data Element Dictionary at Appendix B.

5.6.42.2.2 When used, the AUTHENTICATION DATA (A) Field shall be created by the Originator of the UDM to which it refers.

5.6.42.2.3 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), a 160-bit message hash shall be generated using the SHA-1 hashing algorithm, in accordance with FIPS 180-4.

5.6.42.2.4 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the input to the hash shall start with the Least Significant Bit (LSB) of the first field of the Application Header.

5.6.42.2.5 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the input to the 160-bit SHA-1 hash shall end with the last byte of the uncompressed User Data.

5.6.42.2.6 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION)and generating a 160-bit SHA-1 hash, the AUTHENTICATION DATA (A) Field shall be set to 320 zeroes (0).

5.6.42.2.7 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), a 320-bit Digital Signature shall be generated from the 160-bit SHA-1 hash using the Digital Signature Algorithm (DSA) in accordance with FIPS-186-4.

5.6.42.2.8 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) and when multiple UDMs are present, a signature shall be calculated for each UDM for which authentication is desired by digitally signing the hash of both the Application Header and that particular instance of the UDM.

5.6.42.2.9 When generating an AUTHENTICATION DATA (A) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) and a 320-bit Digital Signature has been generated, the AUTHENTICATION DATA (A) Field shall be set to the 320-bit Digital Signature value.

5.6.43 AUTHENTICATION DATA (B) LENGTH Field.

5.6.43.1 AUTHENTICATION DATA (B) LENGTH Field, Description.

5.6.43.1.1 The AUTHENTICATION DATA (B) LENGTH Field is a 7-bit field that gives the size in 64-bit blocks of the AUTHENTICATION DATA (B) Field which is used when the SECURITY PARAMETERS INFORMATION Field is set to a value which requires authentication using the Secure Hashing Algorithm Version 1 and the Digital Signature Algorithm (as specified in SHA 186-4). The AUTHENTICATION DATA (B) LENGTH Field represents the number of 64-bit blocks in the range of 0 to 127 in steps of 1.

5.6.43.2 AUTHENTICATION DATA (B) LENGTH Field, Requirements.

5.6.43.2.1 The AUTHENTICATION DATA (B) LENGTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the length of the AUTHENTICATION DATA (B) Field in 64-Bit blocks.

5.6.43.2.2 When the response being prepared is a Signed Acknowledgment Response and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the AUTHENTICATION DATA (B) LENGTH Field shall be set to value 4 (5 64-bit blocks).

5.6.44 AUTHENTICATION DATA (B) Field.

5.6.44.1 AUTHENTICATION DATA (B) Field, Description.

5.6.44.1.1 The AUTHENTICATION DATA (B) Field is used when the SECURITY PARAMETERS INFORMATION Field is set to a value which requires authentication using the Secure Hashing Algorithm Version 1 and the Digital Signature Algorithm (as specified in SHA 186-4). The AUTHENTICATION DATA (B) Field is created by the party sending the Signed Acknowledgment Response (which also contains the AUTHENTICATION DATA (A) Field created by the Originator of the UDM). The AUTHENTICATION DATA (B) Field is a variable size up to a maximum of 8,192 bits (128 64-bit blocks) which is reflected in the AUTHENTICATION DATA (B) LENGTH Field. The mechanism that describes how AUTHENTICATION DATA (B) is generated, validated, and processed is determined by the value in the SECURITY PARAMETERS INFORMATION Field.

5.6.44.1.2 The AUTHENTICATION DATA (B) field provides for non-repudiation with proof of delivery (Signed Acknowledgment). It is generated by digitally signing the hash of the entire Original ALPDU being acknowledged including the User Data.

5.6.44.1.3 Verification of AUTHENTICATION DATA (B) Fields will be performed in accordance with the DSA (FIPS-186-4) using the Original ALPDU Application Header and User Data. In this case, non-zeroed AUTHENTICATION DATA (A) fields of the Original Application Header are used for the hash calculation.

5.6.44.2 AUTHENTICATION DATA (B) Field, Requirements.

5.6.44.2.1 The AUTHENTICATION DATA (B) Field shall be set to a value as specified by the Data Element Dictionary at Appendix B.

5.6.44.2.2 When generating an AUTHENTICATION DATA (B) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), a 160-bit message hash shall be generated using the SHA-1 hashing algorithm, in accordance with FIPS 180-4.

5.6.44.2.3 When generating an AUTHENTICATION DATA (B) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the input to the 160-bit SHA-1 hash shall start with the LSB of the first field of the Application Header.

5.6.44.2.4 When generating an AUTHENTICATION DATA (B) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the input to the 160-bit SHA-1 hash shall end with the last byte of the uncompressed UDM.

5.6.44.2.5 When generating an AUTHENTICATION DATA (B) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), a 320-bit Digital Signature shall be generated from the 160-bit SHA-1 hash using the Digital Signature Algorithm (DSA) in accordance with FIPS-186-4.

5.6.44.2.6 When generating an AUTHENTICATION DATA (B) Field value and the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) and a 320-bit Digital Signature has been generated, the AUTHENTICATION DATA (B) Field shall be set to the 320-bit Digital Signature value.

5.6.45 SIGNED ACKNOWLEDGE REQUEST INDICATOR Field.

5.6.45.1 SIGNED ACKNOWLEDGE REQUEST INDICATOR Field, Description.

5.6.45.1.1 The SIGNED ACKNOWLEDGE REQUEST INDICATOR Field is a 1-bit field indicating whether the Originator of a UDM requires a signed response from the Recipient.

5.6.45.2 SIGNED ACKNOWLEDGE REQUEST INDICATOR Field, Requirements.

5.6.45.2.1 The SIGNED ACKNOWLEDGE REQUEST INDICATOR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate whether the Originator requires a signed response from a Recipient.

5.6.46 USER DATA MESSAGE SECURITY PADDING LENGTH Field.

5.6.46.1 USER DATA MESSAGE SECURITY PADDING LENGTH Field, Description.

5.6.46.1.1 The USER DATA MESSAGE SECURITY PADDING LENGTH Field is an 8-bit binary field whose value defines the size in octets, of the USER DATA MESSAGE SECURITY PADDING Field. The USER DATA MESSAGE SECURITY PADDING LENGTH Field value represents the number of octets in the range of 0 to 255.

5.6.46.2 USER DATA MESSAGE SECURITY PADDING LENGTH Field, Requirements.

5.6.46.2.1 The USER DATA MESSAGE SECURITY PADDING LENGTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to indicate the size of the USER DATA MESSAGE SECURITY PADDING Field in Octets.

5.6.47 USER DATA MESSAGE SECURITY PADDING Field.

5.6.47.1 USER DATA MESSAGE SECURITY PADDING Field, Description.

5.6.47.1.1 The USER DATA MESSAGE SECURITY PADDING Field is a variable size up to a maximum of 2040 bits (255 octets) as specified by the USER DATA MESSAGE SECURITY PADDING LENGTH Field. The Message Security Padding is necessary for a block encryption algorithm to ensure that the UDM content to be encrypted is a multiple of the encryption block length. The message security padding rules are specified by the value of the SECURITY PARAMETERS INFORMATION Field.

5.6.47.2 USER DATA MESSAGE SECURITY PADDING Field, Requirements.

5.6.47.2.1 The USER DATA MESSAGE SECURITY PADDING Field shall be set to a value as specified by the Data Element Dictionary at Appendix B, to ensure that the UDM to be encrypted is a multiple of the encryption block length.

5.6.48 HEADER ZERO PADDING Field.

5.6.48.1 HEADER ZERO PADDING Field, Description.

5.6.48.1.1 The Application Header is always a multiple of 8 bits to facilitate processing. If an Application Header is less than a multiple of 8 bits when created, it is zero-filled until it becomes a multiple of 8 bits. This padding allows the User Data portion of the ALPDU to start on a byte boundary.

5.6.48.2 HEADER ZERO PADDING Field, Requirements.

5.6.48.2.1 If an Application Header is created and is not a multiple of 8 bits, zeroes shall be added to the end of the Application Header, as specified by the Data Element Dictionary at Appendix B, until the resultant Application Header is a multiple of 8 bits.

5.7 Group Processing.

5.7.1 ORIGINATOR, RECIPIENT, and INFORMATION ADDRESS Groups (G1, G2 and G3).

5.7.1.1 ORIGINATOR, RECIPIENT, and INFORMATION ADDRESS Group, Description.

5.7.1.1.1 The Originator, Recipient and Information Addressees can be person(s), units(s), platform(s) or process(es). Each group contains a URN Field, a UNIT NAME Field and associated FPIs. The use of the information in the ORIGINATOR, RECIPIENT, AND INFORMATION ADDRESSEE Group Fields depends on the Recipient (person(s), units(s), Platform(s) or process(es)). It should be noted that Information Addressees do not participate in Receipt/Compliance processing and use the information received for awareness only.

5.7.1.2 ORIGINATOR, RECIPIENT, and INFORMATION ADDRESS Group, Requirements.

5.7.1.2.1 When used, the ORIGINATOR ADDRESS Group (G1) Fields shall contain the address of the ALPDU Originator.

5.7.1.2.2 When used, the RECIPIENT ADDRESS Group (G2) Fields shall contain the address(es) of the intended Recipient(s) of the ALPDU.

5.7.1.2.3 When used, the INFORMATION ADDRESS Group (G3) Fields shall contain the address(es) of the intended Information Addressee(s).

5.7.1.2.4 The maximum total number of Recipient and Information Addressees in a single ALPDU shall be 16.

5.7.1.2.5 If the RECIPIENT ADDRESS Group (G2) GPI is set to value 0 (NOT PRESENT) and the INFORMATION ADDRESS Group (G3) GPI is set to value 0 (NOT PRESENT), the ALPDU shall be broadcast in accordance with lower layer broadcast protocols.

5.7.2 FUTURE USE Groups (G4-G8, G15-G19 and G27-G31).

5.7.2.1 FUTURE USE Group, Description.

5.7.2.1.1 Prior to MIL-STD-2045-47001D, the addition of new fields to the Application Header meant that earlier versions might not be compatible. FUGs were introduced into MIL-STD-2045-47001D to allow future Application Header expansion without changing the basic Application Header structure. The FUG approach therefore means that the non-FUG Groups and Fields as reflected in MIL-STD-2045-47001D (and newer versions) form an enduring capability thus facilitating backwards compatibility.

5.7.2.1.2 Each FUG has a mandatory GPI to specify if the Sub-groups or Fields within the Group (if defined) are present in an iteration of the Application Header and a related conditional 12-bit GROUP SIZE Field that indicates the size of the group minus the GROUP SIZE Field when data is present in the group i.e. the FUG GPI is set to value 1 (PRESENT). This means that when System A, which has implemented a version of MIL-STD-2045-47001 from versions D onwards, receives an Application Header from a system implemented to a newer version and that Application Header has data in a FUG that was not defined at the version implemented by System A, System A will be able to determine how much "unknown" data is present and can account for it. In effect, System A will be able to count the bits of "unknown" data and discard them with no further processing. A GROUP SIZE Field is also present in all FUG Sub-groups to allow the same "count and discard" approach to be applied.

5.7.2.1.3 While FUGs were created in MIL-STD-2045-47001D, no contents for any of them were defined in that version (or in D w/Change 1). The GPI for all FUGs will therefore be set to value 0 (NOT PRESENT) on transmission for systems implementing MIL-STD-2045-47001D and D w/CHANGE 1.

5.7.2.2 FUTURE USE Group, Structure Requirements.

5.7.2.2.1 Each sub-group within a primary FUG shall be identified by a GPI.

5.7.2.2.2 The GPI of a sub-group within a primary FUG shall be followed by a GROUP SIZE Field.

5.7.2.2.3 The total size of any FUG, including all sub-groups, shall be limited to a maximum size of 4095 bits.

5.7.2.3 FUTURE USE Group, Processing Requirements.

5.7.2.3.1 When the GPI of a FUG is set to value 1 (PRESENT) in a received Application Header and the structure of that FUG was not defined in the version of MIL-STD-2045-47001 implemented by the Addressee, the number of bits of data as indicated in the FUG GROUP SIZE Field and immediately following that Field shall be discarded without further processing.

5.7.2.3.2 When the GPI of a FUG Sub-group is set to value 1 (PRESENT) in a received Application Header and the structure of that FUG Sub-group was not defined in the version of MIL-STD-2045-47001 implemented by the Addressee, the number of bits of data as indicated in the FUG Sub-group GROUP SIZE Field and immediately following that Field shall be discarded without further processing.

5.7.3 VMF MESSAGE IDENTIFICATION Group (G9).

5.7.3.1 VMF MESSAGE IDENTIFICATION Group, Description.

5.7.3.1.1 The VMF MESSAGE IDENTIFICATION Group is used when the UDMF is VMF. The group contains a FUNCTIONAL AREA DESIGNATOR Field, a MESSAGE NUMBER Field, and a VMF MESSAGE SUBTYPE Field the presence of which is controlled by an FPI. A combination of the FAD Field and the MESSAGE NUMBER Field identifies the VMF message present as User Data and the VMF MESSAGE SUBTYPE Field value, when used, matches the VMF K Series Message Case number.

5.7.3.2 VMF MESSAGE IDENTIFICATION Group, Requirements.

5.7.3.2.1 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 0 (NOT PRESENT) when the UDMF Field is set to value 0 (LINK 16) in an ALPDU prepared for transmission.

5.7.3.2.2 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 0 (NOT PRESENT) when the UDMF Field is set to value 1 (BINARY) in an ALPDU prepared for transmission.

5.7.3.2.3 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 1 (PRESENT) when the UDMF Field is set to value 2 (VARIABLE MESSAGE FORMAT (VMF)) in an ALPDU prepared for transmission.

5.7.3.2.4 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 0 (NOT PRESENT) when the UDMF Field is set to value 3 (NITFS) in an ALPDU prepared for transmission.

5.7.3.2.5 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 0 (NOT PRESENT) when the UDMF Field is set to value 4 (REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT) in an ALPDU prepared for transmission.

5.7.3.2.6 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 0 (NOT PRESENT) when the UDMF Field is set to value 5 (USMTF) in an ALPDU prepared for transmission.

5.7.3.2.7 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 0 (NOT PRESENT) when the UDMF Field is set to value 7 (EXTENSIBLE MARKUP LANGUAGE MESSAGE TEXT FORMAT (XML-MTF)) in an ALPDU prepared for transmission.

5.7.3.2.8 The GPI for the VMF MESSAGE IDENTIFICATION Group (G9) shall be set to value 1 (PRESENT) when the USER DATA MESSAGE FORMAT Field is set to value 8 (VARIABLE MESSAGE FORMAT MARKUP LANGUAGE (VML)) in an ALPDU prepared for transmission.

5.7.3.2.9 When sending a Receipt Compliance response to a received UDM with the USER DATA MESSAGE FORMAT Field set to value 2 (VARIABLE MESSAGE FORMAT (VMF)), the VMF MESSAGE IDENTIFICATION Group (G9) values for that particular UDM shall be the same as those in the received UDM spawning the response.

5.7.3.2.10 When sending a RECEIPT/COMPLIANCE response to a received UDM with the USER DATA MESSAGE FORMAT Field set to value 8 (VARIABLE MESSAGE FORMAT MARKUP LANGUAGE (VML)), the VMF MESSAGE IDENTIFICATION Group (G9) values for that particular UDM shall be the same as those in the received UDM spawning the response.

5.7.4 ORIGINATOR DTG Group (G10).

5.7.4.1 ORIGINATOR DTG Group, Description.

5.7.4.1.1 The fields within the ORIGINATOR DATE TIME GROUP Group (G10) express the date and time at which the UDM was prepared for transmission. The time is expressed in Universal Time Coordinated (UTC) Time. The group contains fields for year, month, day, hour, minute, and seconds, and a DTG Extension Field.

5.7.4.2 ORIGINATOR DTG Group, Requirements.

5.7.4.2.1 The time information within the Originator DTG Group (G10) shall be expressed in Universal Time Coordinated (UTC) time.

5.7.4.2.2 The ORIGINATOR DATE TIME GROUP Group (G10) YEAR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the year that the UDM was prepared for transmission.

5.7.4.2.3 The ORIGINATOR DATE TIME GROUP Group (G10) MONTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the month that the UDM was prepared for transmission.

5.7.4.2.4 The ORIGINATOR DATE TIME GROUP Group (G10) DAY OF MONTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the day that the UDM was prepared for transmission.

5.7.4.2.5 The ORIGINATOR DATE TIME GROUP Group (G10) HOUR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the hour that the UDM was prepared for transmission.

5.7.4.2.6 The ORIGINATOR DATE TIME GROUP Group (G10) MINUTE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the minute that the UDM was prepared for transmission.

5.7.4.2.7 The ORIGINATOR DATE TIME GROUP Group (G10) SECOND Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the second that the UDM was prepared for transmission.

5.7.5 PERISHABILITY DTG Group (G11).

5.7.5.1 PERISHABILITY DTG Group, Description.

5.7.5.1.1 The PERISHABILITY DATE TIME GROUP Group (G11) provides the latest date and time that the User Data associated with it is still of value. Its use ensures that received UDMs that are too old based on the Perishability DATE TIME GROUP Group (G11) are discarded without further processing. It is also used to prevent data which is considered to be stale from being transmitted.

5.7.5.2 PERISHABILITY DTG Group, Requirements.

5.7.5.2.1 The time information within the PERISHABILITY DATE TIME GROUP Group (G11) shall be expressed in Universal Time Coordinated time.

5.7.5.2.2 Only when the time information in the PERISHABILITY DATE TIME GROUP Group (G11) is in the future shall associated User Data be released for transmission.

5.7.5.2.3 The PERISHABILITY DATE TIME GROUP Group (G11) YEAR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the last year that the UDM is valid.

5.7.5.2.4 The PERISHABILITY DATE TIME GROUP Group (G11) MONTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the last month that the UDM is valid.

5.7.5.2.5 The PERISHABILITY DATE TIME GROUP Group (G11) DAY OF MONTH Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the last day that the UDM is valid.

5.7.5.2.6 The PERISHABILITY DATE TIME GROUP Group (G11) HOUR Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the last hour that the UDM is valid.

5.7.5.2.7 The PERISHABILITY DATE TIME GROUP Group (G11) MINUTE Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the last minute that the UDM is valid.

5.7.5.2.8 The PERISHABILITY DATE TIME GROUP Group (G11) SECOND Field shall be set to a value as specified by the Data Element Dictionary at Appendix B reflect the last second that the UDM is valid.

5.7.6 ACKNOWLEDGMENT REQUEST Group (G12).

5.7.6.1 ACKNOWLEDGMENT REQUEST Group (G12), Description.

5.7.6.1.1 The ACKNOWLEDGMENT REQUEST Group (G12) is used to indicate that the Originator of a UDM requires a Machine Acknowledge or an Operator Acknowledge or an Operator Reply from the Recipient. The fields are mutually exclusive; only one form of Receipt/Compliance response can be requested.

5.7.6.2 ACKNOWLEDGMENT REQUEST Group (G12), Requirements.

5.7.6.2.1 Only one of the ACKNOWLEDGMENT REQUEST Group (G12) Fields shall be set to value 1 (REQUIRED) in an iteration of the Group prepared for transmission.

5.7.7 RESPONSE DATA Group (G13).

5.7.7.1 RESPONSE DATA Group (G13), Description.

5.7.7.1.1 The function of the RESPONSE DATA Group (G13) is to provide a Receipt/Compliance response to an Acknowledgment or Reply request or to inform the Originator of a UDM that it cannot be processed by the Recipient. The UDM in question is identified by replicating the related ORIGINATOR DATE TIME GROUP Group (G10) data (including the DATE TIME GROUP EXTENSION Field value if one is used) from the received ALPDU into the RESPONSE DATA Group (G13) and using the ORIGINATOR ADDRESS Group (G1) from the received ALPDU to define the RECIPIENT ADDRESS Group (G2) in the Receipt/Compliance response.

5.7.7.2 RESPONSE DATA Group (G13), Requirements.

5.7.7.2.1 The RESPONSE DATA Group (G13) YEAR Field shall be set to the value from the ORIGINATOR DATE TIME GROUP Group (G10) YEAR Field in the UDM being acknowledged.

5.7.7.2.2 The RESPONSE DATA Group (G13) MONTH Field shall be set to the value from the ORIGINATOR DATE TIME GROUP Group (G10) MONTH Field in the UDM being acknowledged.

5.7.7.2.3 The RESPONSE DATA Group (G13) DAY OF MONTH Field shall be set to the value from the ORIGINATOR DATE TIME GROUP Group (G10) DAY OF MONTH Field in the UDM being acknowledged.

5.7.7.2.4 The RESPONSE DATA Group (G13) HOUR Field shall be set to the value from the ORIGINATOR DATE TIME GROUP Group (G10) HOUR Field in the UDM being acknowledged.

5.7.7.2.5 The RESPONSE DATA Group (G13) MINUTE Field shall be set to the value from the ORIGINATOR DATE TIME GROUP Group (G10) MINUTE Field in the UDM being acknowledged.

5.7.7.2.6 The RESPONSE DATA Group (G13) SECOND Field shall be set to the value from the ORIGINATOR DATE TIME GROUP Group (G10) SECOND Field in the UDM being acknowledged.

5.7.7.2.7 If the ORIGINATOR DATE TIME GROUP Group (G10) DATA TIME GROUP EXTENSION Field is present in the iteration of the USER DATA MESSAGE HANDLING Group (R3) specifying the UDM being acknowledged, it shall be reproduced in the RESPONSE DATA Group (G13) DATE TIME GROUP EXTENSION Field of the Receipt/Compliance response.

5.7.8 REFERENCE USER DATA MESSAGE DATA Group (G14).

5.7.8.1 REFERENCE USER DATA MESSAGE DATA Group (G14), Description.

5.7.8.1.1 The REFERENCE USER DATA MESSAGE DATA Group (G14) is used to reference existing UDMs that are related to a subject UDM. The UDM being referred to is a UDM which is identified by replicating the ORIGINATOR ADDRESS Group (G1) and ORIGINATOR DATE TIME GROUP Group (G10) from the iteration of the USER DATA MESSAGE HANDLING Group (R3) relating to the reference UDM into this Group.

5.7.8.2 REFERENCE USER DATA MESSAGE DATA Group (G14), Requirements.

5.7.8.2.1 The REFERENCE USER DATA MESSAGE DATA Group (G14) URN Field shall be set to the value of the ORIGINATOR ADDRESS Group (G1) URN Field from the UDM being referred to, if present.

5.7.8.2.2 The REFERENCE USER DATA MESSAGE DATA Group (G14) UNIT NAME Field shall be set to the value of the ORIGINATOR ADDRESS Group (G1) UNIT NAME Field from the UDM being referred to, if present.

5.7.8.2.3 The REFERENCE USER DATA MESSAGE DATA Group (G14) YEAR Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) UNIT NAME Field from the UDM being referred to.

5.7.8.2.4 The REFERENCE USER DATA MESSAGE DATA Group (G14) MONTH Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) MONTH Field from the UDM being referred to.

5.7.8.2.5 The REFERENCE USER DATA MESSAGE DATA Group (G14) DAY OF MONTH Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) DAY OF MONTH Field from the UDM being referred to.

5.7.8.2.6 The REFERENCE USER DATA MESSAGE DATA Group (G14) HOUR Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) HOUR Field from the UDM being referred to.

5.7.8.2.7 The REFERENCE USER DATA MESSAGE DATA Group (G14) MINUTE Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) MINUTE Field from the UDM being referred to.

5.7.8.2.8 The REFERENCE USER DATA MESSAGE DATA Group (G14) SECOND Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) SECOND Field from the UDM being referred to.

5.7.8.2.9 The REFERENCE USER DATA MESSAGE DATA Group (G14) DATE TIME GROUP EXTENSION Field shall be set to the value of the ORIGINATOR DATE TIME GROUP Group (G10) DATE TIME GROUP EXTENSION Field from the UDM being referred to, if present.

5.7.9 USER DATA MESSAGE SECURITY Group (G20).

5.7.9.1 USER DATA MESSAGE SECURITY Group (G20), Description.

5.7.9.1.1 The USER DATA MESSAGE SECURITY Group (G20) is complex with a considerable number of nested groups. The function of the Group is to define the settings in use when the one of the security parameter schemes defined by the values in the SECURITY PARAMETERS INFORMATION Field in the Data Element Dictionary at Appendix B is invoked. The Group is mandatory if a security parameter scheme is to be used to provide security services to the Application Layer, albeit some of the nested Groups may not be required.

5.7.9.2 USER DATA MESSAGE SECURITY Group (G20), Requirements.

5.7.9.2.1 For systems implementing one or more security parameter schemes defined by the values in the SECURITY PARAMETERS INFORMATION Field in the Data Element Dictionary at Appendix B, the USER DATA MESSAGE SECURITY Group (G20) GPI shall be set to value 1 (PRESENT) when a security parameter scheme is in use.

5.7.9.2.2 If an ALPDU is received with a USER DATA MESSAGE SECURITY Group (G20) GPI set to value 1 (PRESENT) and the Recipient does not implement any of the security parameter schemes defined by the values in the SECURITY PARAMETERS INFORMATION Field, a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be sent to the Originator for the UDM to which the USER DATA MESSAGE SECURITY Group (G20) refers.

5.7.9.2.3 If an ALPDU is received with a USER DATA MESSAGE SECURITY Group (G20) GPI set to value 1 (PRESENT) and the Addressee does not implement any of the security parameter schemes defined by the values in the SECURITY PARAMETERS INFORMATION Field, the ALPDU shall be discarded without further processing.

5.7.9.2.4 If an ALPDU is received with a SECURITY PARAMETERS INFORMATION Field set to a value that the Recipient does not implement, a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be sent to the Originator for the UDM to which the USER DATA MESSAGE SECURITY Group (G20) refers.

5.7.9.2.5 If an ALPDU is received with a SECURITY PARAMETERS INFORMATION Field set to a value that the Addressee does not implement, the ALPDU shall be discarded without further processing.

5.7.9.2.6 If an ALPDU is received with a SECURITY PARAMETERS INFORMATION Field set to a value that the Recipient does not implement, the CANTPRO REASON Field of the Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be set to value 30 (DO NOT SUPPORT THIS SPI VALUE).

5.7.9.2.7 If an ALPDU is received with a SECURITY PARAMETERS INFORMATION Field set to a value that the Addressee does not implement, the ALPDU shall be discarded without further processing.

5.7.9.3 KEYING MATERIAL Group (G21).

5.7.9.3.1 KEYING MATERIAL Group (G21), Description.

5.7.9.3.1.1 The KEYING MATERIAL Group (G21) includes the KEYING MATERIAL ID Field and a related KEYING MATERIAL ID LENGTH Field. The Group is associated with the provision of encryption.

5.7.9.3.2 KEYING MATERIAL Group (G21), Requirements.

5.7.9.3.2.1 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the KEYING MATERIAL Group (G21) shall be set to value 0 (NOT PRESENT).

5.7.9.4 CRYPTOGRAPHIC INITIALIZATION Group (G22).

5.7.9.4.1 CRYPTOGRAPHIC INITIALIZATION Group (G22), Description.

5.7.9.4.1.1 The CRYPTOGRAPHIC INITIALIZATION Group (G22) includes a CRYPTOGRAPHIC INITIALIZATION Field and an associated CRYPTOGRAPHIC INITIALIZATION LENGTH Field.

5.7.9.4.2 CRYPTOGRAPHIC INITIALIZATION Group (G22), Requirements.

5.7.9.4.2.1 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the CRYPTOGRAPHIC INITIALIZATION Group (G22) shall be set to value 0 (NOT PRESENT).

5.7.9.5 KEY TOKEN Group (G23).

5.7.9.5.1 KEY TOKEN Group (G23), Description.

5.7.9.5.1.1 The KEY TOKEN Group (G23) includes a repeatable KEY TOKEN Field and a related KEY TOKEN LENGTH Field. The Group is associated with the provision of encryption.

5.7.9.5.2 KEY TOKEN Group (G23), Requirements.

5.7.9.5.2.1 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the KEY TOKEN Group (G23) shall be set to value 0 (NOT PRESENT).

5.7.9.6 AUTHENTICATION (A) Group (G24).

5.7.9.6.1 AUTHENTICATION (A) Group (G24), Description.

5.7.9.6.1.1 The AUTHENTICATION (A) Group (G24) includes the AUTHENTICATION DATA (A) Field which is used as the basis for an authenticated response. The block also contains AUTHENTICATION DATA (A) LENGTH Field which is eponymous and facilitates processing.

5.7.9.6.2 AUTHENTICATION (A) Group (G24), Requirements.

5.7.9.6.2.1 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the AUTHENTICATION (A) Group (G24) shall be set to value 1 (PRESENT).

5.7.9.7 AUTHENTICATION (B) Group (G25).

5.7.9.7.1 AUTHENTICATION (B) Group (G25), Description.

5.7.9.7.1.1 The AUTHENTICATION (B) Group (G25) includes the AUTHENTICATION DATA (B) Field which is based on the AUTHENTICATION DATA (A) Field and forms the authenticated response when a Signed Acknowledgment is requested. The block also contains the AUTHENTICATION DATA (B) LENGTH Field which is eponymous and facilitates processing.

5.7.9.7.2 AUTHENTICATION (B) Group (G25), Requirements.

5.7.9.7.2.1 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) and the response is not a Signed Acknowledgment Response, the GPI for the AUTHENTICATION (B) Group (G25) shall be set to value 0 (NOT PRESENT).

5.7.9.7.2.2 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) and the response is a Signed Acknowledgment Response, the GPI for the AUTHENTICATION (B) Group (G25) shall be set to value 1 (PRESENT).

5.7.9.8 USER DATA MESSAGE SECURITY PADDING Group (G26).

5.7.9.8.1 USER DATA MESSAGE SECURITY PADDING Group (G26), Description.

5.7.9.8.1.1 The USER DATA MESSAGE SECURITY PADDING Group (G26) is associated with encryption and includes the USER DATA MESSAGE SECURITY PADDING Field which is used to ensure that the UDM content to be encrypted is a multiple of the encryption block length. The Group also contains the associated USER DATA MESSAGE SECURITY PADDING LENGTH Field which is eponymous and facilitates processing.

5.7.9.8.2 USER DATA MESSAGE SECURITY PADDING Group (G26), Requirements.

5.7.9.8.2.1 When the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the USER DATA MESSAGE SECURITY PADDING Group (G26) shall be set to value 0 (NOT PRESENT).

5.8 Application Header Cases, Conditions, Expected Responses and Special Considerations.

5.8.1 Application Header Cases, Conditions, Expected Responses and Special Considerations, Description.

5.8.1.1 Case Description.

5.8.1.1.1 Case statements are a form of expressing a Condition. The construct in this document indicates there are at least two alternatives. Case statements are used when a condition statement becomes too complex. A case statement may include an "XOR" (Exclusive OR) operator when it is possible to accomplish the same purpose in one or more ways. A case statement may also include an "OR" operator when any, or all, of several data elements can be used. Unlike Cases in MIL-STD-6017, Cases in MIL-STD-2045-47001 are not mutually exclusive and may be used together as required by the nature of the data being transmitted.

5.8.1.2 Condition Description

5.8.1.2.1 Condition statements define the conditions under which a data group, data element, or value in a data element may be used. The Condition statement is very structured in its use. The following is an example of the format of a conditional statement:

```
IF (condition)
     THEN (Sequence of Statements)
ELSIF (condition)
     THEN (Sequence of Statements)
ELSE (Sequence of Statements)
ENDIF
```

5.8.1.2.2 For the execution of an "IF" statement, the condition specified after "IF", and any conditions specified after other keywords are evaluated in succession until one evaluates to "TRUE", or all conditions are evaluated and yield "FALSE". If one condition evaluates to "TRUE", then the corresponding sequence of statements are executed. If all conditions evaluate to "FALSE" and an "ELSE" statement is present, the sequence of statements associated with the "ELSE" are executed; otherwise, none of the sequence statements are executed

5.8.1.3 Defaults, Description.

5.8.1.3.1 Defaults will be defined only if the Addressee system’s default value is of concern to the interface.

5.8.1.4 Expected Responses, Description.

5.8.1.4.1 The expected response by the Recipient of an Application Header will depend on the content of the Application Header fields and is stated as it relates to the case and conditionality statements for the Application Header. It should be noted that expected responses are not transmitted by Information Addressees.

5.8.1.5 Special Considerations, Description.

5.8.1.5.1 Special considerations cover those exceptions that cannot be defined under the preceding paragraphs.

5.8.1.6 Syntax, Description.

5.8.1.6.1 The purpose of the Case and Conditionality statements is to rigorously and unambiguously define the construction rules for the Application Header so that it will be possible to achieve consistent construct implementations across multiple systems. They include cases for each use of the Application Header and the inter-element conditionalities within the Application Header for basic processing, defaults, legal entries, and special considerations.

5.8.1.7 Logical Operators, Description.

5.8.1.7.1 Natural language does not lend itself to rigorous and unambiguous expression, therefore it is necessary to use well established logical operators to establish precise, mathematical meaning for logical relationships. The logical operators that will be used in this document are:

a. AND - separates two discrete values and evaluates to true if both of the discrete values are true.

b. OR - inclusive OR separates two discrete values and evaluates to true if at least one of the discrete conditions is true.

c. XOR - exclusive OR separates two discrete values and evaluates to true if and only if one, not both, of the discrete conditions is true.

d. NOT - a simple negation of the condition so that if A is true then NOT A would yield false.

5.8.1.7.2 TABLE VI illustrates the meaning of the logical operator definitions given above. The TABLE shows, for example, that given both "A" and "B" as true, then "NOT A" will yield false. "A AND B" will yield true, "A OR B" will yield true, and "A XOR B" will yield false. "A AND B" in this example represents names or action designators.

TABLE VI. Logical Operator Definitions

A	B	NOT A	A AND B	A OR B	A XOR B
TRUE	TRUE	FALSE	TRUE	TRUE	FALSE
TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
FALSE	TRUE	TRUE	FALSE	TRUE	TRUE
FALSE	FALSE	TRUE	FALSE	FALSE	FALSE

5.8.1.8 Application, Description.

5.8.1.8.1 Case and Conditionality statements are used only to restrict the structure of the Application Header to a well-defined subset of the possible legal configurations that are specified by the application rules of Application Header construction.

5.8.1.9 Reserved Words, Description.

5.8.1.9.1 Case statements reserved words that will be used in this document are:

a. CASE - Identifies the title (purpose) under which the statement is defined.

b. END CASE - Ends the case statement.

c. IF...THEN...ELSE - Describes conditions under which statements are valid. The statement always starts with "IF" and ends with "ENDIF". An "IF" statement selects for execution, one or none of the enclosed sequence of statements depending on the (truth) value of one or more corresponding conditions.

d. ELSIF - This keyword is used to extend the flexibility of the "IF...THEN...ELSE" construct. It is used when multiple conditions need to be evaluated in order to determine a logic path. Multiple "ELSIF" conditions are permitted. The general form is:

```
IF condition THEN sequence of statements
ELSIF condition THEN sequence of statements
ELSE sequence of statements
ENDIF
```

e. ENDIF - Ends condition statement.

5.8.2 Application Header Cases, Conditions, Expected Responses and Special Considerations Syntax and Procedures.

5.8.2.1 The syntax and procedures expressed below are applied in the formatting and construction of the Application Header.

5.8.3 Case 1: Original Application Layer Protocol Data Unit.

5.8.3.1 Case 1: Original Application Layer Protocol Data Unit, Description.

5.8.3.1.1 This case is used when transmitting Original ALPDUs containing User Data.

5.8.3.2 Case 1: Original Application Layer Protocol Data Unit, Requirements.

5.8.3.2.1 An Original ALPDU shall contain User Data.

5.8.3.2.2 An Original ALPDU shall have the GPI for ORIGINATOR ADDRESS Group (G1) set to value 1 (PRESENT).

5.8.3.2.3 An Original ALPDU shall have the GPI for RESPONSE DATA Group (G13) set to value 0 (NOT PRESENT).

5.8.3.3 Case 1: Original Application Layer Protocol Data Unit, Pseudocode.

```
THIS CASE REQUIRES
       GPI for ORIGINATOR ADDRESS Group (G1) set to value 1
            (PRESENT)
       GPI for RESPONSE DATA Group (G13) set to value 0 (NOT
            PRESENT)
       AND   User Data is present
END CASE
```

5.8.4 Case 2: Receipt/Compliance Response.

5.8.4.1 Case 2: Receipt/Compliance Response, Description.

5.8.4.1.1 This Case is used when transmitting a Receipt/Compliance response to a UDM within a received ALPDU. The need for a response will be stimulated by the presence of the ACKNOWLEDGMENT REQUEST Group (G12) in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within the Original ALPDU. An Originator may ask for an automatic machine-generated response to indicate UDM receipt and the ability to process it, an operator acknowledgment that the UDM has been received and processed, or an indication as to the Recipient's intention with respect to the content of the UDM (usually a command) using an operator generated reply.

5.8.4.1.2 A request for a Receipt/Compliance response is only actioned by Recipients of the Original ALPDU; Information Addressees do not respond. Similarly, a Receipt/Compliance response is only addressed to the Originator of the Original ALPDU which stimulates the response; there are no Information Addressees to a Receipt/Compliance response.

5.8.4.1.3 The other circumstance in which this Case is stimulated is when no Receipt/Compliance response has been requested but a UDM within a received ALPDU or the entire ALPDU cannot be processed by a Recipient. In this instance, the ACKNOWLEDGMENT REQUEST Group (G12) will not be present but a Receipt/Compliance response is sent to the Originator of the stimulating UDM or ALPDU with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO).

5.8.4.2 Case 2: Receipt/Compliance Response, Requirements.

5.8.4.2.1 The ORIGINATOR ADDRESS Group (G1) values in a Receipt/Compliance response shall be set to those for the Recipient in the RECIPIENT ADDRESS Group (G2) of the Original ALPDU.

5.8.4.2.2 The RECIPIENT ADDRESS Group (G2) values in the Receipt/Compliance response shall be set to those in the ORIGINATOR ADDRESS Group (G1) of the Original ALPDU.

5.8.4.2.3 A Receipt/Compliance response shall have the GPI for the PERISHABILITY DATE TIME GROUP Group (G11) set to value 0 (NOT PRESENT).

5.8.4.2.4 A Receipt/Compliance response shall have the GPI for the ACKNOWLEDGMENT REQUEST Group (G12) set to value 0 (NOT PRESENT).

5.8.4.2.5 A Receipt/Compliance response shall have the GPI for the RESPONSE DATA Group (G13) set to value 1 (PRESENT).

5.8.4.2.6 No User Data shall be present in a Receipt/Compliance response.

5.8.4.2.7 Receipt/Compliance responses shall only be transmitted by an addressee in the RECIPIENT ADDRESS Group (G2) within the original ALPDU.

5.8.4.3 Case 2: Receipt/Compliance Response, Pseudocode.

```
THIS CASE REQUIRES
       ORIGINATOR ADDRESS Group (G1) values in a
            Receipt/Compliance response match those for the
            Recipient in the Original ALPDU RECIPIENT ADDRESS
            Group (G2)
       AND  RECIPIENT ADDRESS Group (G2) values in
            Receipt/Compliance response match those in the
            Original ALPDU ORIGINATOR ADDRESS Group (G1)
       AND  GPI for PERISHABILITY DATE TIME GROUP Group (G11) set
            to value 0 (NOT PRESENT)
       AND  GPI for ACKNOWLEDGMENT REQUEST Group (G12) set to
            value 0 (NOT PRESENT)
       AND  GPI for RESPONSE DATA Group (G13) set to value 1
            (PRESENT)
       AND  User Data is not present
 END CASE
```

5.8.5 Case 3: Signed Acknowledgment Response.

5.8.5.1 Case 3: Signed Acknowledgment Response, Description.

5.8.5.1.1 This Case is used by a Recipient when creating a Signed Acknowledgment Response in response to a request for one using the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field. Use of this Case demands that the security parameters scheme being used (as indicated by the setting of the SECURITY PARAMETERS INFORMATION Field) is implemented. The iteration of the USER DATA MESSAGE HANDLING Group (R3) specifying the UDM requiring a Signed Acknowledgment will contain an AUTHENTICATION DATA (A) Field which is used to construct the AUTHENTICATION DATA (B) Field sent in the Signed Acknowledgment Response.

5.8.5.2 Case 3: Signed Acknowledgment Response, Requirements.

5.8.5.2.1 When the SIGNED ACKNOWLEDGE REQUEST INDICATOR in a received UDM is set to value 1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED) in an iteration of the USER DATA MESSAGE HANDLING Group (R3) and the SECURITY PARAMETERS INFORMATION Field in the same USER DATA MESSAGE HANDLING Group (R3) is set to a value implemented by the Recipient, a Signed Acknowledgment Response shall be transmitted.

5.8.5.2.2 No User Data shall be present in A Signed Acknowledgment Response.

5.8.5.2.3 A Signed Acknowledgment Response shall have the GPI for PERISHABILITY DTG Group (G11) set to value 0 (NOT PRESENT).

5.8.5.2.4 A Signed Acknowledgment Response shall have the GPI for ACKNOWLEDGMENT REQUEST Group (G12) set to value 0 (NOT PRESENT).

5.8.5.2.5 A Signed Acknowledgment Response shall have the GPI for RESPONSE DATA Group (G13) set to value 1 (PRESENT).

5.8.5.2.6 A Signed Acknowledgment Response shall have the GPI for AUTHENTICATION (A) Group (G24) set to value 1 (PRESENT).

5.8.5.2.7 A Signed Acknowledgment Response shall have the GPI for AUTHENTICATION (B) Group (G25) set to value 1 (PRESENT).

5.8.5.2.8 A Signed Acknowledgment Response shall have the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field set to value 0 (SIGNED ACKNOWLEDGMENT NOT REQUIRED).

5.8.5.3 Case 3: Signed Acknowledgment Response, Pseudocode.

```
 THIS CASE REQUIRES
      GPI for PERISHABILITY DATE TIME GROUP Group (G11) is set to
           value 0 (NOT PRESENT)
      AND  GPI for ACKNOWLEDGMENT REQUEST Group Group (G12) is
           set to value 0 (NOT PRESENT)
      AND  GPI for RESPONSE DATA Group (G13) set to value 1
           (PRESENT)
      AND  GPI for AUTHENTICATION (A) Group (G24) is set to
           value 1 (PRESENT)
      AND  GPI for AUTHENTICATION (B) Group (G25) is set to
           value 1 (PRESENT)
      AND  the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field is set
           to value 0 (NOT PRESENT)
      AND  User Data is not present
END CASE
```

5.8.7 Condition 1: URN and UNIT NAME Mutual Exclusivity.

5.8.7.1 Condition 1: URN and UNIT NAME Mutual Exclusivity, Description.

5.8.7.1.1 This condition ensures that the URN and UNIT NAME are not present in the same Address Group.

5.8.7.2 Condition 1: URN and UNIT NAME Mutual Exclusivity, Requirements.

5.8.7.2.1 When the FPI of a URN Field is set to value 1 (PRESENT), the FPI of the UNIT NAME Field in the same Group shall be set to value 0 (NOT PRESENT).

5.8.7.2.2 When the FPI of a URN Field is set to value 0 (NOT PRESENT), the FPI of the UNIT NAME Field in the same Group shall be set to value 1 (PRESENT).

5.8.7.3 Condition 1: URN and UNIT NAME Mutual Exclusivity Pseudocode.

```
IF    FPI for URN Field is set to value 1 (PRESENT)
THEN  FPI for UNIT NAME Field is set to value 0 (NOT PRESENT)
ELSE  FPI for URN Field is set to value 0 (NOT PRESENT)
AND   FPI for UNIT NAME Field is set to value 1 (PRESENT)
ENDIF
```

5.8.8 Condition 2: ORIGINATOR DATE TIME GROUP Group Presence in Original User Data Message Requiring a Receipt/Compliance Response.

5.8.8.1 Condition 2: ORIGINATOR DATE TIME GROUP Group Presence in Original User Data Message Requiring a Receipt/Compliance Response, Description.

5.8.8.1.1 This condition ensures that the ORIGINATOR DATE TIME GROUP Group (G10) is included when sending an Original UDM and requesting a Receipt/Compliance response.

5.8.8.2 Condition 2: ORIGINATOR DATE TIME GROUP Group Presence in Original User Data Message Requiring a Receipt/Compliance Response, Requirements.

5.8.8.2.1 When the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field is set to value 1 (REQUIRED) in an iteration of the USER DATA MESSAGE HANDLING Group (R3), the GPI for the ORIGINATOR DATE TIME GROUP Group (G10) in the same USER DATA MESSAGE HANDLING Group (R3) shall be set to value 1 (PRESENT).

5.8.8.2.2 An Originator ALPDU with the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) set to value 1 (REQUIRED) shall set the GPI for ORIGINATOR DTG Group (G10) in the same USER DATA MESSAGE HANDLING Group (R3) to value 1 (PRESENT).

5.8.8.2.3 An Originator ALPDU with the OPERATOR REPLY REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) set to value 1 (REQUIRED) shall set the GPI for ORIGINATOR DTG Group (G10) in the same USER DATA MESSAGE HANDLING Group (R3) to value 1 (PRESENT).

5.8.8.3 Condition 2: ORIGINATOR DATE TIME GROUP Group Presence in Original User Data Message Requiring a Receipt/Compliance Response Pseudocode.

```
IF    MACHINE ACKNOWLEDGE REQUEST INDICATOR Field is set to
          value 1 (REQUIRED)
OR    OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field is set to
          value 1 (REQUIRED)
OR    OPERATOR REPLY REQUEST INDICATOR Field is set to value 1
          (REQUIRED)
THEN  GPI for ORIGINATOR DTG Group (G10) is set to value 1
          (PRESENT)
ENDIF
```

5.8.9 Condition 3: SPI is Value 0 (Authentication/No Encryption).

5.8.9.1 Condition 3: SPI is Value 0 (Authentication/No Encryption), Description.

5.8.9.1.1 This condition ensures that the correct information is provided when the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) indicating that authentication is required but encryption is not applied. The KEYING MATERIAL Group (G21), CRYPTOGRAPHIC INITIALIZATION Group (G22), KEY TOKEN Group (G23) and USER DATA MESSAGE SECURITY PADDING Group (G26) within the USER DATA MESSAGE SECURITY Group (G20) are not present when the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION). The AUTHENTICATION (A) Group (G24) is present when the SECURITY PARAMETERS INFORMATION Field is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION).

5.8.9.2 Condition 3: SPI is Value 0 (Authentication/No Encryption), Requirements.

5.8.9.2.1 When the SECURITY PARAMETERS INFORMATION Field in an iteration of the USER DATA MESSAGE SECURITY Group (G20) is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the KEYING MATERIAL Group (G21) in the same USER DATA MESSAGE SECURITY Group (G20) shall be set to value 0 (NOT PRESENT).

5.8.9.2.2 When the SECURITY PARAMETERS INFORMATION Field in an iteration of the USER DATA MESSAGE SECURITY Group (G20) is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION),the GPI for the CRYPTOGRAPHIC INITIALIZATION Group (G22) in the same USER DATA MESSAGE SECURITY Group (G20) shall be set to value 0 (NOT PRESENT).

5.8.9.2.3 When the SECURITY PARAMETERS INFORMATION Field in an iteration of the USER DATA MESSAGE SECURITY Group (G20) is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the KEY TOKEN Group (G23) in the same USER DATA MESSAGE SECURITY Group (G20) shall be set to value 0 (NOT PRESENT).

5.8.9.2.4 When the SECURITY PARAMETERS INFORMATION Field in an iteration of the USER DATA MESSAGE SECURITY Group (G20) is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the AUTHENTICATION (A) Group (G24) in the same USER DATA MESSAGE SECURITY Group (G20) shall be set to value 1 (PRESENT).

5.8.9.2.5 An Application Header with the SECURITY PARAMETERS INFORMATION Field set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION) shall have the AUTHENTICATION DATA (A) LENGTH Field in the same Application Header set to value 4 (5 64-BIT BLOCKS).

5.8.9.2.6 When the SECURITY PARAMETERS INFORMATION Field in an iteration of the USER DATA MESSAGE SECURITY Group (G20) is set to value 0 (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION), the GPI for the USER DATA MESSAGE SECURITY PADDING Group (G26) in the same USER DATA MESSAGE SECURITY Group (G20) shall be set to value 0 (NOT PRESENT).

5.8.9.3 Condition 3: SPI is Value 0 (Authentication/No Encryption), Pseudocode.

```
IF    SECURITY PARAMETERS INFORMATION Field is set to value 0
          (AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION)
THEN  GPI for KEYING MATERIAL Group (G21) is set to value 0 (NOT
          PRESENT)
AND   GPI for CRYPTOGRAPHIC INITIALIZATION Group (G22) is set to
          value 0 (NOT PRESENT)
AND   GPI for KEY TOKEN Group (G23) is set to value 0 (NOT
          PRESENT)
AND   GPI for AUTHENTICATION (A) Group (G24) is set to value 1
          (PRESENT)
AND   GPI for USER DATA MESSAGE SECURITY PADDING Group (G26) is
          set to value 0 (NOT PRESENT)
ENDIF
```

5.8.10 Condition 4: SIGNED ACKNOWLEDGE REQUEST INDICATOR and ACKNOWLEDGMENT REQUEST Group (G12) Relationship.

5.8.10.1 Condition 4: SIGNED ACKNOWLEDGE REQUEST INDICATOR and ACKNOWLEDGMENT REQUEST Group (G12) Relationship, Description.

5.8.10.1.1 This Condition ensures that the ACKNOWLEDGMENT REQUEST Group (G12) is present when a Signed Acknowledgment Response is requested. This relationship ensures that a RESPONSE DATA Group (G13) is present in the Signed Acknowledgment Response thus allowing the UDM being responded to (in both Receipt/Compliance and Signed Acknowledgment Response terms) to be identified.

5.8.10.1.2 The relationship between the SIGNED ACKNOWLEDGE REQUEST INDICATOR and the ACKNOWLEDGMENT REQUEST Group (G12) only applies when a Signed Acknowledgment Response is required. Setting the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field to value 0 (SIGNED ACKNOWLEDGMENT RESPONSE NOT REQUIRED) does not have any processing implications for the ACKNOWLEDGMENT REQUEST Group (G12); the Group can be present to allow for "routine" Receipt/Compliance processing.

5.8.10.2 Condition 4: SIGNED ACKNOWLEDGE REQUEST INDICATOR and ACKNOWLEDGMENT REQUEST Group (G12) Relationship, Requirements.

5.8.10.2.1 When the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field is set to value 1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED), the GPI for the ACKNOWLEDGMENT REQUEST Group (G12) shall be set to 1 (PRESENT).

5.8.10.3 Condition 4: SIGNED ACKNOWLEDGE REQUEST INDICATOR and ACKNOWLEDGMENT REQUEST Group (G12) Relationship, Pseudocode.

```
IF    SIGNED ACKNOWLEDGE REQUEST INDICATOR Field is set to value
          1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED)
THEN  GPI for the ACKNOWLEDGMENT REQUEST Group (G12) is set to 1
          (PRESENT)
ENDIF
```

5.8.11 Condition 5: Retransmitted User Data Message ORIGINATOR DTG Setting.

5.8.11.1 Condition 5: Retransmitted User Data Message ORIGINATOR DTG Setting, Description.

5.8.11.1.1 This condition ensures that the ORIGINATOR DTG Group (G10) values in a Retransmitted UDM are set to those in the Original iteration of R3 for the same UDM.

5.8.11.2 Condition 5: Retransmitted User Data Message ORIGINATOR DTG Setting, Requirements.

5.8.11.2.1 The ORIGINATOR DATE TIME GROUP Group (G10) values in an iteration of the USER DATA MESSAGE HANDLING Group (R3) with the RETRANSMIT INDICATOR Field set to value 1 (RETRANSMISSION) shall be set to those in the Original iteration of the USER DATA MESSAGE HANDLING Group (R3) for the UDM being retransmitted.

5.8.11.3 Condition 5: Retransmitted User Data Message ORIGINATOR DTG Setting, Pseudocode.

```
IF    RETRANSMIT INDICATOR Field is set to value 1
           (RETRANSMISSION)
THEN  ORIGINATOR DATE TIME GROUP Group (G10) fields are set to
           those in the Original iteration of the USER DATA
           MESSAGE HANDLING Group (R3) for the UDM being
           retransmitted
ENDIF
```

5.8.12 Expected Response 1: Machine Acknowledge Requested.

5.8.12.1 Expected Response 1: Machine Acknowledge Requested, Description.

5.8.12.1.1 When a Machine Acknowledge is requested, the Receipt/Compliance response USER DATA MESSAGE RECEIPT/COMPLIANCE Field is limited to either a MACHINE RECEIPT or CANTPRO response. These values are the only ones which are purely machine-generated; all other responses require operator interaction.

5.8.12.2 Expected Response 1: Machine Acknowledge Requested, Requirements.

5.8.12.2.1 When the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (REQUIRED), the USER DATA MESSAGE RECEIPT/COMPLIANCE Field in the resulting Receipt/Compliance response shall be set to value 1 (MACHINE RECEIPT) or value 2 (CANTPRO), as appropriate.

5.8.12.3 Expected Response 1: Machine Acknowledge Requested, Pseudocode.

```
IF    a received MACHINE ACKNOWLEDGE REQUESTED INDICATOR Field
          in an iteration of the USER DATA MESSAGE HANDLING
          Group (R3) is set to value 1 (REQUIRED)
THEN  Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 1 (MACHINE RECEIPT)
OR    Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM being
          responded to is set to value 2 (CANTPRO)
ENDIF
```

5.8.13 Expected Response 2: Operator Acknowledge Requested.

5.8.13.1 Expected Response 2: Operator Acknowledge Requested, Description.

5.8.13.1.1 When an Operator Acknowledge is requested, the Receipt/Compliance response USER DATA MESSAGE RECEIPT/COMPLIANCE Field is limited to either an Operator Acknowledge or CANTPRO Receipt/Compliance response. The former is the desired response whereas the latter allows for the circumstance in which the received UDM or ALPDU cannot be processed.

5.8.13.2 Expected Response 2: Operator Acknowledge Requested, Requirements.

5.8.13.2.1 When the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (REQUIRED), the USER DATA MESSAGE RECEIPT/COMPLIANCE Field in the resulting Receipt/Compliance response shall be set to value 2 (CANTPRO) or value 3 (OPERATOR ACKNOWLEDGE), as appropriate.

5.8.13.3 Expected Response 2: Operator Acknowledge Requested, Pseudocode.

```
IF    a received OPERATOR ACKNOWLEDGE REQUESTED INDICATOR Field
          in an iteration of the USER DATA MESSAGE HANDLING
          Group (R3) within a received ALPDU is set to value 1
          (REQUIRED)
THEN  Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 2 (CANTPRO)
OR    Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 3 (OPERATOR ACKNOWLEDGE)
ENDIF
```

5.8.14 Expected Response 3: Operator Reply Requested.

5.8.14.1 Expected Response 3: Operator Reply Requested, Description.

5.8.14.1.1 When an Operator Reply is requested, the Receipt/Compliance response USER DATA MESSAGE RECEIPT/COMPLIANCE Field is either set to CANTPRO or one of the Operator Reply values. The Operator Reply values are AVCO, WILCO or CANTCO and require operator interaction unlike CANTPRO (which is automatically generated and transmitted).

5.8.14.2 Expected Response 3: Operator Reply Requested, Requirements.

5.8.14.2.1 When the OPERATOR REPLY REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (REQUIRED), the USER DATA MESSAGE RECEIPT/COMPLIANCE Field in the resulting Receipt/Compliance Response shall be set to value 2 (CANTPRO) or value 4 (WILCO) or value 5 (HAVCO) or value 6 (CANTCO), as appropriate.

5.8.14.3 Expected Response 3: Operator Reply Requested, Pseudocode.

```
IF    the OPERATOR REPLY REQUESTED INDICATOR Field in an
          iteration of the USER DATA MESSAGE HANDLING Group (R3)
          within a received ALPDU is set to value 1 (REQUIRED)
THEN  Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 2 (CANTPRO)
OR    Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 4 (WILCO)
OR    Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 5 (HAVCO)
OR    Receipt/Compliance response USER DATA MESSAGE
          RECEIPT/COMPLIANCE Field in the USER DATA MESSAGE
          HANDLING Group (R3) for that particular UDM is set to
          value 6 (CANTCO)
ENDIF
```

5.8.15 Expected Response 4: Cannot Process a Signed Acknowledgment Request.

5.8.15.1 Expected Response 4: Cannot Process a Signed Acknowledgment Request, Description.

5.8.15.1.1 There are various reasons that a Signed Acknowledgment request cannot be honored. Foremost is that the overall capability is not implemented by the system receiving the Signed Acknowledgment request; this circumstance is addressed elsewhere in this standard. The other most likely failures to generate the requested Signed Acknowledgment Response are related to process failure. In these circumstances, the Originator of the Signed Acknowledgment request is told that the UDM cannot be processed and a reason is provided.

5.8.15.2 Expected Response 4: Cannot Process a Signed Acknowledgment Request, Requirements.

5.8.15.2.1 If the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED) and the Recipient implements the security parameters scheme indicated by the setting of the SECURITY PARAMETERS INFORMATION Field in the same USER DATA MESSAGE HANDLING Group (R3) but cannot authenticate the UDM referred to by the USER DATA MESSAGE HANDLING Group (R3), a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted to the UDM Originator.

5.8.15.2.2 If the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED) and the Recipient implements the security parameters scheme indicated by the setting of the SECURITY PARAMETERS INFORMATION Field in the same USER DATA MESSAGE HANDLING Group (R3) but cannot authenticate the UDM referred to by the USER DATA MESSAGE HANDLING Group (R3), the CANTPRO REASON Field of the CANTPRO Receipt/Compliance response sent to the Originator shall be set to value 27 (AUTHENTICATION FAILURE).

5.8.15.2.3 If the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED) and the Recipient implements the security parameters scheme indicated by the setting of the SECURITY PARAMETERS INFORMATION Field in the same USER DATA MESSAGE HANDLING Group (R3) but cannot generate a Signed Acknowledgment Response, then a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted to the UDM Originator.

5.8.15.2.4 If the SIGNED ACKNOWLEDGE REQUEST INDICATOR Field in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED) and the Recipient implements the security parameters scheme indicated by the setting of the SECURITY PARAMETERS INFORMATION Field in the same USER DATA MESSAGE HANDLING Group (R3) but cannot generate a Signed Acknowledgment Response, the CANTPRO REASON Field of the CANTPRO Receipt/Compliance response sent to the Originator shall be set to value 31 (CANNOT GENERATE A SIGNED ACKNOWLEDGMENT).

5.8.15.3 Expected Response 4: Cannot Process a Signed Acknowledgment Request, Pseudocode.

```
IF    SIGNED ACKNOWLEDGE REQUEST INDICATOR Field in an iteration
          of the USER DATA MESSAGE HANDLING Group (R3) within a
          received ALPDU is set to value 1 (SIGNED
          ACKNOWLEDGMENT RESPONSE REQUIRED)
AND   The value of the SECURITY PARAMETERS INFORMATION Field in
          the same USER DATA MESSAGE HANDLING Group (R3) within
          the received ALPDU is implemented
AND   The UDM cannot be authenticated
THEN  Receipt/Compliance response is transmitted with the USER
          DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2
          (CANTPRO)
AND   CANTPRO REASON Field of the CANTPRO Receipt/Compliance
          response is set to value 27 (AUTHENTICATION FAILURE)
ELSIF SIGNED ACKNOWLEDGE REQUEST INDICATOR Field in an iteration
          of the USER DATA MESSAGE HANDLING Group (R3) within a
          received ALPDU is set to value 1 (SIGNED
          ACKNOWLEDGMENT RESPONSE REQUIRED)
AND   The value of the SECURITY PARAMETERS INFORMATION Field in
          the same USER DATA MESSAGE HANDLING Group (R3) within
          the received ALPDU is implemented
AND   A Signed Acknowledgment Response cannot be generated
THEN  Receipt/Compliance response is transmitted with the USER
          DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2
          (CANTPRO)
AND   CANTPRO REASON Field of the CANTPRO Receipt/Compliance
          response is set to value 31 (CANNOT GENERATE A SIGNED
          ACKNOWLEDGMENT)
ENDIF
```

5.8.16 Expected Response 5: Incorrect Header Size.

5.8.16.1 Expected Response 5: Incorrect Header Size, Description.

5.8.16.1.1 This Expected Response ensures that, if the size of a received Application Header does not equal the value of the HEADER SIZE Field within it, the ALPDU is not processed and the Originator is informed. The Recipient responds with a Receipt/Compliance CANTPRO response and a CANTPRO Reason set to 33 (APPLICATION HEADER SIZE FIELD VALUE DOES NOT EQUAL RECEIVED HEADER SIZE) to inform the Originator of the failure to process and the reason. The complete Application Layer PDU is then discarded without further processing.

5.8.16.2 Expected Response 5: Incorrect Header Size, Requirements.

5.8.16.2.1 When the size of a received Application Header does not equal the value of a HEADER SIZE Field within it, a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted by the Recipient to the Originator.

5.8.16.2.2 When the size of a received Application Header does not equal the value of a HEADER SIZE Field within it, the Receipt/Compliance response sent by the Recipient to the ALPDU Header Originator shall include the CANTPRO REASON Field set to value 33 (APPLICATION HEADER SIZE FIELD VALUE DOES NOT EQUAL RECEIVED HEADER SIZE).

5.8.16.2.3 When the size of a received Application Header does not equal the value of a HEADER SIZE Field within it, the ALPDU shall be discarded without further processing.

5.8.16.3 Expected Response 5: Incorrect Header Size, Pseudocode.

```
IF    The size of a received ALPDU Header does not equal the
          value in the HEADER SIZE Field
THEN  Receipt/Compliance response is transmitted with the USER
          DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2
          (CANTPRO)
AND   CANTPRO REASON Field of the Receipt/Compliance response is
          set to value 33 (APPLICATION HEADER SIZE FIELD VALUE
          DOES NOT EQUAL RECEIVED HEADER SIZE)
AND   The ALPDU is discarded without further processing
ENDIF
```

5.8.17 Expected Response 6: Incorrect User Data Message Size.

5.8.17.1 Expected Response 6: Incorrect User Data Message Size, Description.

5.8.17.1.1 This Expected Response ensures that, if the USER DATA MESSAGE SIZE Field value is not the same as the received UDM size, it is not processed and the Originator is informed. The Recipient responds with a Receipt/Compliance CANTPRO response and a CANTPRO REASON set to 34 (USER DATA MESSAGE SIZE FIELD VALUE DOES NOT EQUAL RECEIVED USER DATA MESSAGE SIZE) to inform the Originator of the failure to process and the reason. The complete Application Layer PDU is then discarded without further processing.

5.8.17.2 Expected Response 6: Incorrect User Data Message Size, Requirements.

5.8.17.2.1 When optional data compression has been applied to the User Data within an ALPDU, comparison of the size of the UDM and the related USER DATA MESSAGE SIZE Field shall take place before the UDM is uncompressed.

5.8.17.2.2 When the size of a received UDM does not equal the value of the related USER DATA MESSAGE SIZE Field, a Receipt/Compliance response for that UDM with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted by a Recipient to the UDM Originator.

5.8.17.2.3 When the size of a received UDM does not equal the value of the related USER DATA MESSAGE SIZE Field, the Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) sent by a Recipient to the UDM Originator shall include the CANTPRO REASON Field set to value 34 (USER DATA MESSAGE SIZE FIELD VALUE DOES NOT EQUAL RECEIVED USER DATA MESSAGE SIZE).

5.8.17.2.4 When the size of a received UDM does not equal the value of the related USER DATA MESSAGE SIZE Field, the complete ALPDU shall be discarded without further processing.

5.8.17.3 Expected Response 6: Incorrect User Data Message Size, Pseudocode.

```
IF    The size of the received UDM (still compressed if
          compressed for transmission) does not equal the value
          in the related USER DATA MESSAGE SIZE Field
THEN  Receipt/Compliance response is transmitted with the USER
          DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2
          (CANTPRO)
AND   CANTPRO REASON Field of the Receipt/Compliance response is
          set to value 34 (USER DATA MESSAGE SIZE FIELD VALUE
          DOES NOT EQUAL RECEIVED USER DATA MESSAGE SIZE)
AND   The UDM is discarded without further processing
ENDIF
```

5.8.18 Expected Response 7: Non Zero Value in HEADER ZERO PADDING Field.

5.8.18.1 Expected Response 7: Non Zero Value in HEADER ZERO PADDING Field, Description.

5.8.18.1.1 The HEADER ZERO PADDING Field ensures that the length of an Application Header is a multiple of 8 bits to allow the UDM portion to start on a byte boundary. The only allowable value in the field is zero. This expected response ensures that if any bit in the HEADER ZERO PADDING Field contains a value other than zero, the Recipient responds with a Receipt/Compliance CANTPRO response, sets the CANTPRO REASON Field to value 35 (APPLICATION HEADER ZERO PADDING FIELD VALUE OTHER THAN "0") and discards the received ALPDU without further processing.

5.8.18.2 Expected Response 7: Non Zero Value in HEADER ZERO PADDING Field, Requirements.

5.8.18.2.1 If any of the bits in a received HEADER ZERO PADDING Field are other than 0, a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted by the Recipient to the Originator.

5.8.18.2.2 If any of the bits in a received HEADER ZERO PADDING Field are other than 0, the Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) sent by the Recipient to the UDM Originator shall include the CANTPRO REASON Field set to value 35 (APPLICATION HEADER ZERO PADDING FIELD VALUE OTHER THAN "0").

5.8.18.2.3 When a received ALPDU whose HEADER ZERO PADDING Field contains any bits other than 0, the received ALPDU shall be discarded without further processing.

5.8.18.3 Expected Response 7: Non Zero Value in HEADER ZERO PADDING Field, Pseudocode.

```
IF    Any bit of the received ALPDU whose HEADER ZERO PADDING
          Field is other than value 0
THEN  The Receipt/Compliance response RECEIPT/COMPLIANCE Field
          is set to value 2 (CANTPRO)
AND   The Receipt/Compliance response CANTPRO REASON Field is set
          to value 35 (APPLICATION HEADER ZERO PADDING FIELD
          VALUE OTHER THAN "0")
AND   The ALPDU is discarded without further processing
ENDIF
```

5.8.19 Expected Response 8: Data Has Perished.

5.8.19.1 Expected Response 8: Data Has Perished, Description.

5.8.19.1.1 This Expected Response ensures that a UDM whose related USER DATA MESSAGE HANDLING Group (R3) has PERISHABILITY DATE TIME GROUP Group (G11) values in the past is not processed. The Expected Response also ensures the Originator of a UDM requiring a Machine Acknowledgment is informed when it has not been processed because the date and time expressed by the PERISHABILITY DATE TIME GROUP Group (G11) is in the past. The Receipt/Compliance response used to carry this information includes the CANTPRO REASON Field set to value 25 (USER DATA MESSAGE TOO OLD, BASED ON PERISHABILITY) to explain why the received UDM has not been processed by the Recipient. In addition, the associated User Data is discarded without further processing.

5.8.19.2 Expected Response 8: Data Has Perished, Requirements.

5.8.19.2.1 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG and the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field in the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is set to value 1 (REQUIRED), a Receipt/Compliance Response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted by the Recipient to the UDM Originator.

5.8.19.2.2 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG and the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field in the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is set to value 1 (REQUIRED), the Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) sent by the Recipient to the UDM Originator shall include the CANTPRO REASON Field set to value 25 (User Data Message too Old, Based On Perishability).

5.8.19.2.3 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG and the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field in the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is set to value 1 (REQUIRED), a Receipt/Compliance Response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted by the Recipient to the UDM Originator.

5.8.19.2.4 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG and the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field in the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is set to value 1 (REQUIRED), a the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) sent by the Recipient to the UDM Originator shall include the CANTPRO REASON Field set to value 25 (USER DATA MESSAGE TOO OLD, BASED ON PERISHABILITY).

5.8.19.2.5 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG and the OPERATOR REPLY REQUEST INDICATOR Field in the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is set to value 1 (REQUIRED), a Receipt/Compliance Response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) shall be transmitted by the Recipient to the UDM Originator.

5.8.19.2.6 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG and the OPERATOR REPLY REQUEST INDICATOR Field in the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is set to value 1 (REQUIRED), a the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) sent by the Recipient to the UDM Originator shall include the CANTPRO REASON Field set to value 25 (USER DATA MESSAGE TOO OLD, BASED ON PERISHABILITY).

5.8.19.2.7 When the PERISHABILITY DTG Group (G11) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the DTG in the PERISHABILITY DTG Group (G11) is earlier than current DTG, the UDM shall be discarded without further processing.

5.8.19.3 Expected Response 8: Data Has Perished, Pseudocode.

```
IF    The date and time in the PERISHABILITY DATE TIME GROUP
          Group (G11) for an iteration of the USER DATA MESSAGE
          HANDLING Group (R3) within a received ALPDU are
          earlier than time of UDM receipt
AND   MACHINE ACKNOWLEDGE REQUEST INDICATOR Field is set to
          value 1 (REQUIRED)
THEN  USER DATA MESSAGE RECEIPT/COMPLIANCE Field is set to value
          2 (CANTPRO) in a Receipt/Compliance response
AND   Receipt/Compliance Response CANTPRO REASON Field is set to
          value 25 (USER DATA MESSAGE TOO OLD, BASED ON
          PERISHABILITY) in same Receipt/Compliance response
AND   The received UDM is discarded without further processing
ENDIF
```

5.8.20 Special Consideration 1: Response to Header Version Non-Interoperability.

5.8.20.1 Special Consideration 1: Response to Header Version Non-Interoperability, Description.

5.8.20.1.1 This Special Consideration ensures correct processing when a Recipient sends a version non-interoperability response to an ALPDU Originator when MIL-STD-2045-47001C has been used to create the ALPDU and that version is not implemented by the Recipient. This response indicates to the Originator that the Original ALPDU has not been processed and allows the Originator to "learn" that the Recipient cannot process ALPDUs created using MIL-STD-2045-47001C.

5.8.20.2 Special Consideration 1: Response to Header Version Non-Interoperability, Requirements.

5.8.20.2.1 When a version non-interoperability response is to be sent with the HEADER VERSION Field value set to value 15 (VERSION SENT NOT IMPLEMENTED), the response shall consist of the HEADER VERSION Field, the DATA COMPRESSION TYPE Field FPI, the ORIGINATOR ADDRESS Group (G1) and the RECIPIENT ADDRESS Group (G2).

5.8.20.2.2 When a version non-interoperability response is sent with the HEADER VERSION Field value set to value 15 (VERSION SENT NOT IMPLEMENTED), the FPI for the DATA COMPRESSION TYPE Field shall be set to 0 (NOT PRESENT).

5.8.20.2.3 When a version non-interoperability response is sent with the HEADER VERSION Field value set to value 15 (VERSION SENT NOT IMPLEMENTED), the RECIPIENT ADDRESS Group (G2) values used to identify the Recipient in the Original ALPDU shall be used to create the ORIGINATOR ADDRESS Group (G1) of the version non-interoperability response.

5.8.20.2.4 When a version non-interoperability response is sent with the HEADER VERSION Field value set to value 15 (VERSION SENT NOT IMPLEMENTED), the ORIGINATOR ADDRESS Group (G1) values in the Original ALPDU shall be used as the RECIPIENT ADDRESS Group (G2) values in the version non-interoperability response.

5.8.20.3 Special Consideration 1: Response to Header Version Non-Interoperability, Pseudocode.

```
IF    Recipient does not implement MIL-STD-2045-47001C
AND   ALPDU is received with HEADER VERSION Field set to value 3
          (MIL-STD-2045-47001C)
THEN  Version non-interoperability response is sent with HEADER
          VERSION Field is set to value 15 (VERSION SENT NOT
          IMPLEMENTED)
AND   DATA COMPRESSION TYPE Field FPI is Set to value 0 (NOT
          PRESENT)
AND   ORIGINATOR ADDRESS Group (G1) values of the Original ALPDU
          are used as the RECIPIENT ADDRESS Group (G2) values
AND   RECIPIENT ADDRESS Group (G2) values for the Original ALPDU
          are used as the ORIGINATOR ADDRESS Group (G1) values
ENDIF
```

5.8.21 Special Consideration 2: User Data Message Concatenation.

5.8.21.1 Special Consideration 2: User Data Message Concatenation, Description.

5.8.21.1.1 The process of concatenating UDMs results in a series of individual UDMs that are combined in a single User Data portion of an ALPDU. The ORIGINATOR ADDRESS Group (G1), RECIPIENT ADDRESS Group (G2) and INFORMATION ADDRESS Groups (G3) are common for all UDMs in the User Data; these Groups will therefore appear once in the Application Header with concatenated UDMs in the User Data element. The USER DATA MESSAGE HANDLING Group (R3) repeats to specify information about each of the concatenated UDMs. It is necessary that all occurrences of the OPERATION INDICATOR Field within an Application Header are common. This is also true for USER DATA MESSAGE SECURITY CLASSIFICATION Fields and CONTROL/RELEASE MARKING Fields. The order in which the USER DATA MESSAGE HANDLING Groups (R3) are presented in the Application Header is matched by the order in which the concatenated UDMs are presented in the User Data portion of the ALPDU. The total size of a single UDM within the User Data portion cannot exceed 1 megabyte (1,048,575 bytes) when concatenation is used.

5.8.21.2 Special Consideration 2: User Data Message Concatenation, Requirements.

5.8.21.2.1 When there is more than one iteration of the USER DATA MESSAGE HANDLING Group (R3), the OPERATION INDICATOR Field value shall be common for each iteration.

5.8.21.2.2 When there is more than one iteration of the USER DATA MESSAGE HANDLING Group (R3), the USER DATA MESSAGE SECURITY CLASSIFICATION Field value shall be common for each iteration.

5.8.21.2.3 When there is more than one iteration of the USER DATA MESSAGE HANDLING Group (R3), and there is more than one occurrence of the CONTROL/RELEASE MARKING Field FPI set to 1 (PRESENT) within an Application Header, the CONTROL/RELEASE MARKING Field value shall be common for each occurrence.

5.8.21.2.4 When there is more than one UDM in the User Data portion of the ALPDU and the USER DATA MESSAGE HANDLING Group (R3) GRI is therefore set to value 1 (REPEATED), the order in which the concatenated UDMs are presented in the User Data portion of the ALPDU shall match the order of the USER DATA MESSAGE HANDLING Groups (R3) which describe them.

5.8.21.2.5 When there is more than one UDM in the User Data portion of the ALPDU and the USER DATA MESSAGE HANDLING Group (R3) GRI is set to value 1 (REPEATED), each User Data portion of the ALPDU, shall be limited to a maximum size of 1,048,575 bytes.

5.8.21.3 Special Consideration 2: User Data Message Concatenation, Pseudocode.

```
IF    USER DATA MESSAGE HANDLING Group (R3) Group Repetition
          Indicator is set to value 1 (REPEATED)
THEN  The ORIGINATOR ADDRESS Group (G1), RECIPIENT ADDRESS Group
          (G2) and INFORMATION ADDRESS Group (G3) addresses
          used are common for all UDMs in the User Data portion
          of the ALPDU
AND   Each iteration of the USER DATA MESSAGE HANDLING Group
          (R3) specifying information about a UDM will follow
          the same order as the UDM in the User Data portion of
          the ALPDU
AND   Each User Data portion of the ALPDU, shall be limited to a
          maximum size of 1,048,575 bytes.
ENDIF
```

5.8.22 Special Consideration 3: Decompression of User Data Prior to Parsing.

5.8.22.1 Special Consideration 3: Decompression of User Data Prior to Parsing, Description.

5.8.22.1.1 This Special Consideration ensures that when the User Data in a received ALPDU has been compressed, the User Data is decompressed by the Addressee prior to parsing.

5.8.22.2 Special Consideration 3: Decompression of User Data Prior to Parsing, Requirements.

5.8.22.2.1 If a received ALPDU has the DATA COMPRESSION TYPE Field FPI set to value 1 (PRESENT), the Addressee shall decompress the User Data prior to parsing.

5.8.22.3 Special Consideration 3: Decompression of User Data Prior to Parsing, Pseudocode.

```
IF    The DATA COMPRESSION TYPE Field FPI is set to value 1
          (PRESENT)
THEN  The Addressee decompresses the User Data prior to parsing
ENDIF
```

5.8.23 Special Consideration 4: UNIT NAME Usage in a Receipt/Compliance Response.

5.8.23.1 Special Consideration 4: UNIT NAME Usage in a Receipt/Compliance Response, Description.

5.8.23.1.1 This Special Consideration ensures that if a received ALPDU used the UNIT NAME Field in the ORIGINATOR ADDRESS Group (G1), the UNIT NAME Field is used in the RECIPIENT ADDRESS Group (G2) in any response and the URN Field is not used.

5.8.23.2 Special Consideration 4: UNIT NAME Usage in a Receipt/Compliance Response, Requirements.

5.8.23.2.1 If the RESPONSE DATA Group (G13) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the ORIGINATOR ADDRESS Group (G1) UNIT NAME Field FPI within the Application Header was set to value 1 (PRESENT), the RECIPIENT ADDRESS Group (G2) UNIT NAME Field FPI in any response shall be set to value 1 (PRESENT).

5.8.23.3 Special Consideration 4: UNIT NAME Usage in a Receipt/Compliance Response, Pseudocode.

```
IF    RESPONSE DATA Group (G13) GPI in an iteration of the USER
          DATA MESSAGE HANDLING Group (R3) is set to value 1
          (PRESENT)
AND   The ORIGINATOR ADDRESS Group (G1) UNIT NAME Field FPI
          within the Application Header was set to value 1
          (PRESENT)
THEN  the RECIPIENT ADDRESS Group (G2) UNIT NAME Field FPI in
          any response is set to value 1 (PRESENT)
ENDIF
```

5.8.24 Special Consideration 5: URN Usage in a Receipt/Compliance Response.

5.8.24.1 Special Consideration 5: URN Usage in a Receipt/Compliance Response, Description.

5.8.24.1.1 This Special Consideration ensures that if a received ALPDU used the URN Field in the ORIGINATOR ADDRESS Group (G1), the URN Field is used in the RECIPIENT ADDRESS Group (G2) in any response and the UNIT NAME Field is not used.

5.8.24.2 Special Consideration 5: URN Usage in a Receipt/Compliance Response, Requirements.

5.8.24.2.1 If the RESPONSE DATA Group (G13) GPI in an iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU is set to value 1 (PRESENT) and the ORIGINATOR ADDRESS Group (G1) URN Field FPI within the Application Header was set to value 1 (PRESENT), the RECIPIENT ADDRESS Group (G2) URN Field FPI within any response shall be set to value 1 (PRESENT).

5.8.24.3 Special Consideration 5: URN Usage in a Receipt/Compliance Response, Pseudocode.

```
IF    RESPONSE DATA Group (G13) GPI in an iteration of the USER
          DATA MESSAGE is set to value 1 (PRESENT)
AND   The ORIGINATOR ADDRESS Group (G1) URN Field FPI within the
          Application Header was set to value 1 (PRESENT)
THEN  The RECIPIENT ADDRESS Group (G2) URN Field FPI in any
          response is set to value 1 (PRESENT)
ENDIF
```

5.8.25 Special Consideration 6: Use of Segmentation/Reassembly Protocol.

5.8.25.1 Special Consideration 6: Use of Segmentation/Reassembly Protocol, Description.

5.8.25.1.1 This Special Consideration seeks to ensure that bandwidth demand is managed and efficient use is made of capability. The Special Consideration is invoked when either the User Datagram Protocol (UDP) or Network Layer Pass Through (NLPT) is being used on a network using Combat Net Radios as the bearer medium and the data transfer size is greater than the Maximum Segment Size. Under these conditions, the Segmentation/Reassembly is used for the data transfer.

5.8.25.2 Special Consideration 6: Use of Segmentation/Reassembly Protocol, Requirements.

5.8.25.2.1 When the UDP is in use and the size of a proposed data transfer is greater than the Maximum Segment Size, the Segmentation/Reassembly Protocol shall be used for the data transfer.

5.8.25.2.2 When NLPT is in use and the size of a proposed data transfer is greater than the Maximum Segment Size, the Segmentation/Reassembly Protocol shall be used for the data transfer.

5.8.25.3 Special Consideration 6: Use of Segmentation/Reassembly Protocol, Pseudocode.

```
IF    UDP is used on a Combat Net Radio-based network
OR    NLPT is used on a Combat Net Radio-based network
AND   Data transfer is greater than the Maximum Segment Size
THEN  Segmentation/Reassembly protocol is used
ENDIF
```

5.8.26 Special Consideration 7: Use of MIL-STD-188-220 Network Layer Pass through (NLPT).

5.8.26.1 Special Consideration 7: Use of MIL-STD-188-220 Network Layer Pass Through (NLPT), Description.

5.8.26.1.1 The intent of this special consideration is to provide guidance as to when NLPT should be used to transmit ALPDUs when MIL-STD-188-220 is used as the lower level protocol. This allows for stations to automatically determine when to use NLPT which reduces network overhead associated with Internet Protocol (IP) Headers.

5.8.26.2 Special Consideration 7: Use of MIL-STD-188-220 Network Layer Pass Through (NLPT), Requirements.

5.8.26.2.1 If the ALPDU is to be broadcast and MIL-STD-188-220 protocols are in use at the lower levels, NLPT shall be used.

5.8.26.2.2 If the only destination address specified for an ALPDU is the Broadcast URN (16777215) and MIL-STD-188-220 protocols are in use at the lower levels, NLPT shall be used.

5.8.26.2.3 If all destination addresses for an ALPDU are in the same IP subnetwork as the Originator and MIL-STD-188-220 protocols are in use at the lower levels, NLPT shall be used.

5.8.26.3 Special Consideration 7: Use of MIL-STD-188-220 Network Layer Pass Through (NLPT), Pseudocode.

```
IF    The ALPDU is to be broadcast
OR    The only destination address specified is the Broadcast
           URN (16777215)
OR    All destination addresses are in the same Internet
           Protocol subnetwork as the Originator
AND   MIL-STD-188-220 protocols are in use in the lower levels
THEN  NLPT is used
ENDIF
```

5.9 User Data Processing.

5.9.1 User Data Processing, General Description.

5.9.1.1 The User Data portion of the ALPDU contains the application process messages or data. The User Data is individually encoded and zero padded before it is passed to the Application Layer to have the Application Header added.

5.9.2 User Data Processing, User Data Message Format.

5.9.2.1 User Data Processing, User Data Message Format, General Description.

5.9.2.1.1 The ALPDU is capable of carrying many different User Data formats as described in this document and as indicated by the USER DATA MESSAGE FORMAT Field setting.

5.9.2.2 User Data Processing, User Data Message Format, Link 16 User Data (UDMF=0).

5.9.2.2.1 User Data Processing, User Data Message Format, Link 16 User Data (UDMF =0), Description.

5.9.2.2.1.1 The transfer of Link 16 data is indicated by setting the USER DATA MESSAGE FORMAT Field to value 0 (LINK 16). The Link 16 data (J Series Messages) being transferred are described in MIL-STD-6016.

5.9.2.2.2 User Data Processing, User Data Message Format, Link 16 User Data (UDMF =0), Requirements.

5.9.2.2.2.1 No specific requirements.

5.9.2.3 User Data Processing, User Data Message Format, Binary File User Data (UDMF =1).

5.9.2.3.1 User Data Processing, User Data Message Format, Binary File User Data (UDMF =1), Description.

5.9.2.3.1.1 The transfer of a binary file or data block is indicated by setting the USER DATA MESSAGE FORMAT Field to value 1 (BINARY FILE). The block of data being transferred is a "logical binary file"; no particular type of file is indicated or intimated by the use of this UDMF.

5.9.2.3.2 User Data Processing, User Data Message Format, Binary File User Data (UDMF =1), Requirements.

5.9.2.3.2.1 No specific requirements

5.9.2.4 User Data Processing, User Data Message Format, VMF User Data (UDMF =2).

5.9.2.4.1 User Data Processing, User Data Message Format, VMF User Data (UDMF =2), Description.

5.9.2.4.1.1 The transfer of VMF User Data is indicated by setting the USER DATA MESSAGE FORMAT Field to value 2 (VARIABLE MESSAGE FORMAT (VMF)). The format of VMF messages are defined in MIL-STD-6017.

5.9.2.4.2 User Data Processing, User Data Message Format, VMF User Data (UDMF =2), Requirements.

5.9.2.4.2.1 No specific requirements.

5.9.2.5 User Data Processing, User Data Message Format, National Imagery Transmission Format System (NITFS) User Data (UDMF =3).

5.9.2.5.1 User Data Processing, User Data Message Format, National Imagery Transmission Format System (NITFS) User Data (UDMF =3), Description.

5.9.2.5.1.1 The transfer of National Imagery Transmission Format System (NITFS) User Data is indicated by setting the USER DATA MESSAGE FORMAT Field to value 3 (NATIONAL IMAGERY TRANSMISSION FORMAT SYSTEM (NITFS)). The format of NITFS image transfers are defined in MIL-STD-2500 (Series) and STANAG 4545/AEDP-4 (Series). The NITFS is a group of standards specifying the format, compression, and communication of image files and amplifying information such as text, graphics, and location. The NITF is the primary document within the standard that specifies the file format, and is designated as US DOD Interface Standard, MIL-STD-2500 (Series). The NITF establishes the requirements for the file format component of the NITFS, provides a detailed description of the standard file format structure, and specifies the valid data content and format for all fields defined within an NITF file. The NATO Secondary Imagery Format (NSIF) Version 1.0, referenced as STANAG 4545 Edition 1 is the NATO equivalent to NITF 2.0 and NATO Allied Engineering Documentation Publication (AEDP-4) Edition 1 is equivalent to NITF 2.1.

5.9.2.5.2 User Data Processing, User Data Message Format, National Imagery Transmission Format System (NITFS) User Data (UDMF =3), Requirements.

5.9.2.5.2.1 Each NITFS file transferred shall comply with either the NITFS 2.0 or NITFS 2.1 Tactical Profiles.

5.9.2.6 User Data Processing, User Data Message Format, Redistributed ALPDU User Data (UDMF =4).

5.9.2.6.1 User Data Processing, User Data Message Format, Redistributed ALPDU User Data (UDMF =4), Description.

5.9.2.6.1.1 The transfer of a Redistributed ALPDU is indicated by setting the USER DATA MESSAGE FORMAT Field to value 4 (REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT). Redistributed ALPDUs in MIL-STD-2045-47001 function similarly to forwarding e-mail messages. When an ALPDU is received, the Recipient may determine that it should be forwarded to one or more other stations. This determination could be automatic (e.g., all ALPDUs from Address X will be automatically forwarded to Address Y), or may be the result of operator action (e.g., the operator believes that the information contained in the ALPDU would be of operational value to another unit and manually forwards the data). The mechanism for determining which ALPDUs should be forwarded is beyond the scope of this document and should be determined by specific platform requirements. The entire ALPDU to be redistributed is reproduced in the User Data portion of the Redistributed ALPDU.

5.9.2.6.2 User Data Processing, User Data Message Format, Redistributed ALPDU User Data (UDMF =4), Requirements.

5.9.2.6.2.1 The User Data portion of a Redistributed ALPDU shall consist of the entire unmodified Original ALPDU.

5.9.2.6.2.2 In a Redistributed ALPDU Application Header, the ORIGINATOR ADDRESS Group (G1) shall reflect that of the system transmitting the Redistributed ALPDU.

5.9.2.6.2.3 In a Redistributed ALPDU Application Header, the OPERATION INDICATOR Field shall be set to the same value as that in the Original ALPDU.

5.9.2.6.2.4 In a Redistributed ALPDU Application Header, the USER DATA MESSAGE SECURITY CLASSIFICATION Field shall be set to the same value as that in the Original ALPDU.

5.9.2.6.2.5 In a Redistributed ALPDU Application Header, the CONTROL/RELEASE MARKING Field shall be set to the same value as that in the Original ALPDU.

5.9.2.6.2.6 When a Redistributed ALPDU is received, the Redistributed ALPDU Application Header shall be processed prior to processing the Original ALPDU present as User Data.

5.9.2.6.2.7 An addressee of a Redistributed ALPDU shall process the Original ALPDU whether or not that addressee is specified in the Original ALPDU.

5.9.2.6.2.8 A Recipient of a Redistributed ALPDU shall respond as required by the ACKNOWLEDGMENT REQUEST Group (G12) in the Redistributed ALPDU Application Header.

5.9.2.6.2.9 A Recipient of a Redistributed ALPDU shall ignore any Receipt/Compliance actions required by the ACKNOWLEDGMENT REQUEST Group (G12) in the Original ALPDU Application Header.

5.9.2.6.2.10 Data from a Redistributed ALPDU shall be identified as such when displayed to an Operator.

5.9.2.6.2.11 Only ALPDUs with UDMs with the same Operation Indicator, Security Classification, and Control/Release Marking fields in their USER DATA MESSAGE HANDLING GROUP (R3) groups shall be concatenated for redistribution.

5.9.2.7 User Data Processing, User Data Message Format, United States Message Text Format (USMTF) User Data (UDMF =5).

5.9.2.7.1 User Data Processing, User Data Message Format, United States Message Text Format (USMTF) User Data (UDMF =5), Description.

5.9.2.7.1.1 The transfer of US Message Text Format messages is indicated by setting the USER DATA MESSAGE FORMAT Field to value 5 (UNITED STATES MESSAGE TEXT FORMAT (USMTF)). The format of US Message Text Format messages is defined in MIL-STD-6040. The block of data being transferred is in US Message Text Format.

5.9.2.7.2 User Data Processing, User Data Message Format, United States Message Text Format (USMTF) User Data (UDMF =5), Requirements.

5.9.2.7.2.1 No current specific requirements.

5.9.2.8 User Data Processing, User Data Message Format, UDMF =6.

5.9.2.8.1 User Data Processing, User Data Message Format, UDMF =6, Description – Not Used

5.9.2.8.2 User Data Processing, User Data Message Format, UDMF =6, Requirements – Not Used.

5.9.2.9 User Data Processing, User Data Message Format, eXtensible Markup Language (XML) - Message Text Format (MTF) User Data (UDMF =7).

5.9.2.9.1 User Data Processing, User Data Message Format, eXtensible Markup Language (XML) - Message Text Format (MTF) User Data (UDMF =7), Description.

5.9.2.9.1.1 The transfer of XML-MTF messages is indicated by setting the USER DATA MESSAGE FORMAT Field to value 7 (EXTENSIBLE MARKUP LANGUAGE MESSAGE TEXT FORMAT (XML-MTF)). The format of XML-MTF messages is defined in MIL-STD-6040, Annex A. The block of data being transferred is in eXtensible Markup Language - Message Text Format (XML-MTF); no host system processing or capability is intimated or inferred by its inclusion in this standard.

5.9.2.9.2 User Data Processing, User Data Message Format, eXtensible Markup Language (XML) - Message Text Format (MTF) User Data (UDMF =7), Requirements.

5.9.2.9.2.1 No specific requirements.

5.9.2.10 User Data Processing, User Data Message Format, Variable Message Format Markup Language (VML) User Data (UDMF =8).

5.9.2.10.1 User Data Processing, User Data Message Format, Variable Message Format Markup Language (VML) User Data (UDMF =8), Description.

5.9.2.10.1.1 The transfer of Variable Message Format Markup Language (VML) messages is indicated by setting the USER DATA MESSAGE FORMAT Field to value 8 (VARIABLE MESSAGE FORMAT MARKUP LANGUAGE (VML)). The format of VML messages is defined in MIL-STD-6017, Appendix F. The block of data being transferred is in VML format; no host system processing or capability is intimated or inferred by its inclusion in this standard.

5.9.2.10.2 User Data Processing, User Data Message Format, Variable Message Format Markup Language (VML) User Data (UDMF =8), Requirements.

5.9.2.10.2.1 No specific requirements.

5.10 Processing Factors.

5.10.1 Duplicate Application Layer Protocol Data Unit Processing.

5.10.1.1 Duplicate Application Layer Protocol Data Unit Processing, Description.

5.10.1.1.1 The detection and management of duplicate UDMs is achieved by comparing the Originator address and date and time values, and the DATE TIME GROUP EXTENSION Field value, if present, from iterations of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU with the same data from UDMs which have been previously received. This requires that a record is kept of each previously received iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU sufficient to allow duplicate checks to be carried out. Iterations of the USER DATA MESSAGE HANDLING Group (R3) which are identified as duplicates are discarded along with the associated UDM albeit any Receipt/Compliance response demands in them are still met.

5.10.1.2 Duplicate Application Layer Protocol Data Unit Processing, Requirements.

5.10.1.2.1 A record shall be kept of the ORIGINATOR ADDRESS Group (G1) values and the ORIGINATOR DATE TIME GROUP Group (G10) values in each iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU.

5.10.1.2.2 On receipt, the ORIGINATOR ADDRESS Group (G1) values and the ORIGINATOR DATE TIME GROUP Group (G10) values in each iteration of the USER DATA MESSAGE HANDLING Group (R3) within a received ALPDU shall be checked against the same data from previously received ALPDUs.

5.10.1.2.3 If a duplicate combination of ORIGINATOR ADDRESS Group (G1) and ORIGINATOR DATE TIME GROUP Group (G10) is detected and the USER DATA MESSAGE HANDLING Group (R3) has the GPI of the ACKNOWLEDGMENT REQUEST Group (G12) set to value 1 (PRESENT), the Recipient shall comply with the expressed Receipt/Compliance request.

5.10.1.2.4 If a duplicate combination of ORIGINATOR ADDRESS Group (G1) and ORIGINATOR DATE TIME GROUP Group (G10) is detected and the USER DATA MESSAGE HANDLING Group (R3) has the GPI of the ACKNOWLEDGMENT REQUEST Group (G12) set to value 1 (PRESENT) and the Recipient has complied with the expressed Receipt/Compliance request, the UDM associated with that iteration of the USER DATA MESSAGE HANDLING Group (R3) shall be discarded with no further processing.

5.10.1.2.5 If a duplicate combination of ORIGINATOR ADDRESS Group (G1) and ORIGINATOR DATE TIME GROUP Group (G10) is detected, the UDM associated with that iteration of the USER DATA MESSAGE HANDLING Group (R3) shall be discarded with no further processing.

5.10.2 User Data Message Retransmission.

5.10.2.1 User Data Message Retransmission, Description.

5.10.2.1.1 The facility is provided for any UDM to be retransmitted on operator action; the fact that the UDM is a retransmission is indicated through use of the RETRANSMIT INDICATOR Field within the USER DATA MESSAGE HANDLING Group (R3) for the UDM. A capability is also provided which enables the automatic retransmission of a UDM when a Machine Acknowledgment was requested and a Receipt/Compliance response is not received within a certain time period. The number of automatic retransmissions is selectable and there are various other demands associated with this capability.

5.10.2.2 User Data Message Retransmission, Requirements.

5.10.2.2.1 The operator shall be provided with the capability to select any previously transmitted UDM for retransmission.

5.10.2.2.2 The operator shall be provided with the capability to enable the automatic retransmission of a UDM with the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field within the USER DATA MESSAGE HANDLING Group (R3) for the UDM set to value 1 (REQUIRED) and for which a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field within the USER DATA MESSAGE HANDLING Group (R3) for the UDM set to value 1 (MACHINE RECEIPT) has not been received.

5.10.2.2.3 When the automatic retransmission of a UDM for which there is an outstanding MACHINE RECEIPT Receipt/Compliance response is enabled, the number of automatic retransmissions for a UDM shall be operator selectable with a range of 1 to 3 in steps of 1.

5.10.2.2.4 A retransmission timer with a range of 5 to 600 seconds in steps of 5 seconds shall be provided to schedule the automatic retransmission of an ALPDU containing a UDM for which there is an outstanding MACHINE RECEIPT Receipt/Compliance response.

5.10.2.2.5 The retransmission timer shall be started when an ALPDU containing a UDM with the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field within the USER DATA MESSAGE HANDLING Group (R3) for the UDM set to value 1 (REQUIRED) is sent for transmission.

5.10.2.2.6 If a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 1 (MACHINE RECEIPT) is not received in response to an ALPDU with a UDM with the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field set to value 1 (REQUIRED) when the retransmission timer expires and the number of automatic retransmissions allowed has not been reached, the UDM shall be retransmitted by the Originator.

5.10.2.2.7 If a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 1 (MACHINE RECEIPT) is not received in response to an ALPDU with a UDM with the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field set to value 1 (REQUIRED) when the retransmission timer expires and the number of automatic retransmissions allowed for that UDM is reached, the Operator shall be alerted.

5.10.2.2.8 Receipt of a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to other than value 1 (MACHINE RECEIPT) in response to a UDM which also has an outstanding MACHINE RECEIPT Receipt/Compliance response shall prevent automatic retransmission processing being invoked.

5.10.2.2.9 When a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to other than value 1 (MACHINE RECEIPT) is received in response to a UDM which has an outstanding MACHINE RECEIPT Receipt/Compliance response, the Operator shall be alerted.

5.10.3 Application Header Transmission Validation Process.

5.10.3.1 Application Header Transmission Validation Process, Description.

5.10.3.1.1 The Application Header Transmission validation process ensures that the contents and structure of an Application Header meet the requirements of this standard. Only Application Headers that pass validation can be transmitted and any validation failures are reported to the Operator.

5.10.3.2 Application Header Transmission Validation Process, Requirements.

5.10.3.2.1 The system shall validate an Application Header prepared for transmission against the requirements in this standard.

5.10.3.2.2 Only ALPDUs with Application Headers that have been successfully validated shall be released for transmission.

5.10.3.2.3 The system shall validate received Application Headers against the requirements in this standard.

5.10.3.2.4 If the system detects an Application Header which does not pass validation, the Operator shall be alerted, with the reason for validation failure being made available as part of the alert process.

5.10.4 Application Header Values Reception Validation Process.

5.10.4.1 Application Header Values Reception Validation Process, Description.

5.10.4.1.1 The reception validation process ensures that ALPDUs received containing illegal values are not processed by Addressees and a CANTPRO Receipt/Compliance response and CANTPRO Reason are sent by Recipients. The processing also ensures that processing continues when Disused, Undefined or Reserved values as defined in the Data Element Dictionary at Appendix B are encountered.

5.10.4.2 Application Header Values Reception Validation Process, Requirements.

5.10.4.2.1 A received Application Header shall be processed if it contains a value defined as Disused in the Data Element Dictionary at Appendix B.

5.10.4.2.2 A received Application Header shall be processed if it contains a value defined as Undefined in the Data Element Dictionary at Appendix B.

5.10.4.2.3 A received Application Header shall be processed if it contains a value defined as Reserved in the Data Element Dictionary at Appendix B

5.10.4.2.4 If an Application Header is received containing Illegal values, the system shall discard the ALPDU without further processing.

5.10.4.2.5 When an Application Header is received containing Illegal values, the Recipient shall send a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field be set to value 2 (CANTPRO).

5.10.4.2.6 When an Application Header is received containing Illegal values and a Receipt/Compliance response with the USER DATA MESSAGE RECEIPT/COMPLIANCE Field be set to value 2 (CANTPRO) is sent by the Recipient, the CANTPRO REASON Field in the response shall be set to 1 (FIELD CONTENT INVALID).

5.10.5 Perishability Processing.

5.10.5.1 Perishability Processing, Description.

5.10.5.1.1 Perishability processing ensures that data are not dropped from a display or purged from a database based purely on the time expressed by the PERISHABILITY DATE TIME GROUP Group (G11). The processing also ensures that the operator is aware which data is older than the time from the PERISHABILITY DATE TIME GROUP Group (G11).

5.10.5.2 Perishability Processing, Requirements.

5.10.5.2.1 No data shall be dropped from the display based on the time expressed by the PERISHABILITY DATE TIME GROUP Group (G11).

5.10.5.2.2 No data shall be purged from any host system database based on the time expressed by the PERISHABILITY DATE TIME GROUP Group (G11).

5.10.5.2.3 Data which are retained after the time expressed by the PERISHABILITY DATE TIME GROUP Group (G11) of the source UDM shall be highlighted as such to the operator.

5.10.6 Receipt/Compliance Response Receive Processing.

5.10.6.1 Receipt/Compliance Response Receive Processing, Description.

5.10.6.1.1 Receipt of a Receipt/Compliance response demands that an attempt is made to match it to a transmitted UDM for which Receipt/Compliance actions were requested. Sufficient data about such a UDM must therefore be retained in order to facilitate checking. A discrete record is created for each where the ACKNOWLEDGMENT REQUEST Group (G12) is present.

5.10.6.1.2 If a received Receipt/Compliance response is found to match an outstanding Receipt/Compliance request, it is processed. A subsequent check is made that the Receipt/Compliance response value is logical e.g. a Machine Acknowledgment request stimulates a MACHINE RECEIPT. Requirements exist in this section that defined both for when the match is logical and when it is not.

5.10.6.1.3 Received Receipt/Compliance responses with a USER DATA MESSAGE RECEIPT/COMPLIANCE Field set to value 2 (CANTPRO) are always processed. It is however still relevant whether there is an outstanding Receipt/Compliance request as a CANTPRO response when there is a Receipt/Compliance request outstanding is likely to have more impact than one which does not.

5.10.6.2 Receipt/Compliance Response Receive Processing, Requirements.

5.10.6.2.1 A discrete record shall be kept containing the RECIPIENT ADDRESS Group (G2) and the ORIGINATOR DATE TIME GROUP Group (G10) and the ACKNOWLEDGMENT REQUEST Group (G12) values of each iteration of the MESSAGE HANDLING Group (R3) within a transmitted Application Header which contains an ACKNOWLEDGMENT REQUEST Group (G12) GPI set to 1 (PRESENT).

5.10.6.2.2 When a Receipt/Compliance response is received, a Receipt/Compliance receive check shall be carried out.

5.10.6.2.3 A Receipt/Compliance receive check shall be passed when retained RECIPIENT ADDRESS Group (G2) values match the received ORIGINATOR ADDRESS Group (G1) values and retained ORIGINATOR DATE TIME GROUP Group (G10) values from the same record match the date, time and DATE TIME GROUP EXTENSION Field (if present) values in the received RESPONSE DATA Group.

5.10.6.2.4 If a received Receipt/Compliance response fails the Receipt/Compliance receive check but the USER DATA MESSAGE RECEIPT/COMPLIANCE Field of the Receipt/Compliance response is set to value 2 (CANTPRO), the Receipt/Compliance response shall be processed.

5.10.6.2.5 If a received Receipt/Compliance response fails the Receipt/Compliance receive check and the USER DATA MESSAGE RECEIPT/COMPLIANCE Field of the Receipt/Compliance response is set to other than value 2 (CANTPRO), the Receipt/Compliance response shall be discarded without further processing.

5.10.6.2.6 If a received Receipt/Compliance response passes the Receipt/Compliance receive check and a Receipt/Compliance response is outstanding for the transmitted User Data Message, the Receipt/Compliance response shall be processed.

5.10.6.2.7 If a received Receipt/Compliance response passes the Receipt/Compliance receive check but no Receipt/Compliance response is outstanding for the transmitted User Data Message, the Receipt/Compliance response shall be discarded without further processing.

5.10.6.2.8 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with an Undefined value as defined in the Data Element Dictionary at Appendix B, the Operator shall be alerted and presented with the Receipt/Compliance response and associated data.

5.10.6.2.9 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 1 (MACHINE RECEIPT), the Receipt/Compliance response shall be processed.

5.10.6.2.10 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field to 1 (Required) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 2 (CANTPRO), the Receipt/Compliance response shall be processed.

5.10.6.2.11 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the MACHINE ACKNOWLEDGE REQUEST INDICATOR Field to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value other than 1 (MACHINE RECEIPT) or 2 (CANTPRO), the Receipt/Compliance response shall be discarded without further processing.

5.10.6.2.12 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field to 1 (REQUIRED) and the Receipt/Compliance has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 2 (CANTPRO), the Receipt/Compliance response shall be processed.

5.10.6.2.13 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field to 1 (REQUIRED) and the Receipt/Compliance has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 3 (OPERATOR ACKNOWLEDGE), the Receipt/Compliance response shall be processed.

5.10.6.2.14 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR ACKNOWLEDGE REQUEST INDICATOR Field to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value other than 2 (CANTPRO) or 3 (OPERATOR ACKNOWLEDGE), the Receipt/Compliance response shall be discarded without further processing.

5.10.6.2.15 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR REPLY REQUEST INDICATOR Field set to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 2 (CANTPRO), the Receipt/Compliance response shall be processed.

5.10.6.2.16 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR REPLY REQUEST INDICATOR Field set to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 4 (WILCO), the Receipt/Compliance response shall be processed.

5.10.6.2.17 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR REPLY REQUEST INDICATOR Field set to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 5 (HAVCO), the Receipt/Compliance response shall be processed.

5.10.6.2.18 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR REPLY REQUEST INDICATOR Field set to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value of 6 (CANTCO), the Receipt/Compliance response shall be processed.

5.10.6.2.19 When processing a Receipt/Compliance response which has passed the Receipt/Compliance receive check and which has a Receipt/Compliance response outstanding as a result of setting the OPERATOR REPLY REQUEST INDICATOR Field set to 1 (REQUIRED) and the Receipt/Compliance response has a USER DATA MESSAGE RECEIPT/COMPLIANCE Field with a value other than 2 (CANTPRO) or 4 (WILCO) or 5 (HAVCO) or 6 (CANTCO), the Receipt/Compliance response shall be discarded without further processing.

5.10.7 Lower Layer Interactions.

5.10.7.1 Lower Layer Interactions General, Description.

5.10.7.1.1 Several Application Header Groups or Fields are used as guidance by lower layer protocols. The following Groups or Fields are used by the lower layers but have no particular requirements associated with them that require expression in this standard:

a. USER DATA MESSAGE SECURITY CLASSIFICATION Field.

b. USER DATA MESSAGE PRECEDENCE Field.

c. ORIGINATOR ADDRESS Group (G1).

d. RECIPIENT ADDRESS Group (G2).

e. INFORMATION ADDRESS Group (G3).

f. PERISHABILITY DTG Group (G11).

5.10.7.2 Lower Layer Interactions General, Requirements.

5.10.7.2.1 No specific general requirements.

5.10.7.3 Lower Layer Interactions Security Classification.

5.10.7.3.1 Lower Layer Interactions Security Classification, Description.

5.10.7.3.1.1 The USER DATA MESSAGE SECURITY CLASSIFICATION Field as described in paragraph 5.6.17 provides the desired guidance to the lower layers for establishing security classification.

5.10.7.3.2 Lower Layer Interactions Security Classification, Requirements.

5.10.7.3.2.1 No specific requirements.

5.10.7.4 Lower Layer Interactions User Data Message Precedence.

5.10.7.4.1 Lower Layer Interactions User Data Message Precedence, Description.

5.10.7.4.1.2 This USER DATA MESSAGE PRECEDENCE Field as described in paragraph 5.6.16 provides the desired guidance to the lower layers for setting transmission precedence.

5.10.7.4.2 Lower Layer Interactions User Data Message Precedence, Requirements.

5.10.7.4.2.1 The USER DATA MESSAGE PRECEDENCE Field shall be set by the transmitting system.

5.10.7.5 Lower Layer Interactions Quality of Service (QOS).

5.10.7.5.1 Lower Layer Interactions Quality of Service (QOS), Description.

5.10.7.5.1.1 Determination of the Quality of Service (QOS) to be provided to the ALPDU by lower layer protocols uses the values in the following Application Header elements:

a. USER DATA MESSAGE SIZE Field.
b. USER DATA MESSAGE PRECEDENCE Field.
c. ORIGINATOR DATE TIME GROUP Group (G10) date and time fields.
d. PERISHABILITY DATE TIME GROUP Group (G11) date and time fields.
e. MACHINE ACKNOWLEDGE REQUEST INDICATOR Field.

5.10.7.5.1.2 A calculated parameter, USER DATA MESSAGE VALIDITY, is used in QOS determination. It is expressed in seconds and is used to express the "life" of the UDM on the interface. USER DATA MESSAGE VALIDITY is calculated by subtracting the date and time values of the ORIGINATOR DATE TIME GROUP Group (G10) from the date and time values of the PERISHABILITY DATE TIME GROUP Group (G11) for a particular UDM.

5.10.7.5.1.3 Two other parameters are also used to determine the required QOS. These are:

a. USER DATA MESSAGE SIZE THRESHOLD.
b. PERISH.

5.10.7.5.1.4 USER DATA MESSAGE SIZE THRESHOLD is an external parameter that is set by the host system. The parameter allows the host system to influence the point at which RELIABILITY is changed from Normal to High.

5.10.7.5.1.5 PERISH is an external parameter that is set by the host system. The parameter allows the host system to influence the point at which DELAY is changed from Normal to Low and RELIABILITY is changed from Normal to High.

5.10.7.5.1.6 The following QOS parameters, which are mapped from various combinations of the Application Header fields and parameters identified above, are:

a. DELAY expressed as Normal or Low.
b. RELIABILITY, expressed as Normal or High.
c. THROUGHPUT, expressed as Normal or High.

5.10.7.5.1.7 The Default value for each of the QOS parameters is 0 (NORMAL). The QOS parameters will only change from Normal when a specific combination of parameter and Application Header field values are present.

5.10.7.5.2 Lower Layer Interactions Quality of Service (QOS), Requirements.

5.10.7.5.2.1 USER DATA MESSAGE VALIDITY shall be calculated by subtracting the date and time values of the ORIGINATOR DATE TIME GROUP Group (G10) within an iteration of the USER DATA MESSAGE HANDLING Group (R3) from the date and time values of the PERISHABILITY DATE TIME GROUP Group (G11) within the same iteration of USER DATA MESSAGE HANDLING Group (R3).

5.10.7.5.2.2 USER DATA MESSAGE SIZE THRESHOLD shall be a parameter with a range of 1 to 1,048,575 bytes in steps of 1 with a default value of 1440.

5.10.7.5.2.3 USER DATA MESSAGE SIZE THRESHOLD shall be set by the host system to influence the point at which RELIABILITY is changed from Normal to High.

5.10.7.5.2.4 PERISH shall be a parameter with a range of 1 to 10800 seconds in 1 second steps.

5.10.7.5.2.5 PERISH shall be set by the host system to influence the point at which DELAY is changed from Normal to Low and RELIABILITY is changed from Normal to High.

5.10.7.5.2.6 DELAY shall have a default value of 0 (NORMAL).

5.10.7.5.2.7 Only if USER DATA MESSAGE VALIDITY for an iteration of the USER DATA MESSAGE HANDLING Group (R3) is less than or equal to PERISH and the USER DATA MESSAGE PRECEDENCE Field within the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is anything other than 0 (ROUTINE) shall DELAY be set to value 1 (LOW).

5.10.7.5.2.8 RELIABILITY shall have a default value of 0 (NORMAL).

5.10.7.5.2.9 Only if USER DATA MESSAGE VALIDITY for an iteration of the USER DATA MESSAGE HANDLING Group (R3) is greater than PERISH and the MACHINE ACKNOWLEDGE REQUEST INDICATOR within the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is 1 (REQUIRED) and the value in the USER DATA MESSAGE SIZE Field within the same iteration of the USER DATA MESSAGE HANDLING Group (R3) is equal to or greater than USER DATA MESSAGE SIZE THRESHOLD shall RELIABILITY be set to value 1 (HIGH).

5.10.7.5.2.10 THROUGHPUT shall have a default value of 0 (NORMAL).

5.10.7.5.2.11 Only if the value in the USER DATA MESSAGE SIZE Field is greater than or equal to USER DATA MESSAGE SIZE THRESHOLD and DELAY is set to value 0 (NORMAL) and RELIABILITY is set to value 0 (NORMAL) shall THROUGHPUT be set to value 1 (HIGH).

5.10.7.5.3 Lower Layer Interactions Quality of Service (QOS), Pseudocode.

```
IF    USER DATA MESSAGE VALIDITY <= PERISH
AND   USER DATA MESSAGE PRECEDENCE Field <> 0 (ROUTINE)
THEN  DELAY = 1 (LOW)
ELSE  DELAY = 0 (NORMAL)
ENDIF

IF    USER DATA MESSAGE VALIDITY > PERISH
AND   MACHINE ACKNOWLEDGE REQUEST INDICATOR = 1 (Required)
AND   USER DATA MESSAGE SIZE Field value >= USER DATA MESSAGE
      SIZE THRESHOLD
THEN  RELIABILITY = 1 (HIGH)
ELSE  RELIABILITY = 0 (NORMAL)
ENDIF

IF    USER DATA MESSAGE SIZE Field value >= USER DATA MESSAGE
      SIZE THRESHOLD
AND   DELAY == Normal
AND   RELIABILITY = 0 (NORMAL)
THEN  THROUGHPUT = 1 (HIGH)
ELSE  THROUGHPUT = 0 (NORMAL)
ENDIF
```

5.10.7.6 Lower Layer Interactions ORIGINATOR ADDRESS Group.

5.10.7.6.1 Lower Layer Interactions ORIGINATOR ADDRESS Group, Description.

5.10.7.6.1.1 The ORIGINATOR ADDRESS Group (G1) as described in paragraph 5.7.1 provides the desired guidance to the lower layers for the Originator Address.

5.10.7.6.2 Lower Layer Interactions ORIGINATOR ADDRESS Group, Requirements.

5.10.7.6.2.1 No current specific requirements.

5.10.7.7 Lower Layer Interactions RECIPIENT ADDRESS Group.

5.10.7.7.1 Lower Layer Interactions RECIPIENT ADDRESS Group, Description.

5.10.7.7.1.1 The RECIPIENT ADDRESS Group (G2) as described in paragraph 5.7.1 provides the desired guidance to the lower layers for the Recipient Address.

5.10.7.7.2 Lower Layer Interactions RECIPIENT ADDRESS Group, Requirements.

5.10.7.7.2.1 No specific requirements.

5.10.7.8 Lower Layer Interactions Perishability DTG.

5.10.7.8.1 Lower Layer Interactions Perishability DTG, Description.

5.10.7.8.1.1 The PERISHABILITY DTG Group (G11) as described in paragraph 5.7.5 provides the desired guidance to the lower layers for the Perishability DTG.

5.10.7.8.2 Lower Layer Interactions Perishability DTG, Requirements.

5.10.7.8.2.1 The PERISHABILITY DTG Group (G11) shall be used by the lower layers to determine if a UDM in a queue for transmission is to be processed.

5.10.7.9 Lower Layer Interactions Destination Port Number.

5.10.7.9.1 Lower Layer Interactions Destination Port Number, Description.

5.10.7.9.1.1 The port named "mil-2045-47001" has been registered with the Internet Assigned Number Authority and has been assigned port number 1581 (decimal) to indicate the MIL-STD-2045-47001 ALP as defined by this standard. APPENDIX A - SEGMENTATION/REASSEMBLY PROTOCOL provides further information on exchanging data using the Segmentation/Reassembly protocol. If NLPT is invoked without Segmentation/Reassembly, the next lower layer is the intranet layer and destination port number is not required.

5.10.7.9.2 Lower Layer Interactions Destination Port Number, Requirements.

5.10.7.9.2.1 The "mil-2045-47001" (1581 decimal) port shall be passed as the destination port parameter value to the lower layer protocol.

5.10.7.9.2.2 The value for the UDP Destination Port number for IP/UDP data exchanges using MIL-STD-2045-47001 Application Layer Protocol shall be 1581 decimal.

5.10.7.9.2.3 The value for the UDP Source Port number for IP/UDP data exchanges using MIL-STD-2045-47001 Application Layer Protocol shall be defined by the host system.

6 NOTES

6.1 General.

6.1.1 This section contains information of a general or explanatory nature that may be helpful, but is not prescriptive.

6.2 Management of TCP Connections.

6.2.1 When TCP is used to transport the MIL-STD-2045-47001 ALP over low bit rate combat network radio (CNR) networks, the overhead for opening and closing connections can contribute substantially to the offered load presented to the CNR network. The following conventions for the management of TCP connections used to transport the ALP are offered to allow the amount of overhead generated as the result of opening and closing TCP connections to be controlled.

a. When a MIL-STD-2045-47001 message becomes available for transport, a TCP connection will be opened to the destination if a connection to the destination hasn’t already been established.

b. An established TCP connection to a given destination will be gracefully closed if no activity (transmitted or received data) occurs on the connection within some configurable time period of the most recent activity on that connection.

c. If a connection already exists to a given destination and an additional connection offer is received from the same destination, the older connection will be closed at the end of the normal completion of any pending message transports such that only one connection is maintained and utilized for each destination.

d. MIL-STD-2045-47001 messages will be offered for transport over the TCP connection to the specified destination in the order established by the USER DATA MESSAGE PRECEDENCE Field of the MIL-STD-2045-47001 Application Header. If a higher priority message becomes available for transport to a destination while a lower priority message is in the process of being transported to the same destination, the transport of the higher priority message will begin immediately after the transport of the lower priority message is completed. Lower priority messages that have not already been offered for transport on the connection should not be offered for transport until after higher priority messages have been offered for transport on the connection.

e. The number of connections/destinations that can be utilized simultaneously by a single MIL-STD-2045-47001 application should be limited to a configurable number. Once this limit is reached there are two reasons additional connections might need to be established: either a message becomes available locally for transport to an additional destination, or a connection offer is received from a new remote source.

1. In the case of a locally generated message to an additional destination, the Least Recently Active (LRA) connection that is not currently being used for the transport of messages, should be closed prior to the establishment of a connection to the new destination. If all connections are actively being used, then the new message transport request should be discarded and treated as a transport failure.

2. In the case that a connection offer is accepted from an additional remote source, the LRA connection that is not currently being used for the transport of messages should be closed. If all connections are actively being used, then the new recently accepted connection should be abruptly closed. Abruptly closing the newly accepted connection will terminate any pending transmissions from the remote source and inform the remote source that any pending messages were not transported successfully.

6.3 Changes from Previous Issue.

6.3.1 Marginal notations are not used in this revision to identify changes with respect to the previous issue due to the extent of the changes.

APPENDIX A

SEGMENTATION/REASSEMBLY PROTOCOL

A.1 GENERAL.

A.1.1 Scope.

A.1.1.1 This appendix specifies requirements supporting the exchange of Application Layer Protocol Data Units (ALPDU) using the S/R protocol. These requirements address the implementation of a segmentation-and-reassembly capability, segmentation of large ALPDUs into two-or-more segments, the transmission of these segments, and their subsequent reassembly at destination nodes.

A.1.1.2 It should be noted that S/R is principally used in the exchange of ALPDUs in a tactical environment. This exchange is accomplished over either Universal Datagram Protocol (UDP) or MIL-STD-188-220's Network Layer Pass Through (NLPT) protocol. However, both UDP and NLPT are external to S/R. Accordingly, although reference is made to both transmission protocols, requirements specific to the implementation of S/R on either are outside the scope of this appendix.

A.1.2 Definitions.

A.1.2.1 Definition of Terms.

Application PDU Identifier	An identifier which uniquely identifies the ALPDU for which the S/R transaction is instantiated. This identifier consists of the Originator Address (as provided by the lower level protocol) combined with the S/R Header Serial Number of the transfer. Serial Number is unique to the S/R Originator, but may be replicated between different Originators, which is why this value is paired with the Originator Address. On NLPT networks, "source address" is the data link address. On IP networks, "source address" is the source IP address.
Destination	The S/R node receiving ALPDU segments.
Originator	The S/R node sending ALPDU segments.

Parameter	Parameters are entities that are external to the implementation, whose values are passed into the system (i.e., using a configuration message or non-volatile storage) and used in calculations by either an Originator or Destination. Parameters usually remain fixed during run-time; however, systems implementing advanced algorithms may wish to adjust these variables during run-time based on measured data collected during operation. This appendix provides minimum, maximum, and default values for parameters. Parameter values are stored in a manner supporting system modification of default values.
Rate Limited CNR	Low bandwidth, shared radio networks used for tactical combat operations (e.g., Command and Control for Fire Support and the MIL-STD-188-220 Networks used for Close Air Support). Ground Communications over these shared VHF radio nets using the SINCGARS Enhanced Data Mode waveform are characterized by frequently corrupted transmissions (even after Forward Error Correction (FEC) has been applied at the receiver) due to obstructions, range limitations, noise, jamming, poor antenna location, limited transmit power, collisions, etc. When these slow nets become congested due to heavy loads, they demonstrate extremely high latencies and/or high discard rates.
Request for Acknowledgment	A Request for Acknowledgment is general terminology referencing either Acknowledgment Request (AR) PDUs or a Data Segment (DS) PDU with its P-Bit set to a value of one (1). The term's correct usage is when referring to both PDU types as a category of S/R PDUs, and should not be used as a synonym of either.

Segment Number	Segment Number (SN) refers to the value of the Segment Number field contained in the Data Segment PDU.
Selective Retransmission	S/R employs "Selective Retransmission" to improve efficiency for bandwidth-constrained or rate-limited networks by using the comprehensive receive status for all data segments, as reported by Destinations using the Partial Acknowledgments (PA) PDU, to help avoid unnecessary retransmission of segments by the Originator. The PA requires each Destination to report the receive status of all segments (i.e., report a status for every segment of the transfer indicating whether the segment has been received or has not been received). The Originator utilizes the reported segment status to retransmit missing lower-numbered unacknowledged segments, and not unnecessarily retransmit higher number acknowledged segments received out of sequence. For a better understanding of the importance of Selective Retransmission for rate-limited or bandwidth-constrained networks, consider the performance implications of a simpler approach (i.e., where the PA is limited to reporting the first missing segment). This PA reporting limitation would cause the Originator to conclude that all unacknowledged segments starting with the first missing segment may need to be retransmitted, even though some of the unacknowledged segments might have already been received correctly, but out of sequence at the destination generating the PA.
Sent	For the purpose of the S/R Appendix, the term "sent" refers to the action of the S/R Layer making a data transfer request to the next lower level layer in the protocol stack (e.g., UDP or Network Layer Pass Through) to transmit data.
Transport Layer	The layer in the Open System Interconnection (OSI) model responsible for end-to-end communication over a network.

A.1.3 Summary of S/R Acronyms, Terms, Explanations, and Applications.

A.1.3.1 Acronyms and terms used in this appendix are defined in Table A-I below:

TABLE A - I Summary of Acronyms Used in S/R

Acronym	Clear Text
ABC	Abort Confirm
ABR	Abort Request
ABRIL	Abort Request Interval Limit
ABCRL	Abort Confirm Retry Limit
ABRRL	Abort Request Retry Limit
AR	Acknowledgment Request
bps	Bits per second
CA	Complete Acknowledgment
CARL	Complete Acknowledgment Retry Limit
DS	Data Segment
DSCP	Different Services Code Point
DSEDTANR	Data Segment with End of Data Transfer Acknowledgment Required
DSEDTAR	Data Segment with End of Data Transfer Acknowledgment Not Required
EDT	End of Data Transfer
EDTANR	End of Data Transfer Acknowledgment Not Required
EDTAR	End of Data Transfer Acknowledgment Required
ERTD	Estimated Round Trip Delay
FEC	Forward Error Correction
HNSR	Highest Numbered Segment Received
HOPCNT	Hop Count
IARL	Immediate Acknowledgment Request Limit
ISRIEL	Inter-Segment Receive Interval Expirations Limit
ISRIL	Inter-Segment Receive Interval Limit
ISSIL	Inter-Segment Send Interval Limit
LSN	Last Segment Number

LSSN	Last Sent Segment Number
MAX_ISRIL_VALUE	Maximum Inter-Segment Receive Interval Limit Value
MAX_RFAIL_VALUE	Maximum Request For Acknowledgment Interval Limit Value
MSRL	Missing Segment Range Limit
MSS	Maximum Segment Size
MTU	Maximum Transfer Unit
NOMSL	Number of Missing Segments Limit
NS	Number of Segments
PA	Partial Acknowledgment
PAIL	Partial Acknowledgment Interval Limit
PARL	Partial Acknowledgment Retry Limit
P/F	Poll/Final
RFAIL	Request For Acknowledgment Interval Limit
RFARL	Request For Acknowledgment Retry Limit
RSCL	Received Segments Count Limit
RTECL	Reassembly Time Expiration Count Limit
RTL	Reassembly Time Limit
SCL	Segment Credit Limit
SN	Segment Number
SRCL	Segment Retry Count Limit
SSCL	Sent Segments Count Limit
SSN	Starting Segment Number
SSRLPO	Segment Send Rate Limit Per Originator
TCL	Transaction Completion Limit
T2AT	Type 2 Acknowledgment Timer

Appendix A

A.2 APPLICABLE DOCUMENTS.

RFC 791	Internet Protocol - DARPA Internet Protocol Specification
RFC 768	User Datagram Protocol
RFC-1122	Requirements for Internet Hosts, Communication Layers
RFC-2460	Internet Protocol, Version 6 (IPv6) Specification https://www.rfc-editor.org/info/
MIL-STD-188-220	Digital Message Transfer Device Subsystems https://assist.dla.mil/

Appendix A

A.3 SEGMENTATION/REASSEMBLY.

A.3.1 S/R, General.

A.3.1.1 S/R, General, Description.

A.3.1.1.1 The S/R Protocol provides systems the ability to support the exchange of ALPDUs that exceed a network's maximum packet size. The optional S/R capabilities provide additional controls to help further manage/optimize these ALPDU transfers. The capabilities described in this appendix support Point-to-Point and Point-to-Multipoint transmission of large ALPDUs. Many of the optional capabilities identified in this specification support additional logic required to affect reliable tracking of data segment transmission and receipt in one-to-many transmissions.

A.3.1.1.2 The S/R protocol supports Selective Retransmission, an important concept ensuring that segments are only re-sent if they were not previously received. The S/R Selective Retransmission mechanism avoids unnecessary retransmission of segments, helping to maximize efficiency in the limited bandwidth of Combat Net Radio (CNR) networks. The S/R protocol provides a reliable, connectionless transport layer service using User Datagram Protocol (UDP) [refer to RFC 768]/Internet Protocol (IP) lower layer protocol [refer to RFC 791, RFC 1122 and RFC 2460] or using MIL-STD-188-220 NLPT lower layer protocol to exchange S/R segments. The S/R Protocol avoids the UDP/IP reliability degradation typically associated with Internet Protocol version 4 (IPv4) Fragmentation by limiting the size of S/R segment to preclude IPv4 fragmentation when sending via UDP/IPv4.

A.3.1.1.3 S/R processing occurs between the Upper Layer Protocol (e.g., MIL-STD-2045-47001 Application Layer) and the next lower level layer (i.e., UDP/IP or the MIL-STD-188-220 Intranet Layer via NLPT). S/R supports guaranteed delivery, and is used in conjunction with UDP/IP as a lighter-weight (i.e., lower processing overhead) alternative to TCP (Transmission Control Protocol)/IP when sending large ALPDUs over slower, unreliable CNR. Because the Transport Layer functions supported by UDP/IP are minimal, supporting S/R over UDP/IP does not result in significant inefficiencies due to duplication of functions. The use of UDP/IP by S/R allows it to support multiple platforms, as most operating systems provide built in UDP/IP support. S/R is not intended for use over TCP/IP because of the overlap in reliable delivery functions and resultant network inefficiencies.

A.3.1.1.4 The S/R protocol performs all S/R functions transparently to the Upper Layer Protocol, both at the origination and destination nodes. Note that the S/R protocol does not directly examine or modify the ALPDU itself (other than to perform segmentation and reassembly).

A.3.1.1.5 All S/R data segments within a transaction should have the same data link precedence (usually accomplished by using the same intranet precedence) or network precedence level. This ensures that timers function properly, as changing the precedence of packets can potentially cause wide variations in the timing packet transmission.

A.3.1.2 S/R (MIL-STD-188-220), Description.

A.3.1.2.1 This section addresses implementation topics specific to employment of the S/R protocol over MIL-STD-188-220 networks. While this discussion falls outside the scope of general S/R implementation, it is included here as background information. For a fuller discussion of these topics, refer to MIL-STD-188-220.

A.3.1.2.2 S/R Protocol Data Unit (PDU) exchanges over low traffic (e.g., Close Air Support) MIL-STD-188-220 nets using UDP/IP or NLPT should maximize use of MIL-STD-188-220 Type 1 data link procedures for segments with P-Bit or F-Bit set to zero (0), and take advantage of MIL-STD-188-220 Type 3 and/or Type 4 data link procedures for data segments with P-Bit or F-Bit set to one (1). Use of MIL-STD-188-220 Type 2 data link procedures should be minimized for low traffic networks. For explanation of P-Bit and F-Bit see paragraph A.6.2.7.

A.3.1.2.3 S/R PDU exchanges over high traffic (e.g., Fire Support) MIL-STD-188-220 nets using UDP/IP or NLPT should maximize the use of MIL-STD-188-220 Type 1 or MIL-STD-188-220 Type 2 data link procedures and minimize the use of MIL-STD-188-220 Type 3 and/or Type 4. This increases the odds of a successful S/R transaction with the respective network types, decreases the time required to complete the S/R exchanges, and minimizes bandwidth required for the exchange.

A.3.1.2.4 When sent over a MIL-STD-188-220 CNR net, S/R Segments that have the P-Bit set to zero (0), should not be sent as a Data Link Layer Type 3 Packets, regardless of the Precedence and/or Type Of Service (TOS) for the associated ALPDU, since the guarantee of delivery is provided via S/R Acknowledgments. S/R Segments that have the P-Bit set to one (1) should be sent reliably at the Data Link Layer, which will allow for increased performance of the S/R protocol as S/R timers will be less likely to increase to maximum values due to missed packets.

A.3.1.2.5 While the MIL-STD-188-220 Type 3 data link procedure is somewhat reliable and recovers from transmission failures quickly, its use for S/R PDU) exchanges should be minimized because it is comparatively bandwidth inefficient, as only one MIL-STD-188-220 Type 3 message is sent for each net access, and because MIL-STD-188-220 Type 3 requires destinations to respond with an acknowledgment each time they receive a MIL-STD-188-220 Type 3 message. However, MIL-STD-188-220 Type 3 has been shown to improve efficiency in low traffic networks if it is used only when a segment with the P-Bit or F-Bit set to one (1) is transmitted and with ARs. System implementers should, however, exercise caution when using MIL-STD-188-220 Type 3 with any S/R transaction, as the MIL-STD-188-220 Type 3 Retry Mechanism can cause an S/R transaction to fail if MIL-STD-188-220 Type 3 Acknowledgments are not received properly. If optionally using MIL-STD-188-220 Type 3 with S/R, system implementers should set the Segment Retry Count Limit (SRCL) to a higher value than the MIL-STD-188-220 Type 3 Retry Limit value for their network to avoid this potential issue.

A.3.1.2.6 The MIL-STD-188-220 Type 4 data link procedure is reliable, but its timer based retransmission mechanism results in unacceptably slow S/R PDU transmission failure recoveries when used in a high traffic network environment. However, using MIL-STD-188-220 Type 4 for segments with the P-Bit or F-Bit set to one (1) and with Acknowledgment Requests is more efficient than using MIL-STD-188-220 Type 1 for those transmissions in low traffic networks.

A.3.1.2.7 When an originating station and a destination support MIL-STD-188-220 Type 2, Type 2 should be utilized for S/R PDUs sent to each unicast destination address in a high traffic network. When an originating station or a destination station does not support MIL-STD-188-220 Type 2, MIL-STD-188-220 Type 1 should normally be utilized for S/R PDUs sent to each unicast destination address. MIL-STD-188-220 Type 1 should normally be utilized for S/R PDUs sent to a multicast or a broadcast address.

A.3.2 S/R (General), Requirements.

A.3.2.1 The S/R protocol implementation shall be applied between the ALPDU source and the interface to the underlying network protocol (e.g., UDP/IP, 188/220 via NLPT, etc.).

A.3.2.2 When a MIL-STD-2045-47001 ALPDU exceeds a network's Maximum Segment Size (MSS), the Originator shall transmit the ALPDU using the S/R protocol.

A.3.2.3 When a MIL-STD-2045-47001 ALPDU does not exceed a network's MSS, it shall be a system option to implement Originator functionality to transmit the Application PDU ALPDU using the S/R protocol.

A.3.3 S/R (General, Optional).

A.3.3.1 S/R (General, Optional), Description.

A.3.3.1.1 Optional S/R functionality can facilitate greater control over transmission congestion, targeting reduced transfer completion times and an increased probability of a successful exchange for large ALPDU transfers over slower and less reliable CNR. A single S/R transmission may contain any mix of Unicast Addresses and/or Multicast Addresses (including the Global address).

A.3.3.1.2 Optional S/R functionality supports three distinct mechanisms that the Originator can use, individually or in combination, to effect congestion control;

a. Credit based congestion control using the SCL

b. Sliding window based congestion control using a Missing Segment Range Limit (MSRL)

c. Source rate congestion control using an Inter-Segment Send Interval Limit (ISSIL).

A.3.3.1.3 SCL identifies the maximum number of segments that can be outstanding (sent but not yet acknowledged) to minimize discards and/or high queue latency by lower layers when nets are congested.

A.3.3.1.4 MSRL identifies the maximum difference between segment numbers of the highest and lowest numbered outstanding segments (or Sliding Window size), establishing a maximum size for the Bit Mask Field in a PA PDU.

A.3.3.1.5 ISSIL establishes a rate at which segments can be sent, to prevent a single station from offering segments for transmission in bursts that exceed the maximum rate that can be supported by a shared network.

A.3.3.1.6 Normally, MSRL is set to a much larger value than SCL, making SCL the constraining element between the two congestion control mechanisms. The use of a smaller SCL value as the dominant congestion control mechanism in combination with larger MSRL values avoids concerns normally associated with the use of the MSRL controlled Sliding Window mechanism for CNR nets with high Bandwidth-delay products. When SCL and MSRL are used together in this manner, segments can continue to be sent for a long time while a lowered numbered segment is retransmitted several times (before it is reported as being received by all destinations), since SCL will not be reached so long as most higher number segments are acknowledged by all destinations.

A.3.3.1.7 Optional S/R functionality also adds the concept of Destination Learning for transaction to Multicast addresses. When transmitting S/R PDUs to Multicast Addresses (including the Global Address), Destination Learning is the process the Originator uses to build a list of Unicast Addresses that the ALPDU is being transmitted to, based on Destination responses to the first segment sent.

A.3.3.1.8 Under S/R's optional functionality, an Abort Request (ABR) PDU can be sent with P-Bit set to one (1). This explicitly requests an Abort Confirm (ABC) PDU from the recipient, supporting retries of ABRs when an ABC is not received in response to the initial transmission. This facilitates acknowledged termination of S/R transactions, supporting status reporting to the invoking application.

A.3.4 S/R (General), Maximum Segment Size.

A.3.4.1 S/R (General), Maximum Segment Size, IP.

A.3.4.1.1 S/R (General), Maximum Segment Size, IP, Description.

A.3.4.1.1.1 The MSS identifies the maximum size of a segment payload under the S/R protocol. The MSS values are calculated using the equations and values identified below.

MSS(IP) = MTU - (SH + UDP + IPHS) for IP datagrams, and,
MSS(NLPT) = MTU - SH for NLPT
MSS(Packet Mode) = MTU - SH for NLPT using Packet Mode

where
MTU is Maximum Transfer Unit size at the network layer
SH is S/R Header size
UDP is UDP header size
IPHS is IP header size

and
MTU = 576 octets (IPv4) or 1280 octets (IPv6), 3090 octets (NLPT, Theoretical), or 576 octets (NLPT, Mandated Default)
SH = 12 octets
UDP = 8 octets
IPHS = 60 octets (IPv4) or 174 octets (IPv6)

Note: It is desirable that IP datagrams, which may be transmitted across multiple subnetworks, do not exceed 576 octets with IPv4 or 1280 octets with IPv6. An MSS of 496 octets for both IPv4 and IPv6 will assure that IP fragmentation will not occur at any IP router/gateway devices.

A.3.4.1.2 S/R (General), Maximum Segment Size, IP, Requirements.

A.3.4.1.2.1 An S/R implementation's MSS for an IPv4 network shall be 496 octets.

A.3.4.1.2.2 An S/R implementation's MSS for an IPv6 network shall be 1086 octets.

A.3.4.1.2.3 MSS(IP) shall equal the MTU value minus the SH, UDP and IPHS header size values.

A.3.4.1.2.4 MSS(NLPT) shall equal the MTU value minus the SH value.

A.3.4.1.2.5 MSS(Packet Mode) shall equal the MTU value minus the SH value.

A.3.4.2 S/R (General), Maximum Segment Size, NLPT.

A.3.4.2.1 S/R (General), Maximum Segment Size, NLPT, Description.

A.3.4.2.1.1 The MSS value for NLPT shall be computed based on the MTU value specified in the MIL-STD-188-220 Parameter Tables using the formulas previously identified for calculating MSS. An MTU of 576 is used when no MTU value in the MIL-STD-188-220 Parameter Tables is applicable for the network configuration.

A.3.4.2.1.2 Since neither UDP nor IP are present with NLPT, IP fragmentation is not a concern. Therefore the only theoretical limitation on size is based on maximum transmission size allowed by the intranet layer. For NLPT, the following components take on the maximized constant values provided below.

MTU = 3090 octets (theoretical) or 576 octets (mandated default)
SH = 12 octets

A.3.4.2.1.3 Thus:

MSS = 3090 - 12 = 3078 octets (theoretical), or a default value of 496 for CNR when no value can be obtained from a Parameter Tables.

A.3.4.2.1.4 Although the MSS for NLPT is theoretically 3078 octets, the default MSS value for NLPT is 496 octets in the absence of a MIL-STD-188-220 Parameter Table MTU value.

A.3.4.2.2 S/R (General), Maximum Segment Size, NLPT, Requirements.

A.3.4.2.2.1 An S/R implementation's MSS (theoretical) for a NLPT network shall be 3078 octets.

A.3.4.2.2.2 When a value for MSS for a NLPT network can be obtained from a MIL-STD-188-220 Parameter Table, the S/R implementation shall use the value for MSS obtained from the MIL-STD-188-220 Parameter Table.

A.3.4.2.2.3 When a value for MSS for a NLPT network cannot be obtained from a MIL-STD-188-220 Parameter Table, the S/R implementation shall use a default MSS value of 496 octets.

A.3.5 S/R (General), Port Settings.

A.3.5.1 S/R (General), Port Settings, UDP/IP.

A.3.5.1.1 S/R (General), Port Settings, UDP/IP, Description.

A.3.5.1.1.1 This section identifies values for the UDP and S/R ports, when conducting an S/R transaction over an IP network using UDP datagrams. Table A-II provides an overview of the attribute/value pairings for S/R PDU exchange via UDP/IP.

A.3.5.1.1.2 The port named udp-sr-port, which has been registered with the Internet Assigned Number Authority and assigned port number 1624 (decimal), is the destination UDP port in all S/R invocations of the UDP service interface for sending S/R PDUs (e.g., Data Segment (DS), AR, PA, etc.).

A.3.5.1.1.3 When receiving UDP datagrams, a UDP port value of 1624 indicates a payload conforming to the S/R protocol as defined by this standard.

TABLE A - II S/R and UDP Destination/Source Port field values for S/R PDUs Sent via UDP/IP in Support of MIL-STD-2045-47001 ALP exchanges

Field	Value
S/R Destination Port	1581 (mil-2045-47001)
S/R Source Port	Any value as specified in S/R-Unitdata Request
UDP Destination Port	1624 (udp-sr-port)
UDP Source Port	Any value defined by the Originator host system

A.3.5.1.2 S/R (General), Port Settings, UDP/IP, Requirements.

A.3.5.1.2.1 An S/R implementation processing S/R PDUs over UDP shall set UDP Destination Port to the value 1624.

A.3.5.1.2.2 An S/R implementation processing S/R PDUs over UDP shall set UDP Source Port to a value determined by the Originator node.

A.3.5.1.2.3 When an S/R node receives a UDP datagram on Port 1624, the node shall process the datagram payload as an S/R PDU.

A.3.5.2 S/R (General), Port Settings, NLPT.

A.3.5.2.1 S/R (General), Port Settings, NLPT, Description.

A.3.5.2.1.1 This section identifies values for the S/R ports, when conducting an S/R transaction over CNR network via MIL-STD-188-220 NLPT. Table A-III provides an overview of the attribute/value pairings for S/R PDU exchange via UDP/IP. The MIL-STD-188-220 Intranet Message Type field value of 10, S/R Protocol has been reserved for sending S/R PDUs (e.g., AR, PA, etc.) via MIL-STD-188-220 NLPT.

A.3.5.2.1.2 At the receiving station, MIL-STD-188-220 Intranet Message Type field value of 10 indicates the S/R protocol as defined by this standard.

TABLE A - III S/R Destination/Source Port and MIL-STD-188-220 Intranet Message Type Field Values for S/R PDUs Sent Via MIL-STD-188-220 NLPT in Support of MIL-STD-2045-47001 ALP Exchanges.

Field	Value
S/R Destination Port	1581 (mil-2045-47001)
S/R Source Port	Any value, as specified in S/R-Unitdata Request
MIL-STD-188-220 Intranet Message Type	10, S/R Protocol

A.3.5.2.2 S/R (General), Port Settings, NLPT, Requirements.

A.3.5.2.2.1 An S/R implementation processing S/R PDUs with MIL-STD-2045-47001 payloads via MIL-STD-188-220 NLPT shall set the value of MIL-STD-188-220's Intranet Message Type Field to ten (10).

A.3.6 S/R (General), Implementing Optional Functionality.

A.3.6.1 S/R (General), Implementing Optional Functionality, Description.

A.3.6.1.1 Optional S/R functionality is identified throughout this specification. Optional functionality is either explicitly identified using the phrase "It shall be a system option…", or is conditioned on implementation of an optional capability (i.e., "When the optional XYZ capability is implemented, the S/R implementation shall..."). Typically, the functionality is intended to help optimize usage of the network's available bandwidth by adding additional node-level processing to decrease the amount of inter-node communication.

A.3.6.1.2 The incorporation of optional functionality is, as indicated, optional. However, optional functionality should not place any requirements on, nor should their implementation result in any non-interoperability issues with, S/R implementations that do not support the optional functionality.

A.3.6.2 S/R (General), Implementing Optional Functionality, Requirements.

A.3.6.2.1 When a system implements optional S/R capabilities, the system shall maintain interoperability with S/R implementations implementing only mandatory capabilities.

A.4 INTERFACE.

A.4.1 Interface, Description.

A.4.1.1 The S/R protocol interacts with both the next higher layer (e.g., the MIL-STD-2045-47001 implementation or an implementation requiring S/R services) and the next lower layer (i.e., the logical transport, either UDP or NLPT). This section identifies key interface profiles for managing the interaction between the MIL-STD-2045-47001 S/R implementation and the invoking Upper Layer Protocol (ULP).

A.4.2 Interface, Data Transfer.

A.4.2.1 Interface, Data Transfer, IP (UDP).

A.4.2.1.1 Interface, Data Transfer, IP (UDP), Description.

A.4.2.1.1.1 The interface supporting a data transfer request by an ULP to one-or-more destinations, each identified by a unicast IP address, should support the following parameters:

IN: 1-to-16 Destination IP Addresses
Source unicast IP Address
S/R Port (Source)
End-of-Data-Transfer Acknowledgment Required (boolean)
Time Allowed From Request for Transfer to Complete
IP Type Of Service (TOS)
IP Differentiated Services Code Point (DSCP)
Data
Data Length
OUT: ALPDU Identifier

A.4.2.1.1.2 This interface allows IP transfers to be supported at the data link layer using unacknowledged IP-based services (i.e., UDP, MIL-STD-188-220 Type 1 broadcast).

A.4.2.1.1.3 If the global broadcast IP address (i.e., 255.255.255.255) is specified as one of the unicast destination IP addresses, the source IP unicast address of Destinations acknowledging receipt of the first Segment may be dynamically added to the list of Destination unicast IP Addresses for tracking of delivery status (i.e., as if the transmission is being performed via Unicast semantics). While subsequent S/R PDU transmissions should continue to be performed on the broadcast IP address, the result of the transfer to the destination should be reported to the Application via a SR -Status Indication.

Implementation Note: IP addresses are classified into three (3) categories:

Broadcast: For IPv4, host address XOR with bit-complement of subnet mask
Example: For network 172.16.0.0 with subnet mask of 255.240.0.0
Bit complement of 255.240.0.0 is 0.15.255.255
Broadcast IP = 172.16.0.0 | 0.15.255.255 = 172.31.255.255

Multicast: For IPv4, 224.0.0.0 through 239.255.255.255, where:
224.0.0.0-224.0.0.255 are reserved for "well known" multicast addresses
224.0.1.0-238.255.255.255 are globally-scoped (Internet-wide) multicast addresses
239.0.0.0-239.255.255.255 are locally-scoped (local) multicast addresses

Unicast: For IPv4, addresses that are neither broadcast nor multicast, which uniquely identify a specific device.

A.4.2.1.2 Interface, Data Transfer, IP (UDP), Requirements.

A.4.2.1.2.1 An S/R implementation shall implement an interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations.

A.4.2.1.2.2 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP designation of multicast IP addresses.

A.4.2.1.2.3 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP designation of broadcast IP addresses.

A.4.2.1.2.4 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP designation of at least 16 IP address destinations.

A.4.2.1.2.5 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall require ULP identification of a source Unicast IP address.

A.4.2.1.2.6 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall require ULP identification of a source S/R port.

A.4.2.1.2.7 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP designation for required use of End-of-Data Transfer Acknowledgment Required processing.

A.4.2.1.2.8 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP identification of the time interval allowed for successful completion of the requested S/R transaction.

A.4.2.1.2.9 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP designation of the IP TOS used for S/R PDUs.

A.4.2.1.2.10 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP designation of the IP Differentiated Services used for S/R PDUs.

A.4.2.1.2.11 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP identification of the transaction's data payload.

A.4.2.1.2.12 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support ULP identification of the length of the transaction's data payload.

A.4.2.1.2.13 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more IP address destinations, shall support notification to the ULP of the ALPDU Identifier generated for the requested transaction.

A.4.2.2 Interface, Data Transfer, IP (188-220).

A.4.2.2.1 Interface, Data Transfer, IP (188-220), Description.

A.4.2.2.1.1 When sending to multiple unicast destination IP addresses that are on the same MIL-STD-188-220 net (using selective directed broadcast, reference RFC 1770), requests for transfer of data should be made by the upper layer (Application layer) at the originator, using the S/R-Unitdata Request primitive with the following parameters. The use of this mechanism allows the transfer to be supported at the Data Link layer using reliable MIL-STD-188-220 services, e.g., Type 2 with multiple unicast addresses.

A.4.2.2.1.2 The interface supporting a data transfer request by an external entity to multiple destinations, each identified by a unicast Link address via NLPT, should support the following parameters:

IN: Net-Directed IP broadcast Address
2-to-16 Destination unicast IP Addresses
Source unicast IP Address
S/R Port (Source)
End-of-Data-Transfer Acknowledgment Required (boolean)
Time Allowed From Request for Transfer to Complete
IP TOS
IP Differentiated Services Code Point (DSCP)
Data
Data Length
OUT: ALPDU Identifier

A.4.2.2.2 Interface, Data Transfer, IP (188-220), Requirements.

A.4.2.2.2.1 An S/R implementation shall implement an interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network.

A.4.2.2.2.2 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of a Net-directed IP broadcast address on the transaction's target network.

A.4.2.2.2.3 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of 2-to-16 Destination unicast IP addresses as targets for the data transfer.

A.4.2.2.2.4 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of a Source unicast IP address for the sending node.

A.4.2.2.2.5 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of the transaction's Source S/R port.

A.4.2.2.2.6 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP designation for required use of End-of-Data Transfer Acknowledgment Required processing.

A.4.2.2.2.7 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of a maximum time interval allowed for successful completion of the data transfer transaction.

A.4.2.2.2.8 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of the IP TOS used for the transaction.

A.4.2.2.2.9 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of the IP Differentiated Services used for the transaction.

A.4.2.2.2.10 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of the transaction's data payload.

A.4.2.2.2.11 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support ULP identification of the length of the transaction's data payload.

A.4.2.2.2.12 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more unicast IP address destinations on a MIL-STD-188-220 network, shall support notification to the ULP of the ALPDU Identifier generated for the requested transaction.

A.4.2.3 Interface, Data Transfer, NLPT.

A.4.2.3.1 Interface, Data Transfer, NLPT, Description.

A.4.2.3.1.1 The interface supporting a data transfer request by an external entity to multiple destinations, each identified by a unicast Link address via NLPT, should support the following parameters:

IN: Source IP unicast Address on Destination Network
1-to-16 Destination unicast Data Link Addresses
Source Data Link Address
S/R Port (Source)
End-of-Data-Transfer Acknowledgment Required (boolean)
Time Allowed From Request for Transfer to Complete
IP Type Of Service (TOS)
IP Differentiated Services Code Point (DSCP)
Data
Data Length
OUT: ALPDU Identifier

A.4.2.3.1.2 If the global broadcast Link address, e.g., 7-bit address 127, is specified as one of the unicast destination Data Link addresses, the source Data Link unicast address of the acknowledgment for the first Segment from any Destination may optionally be dynamically added to the list of Destination unicast Data Link Addresses (if not already present). The dynamically added Destination unicast Data Link address will be treated the same as Destination unicast Data Link addresses specified by the Application, i.e., the destination should have an opportunity to receive subsequent segments and the result of the transfer to the destination should be reported to the Application via an S/R-Status Indication.

Note: The value of the parameter "Source IP unicast Address on the destination net" is used to specify which MIL-STD-188-220 net the S/R PDU is to be sent over in cases where a single station is attached to multiple MIL-STD-188-220 nets and has a different Source IP unicast address on each net.

A.4.2.3.2 Interface, Data Transfer, NLPT, Requirements.

A.4.2.3.2.1 An S/R implementation shall provide an interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network using NLPT.

A.4.2.3.2.2 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of a Source IP unicast address on the destination network.

A.4.2.3.2.3 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of up to 16 Data Link addresses as the targets for the data transfer transaction.

A.4.2.3.2.4 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of a Source Data Link Address for the transaction.

A.4.2.3.2.5 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation for required use of End-of-Data Transfer Acknowledgment Required processing.

A.4.2.3.2.6 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of the time interval allowed for successful completion of the data transfer transaction.

A.4.2.3.2.7 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of an IP TOS to be used for the transaction.

A.4.2.3.2.8 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of the IP Differentiated Services to be used for the transaction.

A.4.2.3.2.9 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP designation of the data payload for the transaction.

A.4.2.3.2.10 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support ULP identification of the length of the data payload for the transaction.

A.4.2.3.2.11 An S/R interface enabling an ULP to initiate an S/R transaction to one-or-more Unicast Data Link address destinations on a MIL-STD-188-220 network, shall support notification to the ULP of the ALPDU Identifier generated for the requested transaction.

A.4.3 Interface, Notification.

A.4.3.1 Interface, Notification, First Data Segment (Destination).

A.4.3.1.1 Interface, Notification, First Data Segment (Destination), Description.

A.4.3.1.1.1 The interface supporting notification to an external entity on initial receipt at a Destination of the first DS PDU for a transaction should support the following parameters:

OUT: ALPDU Identifier
Data
Data Length

A.4.3.1.2 Interface, Notification, First Data Segment (Destination), Requirements.

A.4.3.1.2.1 An S/R implementation shall implement an interface enabling notification of an ULP on receipt of the first DS PDU for an S/R transaction.

A.4.3.1.2.2 An S/R interface enabling notification of an ULP on receipt of the first DS PDU for an S/R transaction, shall identify the transaction for which the notification is provided.

A.4.3.1.2.3 An S/R interface enabling notification of an ULP on receipt of the first DS PDU for an S/R transaction, shall provide the received data segment to the ULP.

A.4.3.1.2.4 An S/R interface enabling notification of an ULP on receipt of the first DS PDU for an S/R transaction, shall identify the length of the received data segment to the ULP.

A.4.3.2 Interface, Notification, Transaction Termination (Originator).

A.4.3.2.1 Interface, Notification, Transaction Termination (Originator), Description.

A.4.3.2.1.1 The interface supporting notification of an external entity on completed transmission of an S/R transaction should support the following parameters:

OUT: ALPDU Identifier
For each Destination being reported...
- Destination (IP Address or Link Address)
- Acknowledgment Result (i.e., SUCCESS/FAILURE)
- Acknowledgment Failure Reason (i.e., descriptive text)
- Size of Data Segment (Full)
- Size of Data Segment (Last)
- Number of Data Segments (Total)
- Number of Data Segments (Acknowledged)
- Acknowledgment Status (Per Data Segment)

Note: Depending on the implementation, there may be multiple notifications against a single transaction, due to differing completion times.

A.4.3.2.2 Interface, Notification, Transaction Termination (Originator), Requirements.

A.4.3.2.2.1 An S/R implementation shall implement an interface enabling notification of an ULP at the Originator node on termination of an S/R transaction.

A.4.3.2.2.2 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall identify the S/R transaction being reported.

A.4.3.2.2.3 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall identify each Destination being reported with its associated IP Address or Data Link Address.

A.4.3.2.2.4 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify the transaction state (i.e., SUCCESS/FAILURE).

A.4.3.2.2.5 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify any applicable Acknowledgment Failure Reason as descriptive text.

A.4.3.2.2.6 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify the size of a full data segment.

A.4.3.2.2.7 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify the size of the last data segment.

A.4.3.2.2.8 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify the total number of DS PDUs in the transaction.

A.4.3.2.2.9 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify the number of data segments acknowledged by the Destination.

A.4.3.2.2.10 An S/R interface enabling notification of an ULP at the Originator node on termination of an S/R transaction, shall, for each reported Destination, identify the receipt status for each DS PDU.

A.4.3.3 Interface, Notification, Transaction Termination (Destination).

A.4.3.3.1 Interface, Notification, Transaction Termination (Destination), Description.

A.4.2.3.1.1 The interface supporting notification of an external entity on completed receipt of an S/R transaction should support the following parameters:

OUT: Originator (IP Address or Link Address)
Data
Data Length
Reassembly Result (i.e., SUCCESS or FAILURE)
Size of Full Segment
Size of Last Segment
Number of Segments (Total)
Number of Segments (Received)
Receipt Status (Individual Segments)

A.4.3.3.2 Interface, Notification, Transaction Termination (Destination), Requirements.

A.4.3.3.2.1 An S/R implementation shall implement an interface enabling notification of an ULP at the Destination node on termination of an S/R transaction.

A.4.3.3.2.2 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall identify the transaction Originator, using either the Originator's IP Address or Data Link Address.

A.4.3.3.2.3 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall, for successfully completed transactions, provide the reassembled data payload.

A.4.3.3.2.4 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall, for successfully completed transactions, identify the length of reassembled data payload.

A.4.3.3.2.5 An S/R interface enabling notification of an ULP at the Destination node at the Destination node on termination of an S/R transaction, shall identify the transaction's completion state (i.e., success/failure).

A.4.3.3.2.6 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall identify the size of a full data segment.

A.4.3.3.2.7 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall, if received, identify the size of the last data segment.

A.4.3.3.2.8 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall identify the total number of data segments in the transaction.

A.4.3.3.2.9 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall identify the number of data segments received for the transaction.

A.4.3.3.2.10 An S/R interface enabling notification of an ULP at the Destination node on termination of an S/R transaction, shall identify the receipt status for each transaction DS PDU.

A.4.4 Interface, Status Request.

A.4.4.1 Interface, Status Request, Description.

A.4.4.1.1 The interface supporting a request by an external entity for transaction status should support the following parameters:

IN: ALPDU Identifier
OUT: Status (Percentage Transferred)

A.4.4.2 Interface, Status Request, Requirements.

A.4.4.2.1 An S/R implementation shall implement an interface enabling an ULP to request the status of an S/R transaction.

A.4.4.2.2 An S/R interface enabling an ULP to request the status of an S/R transaction, shall support ULP identification of the transaction for which status information is requested.

A.4.4.2.3 An S/R interface enabling an ULP to request the status of an S/R transaction, shall provide the transaction status expressed as a percentage of DS PDUs successfully received.

A.4.5 Interface, Abort.

A.4.5.1 Interface, Abort, Description.

A.4.5.1.1 The interface supporting a request by an external entity to abort a transaction should support the following parameters:

IN: ALPDU Identifier

A.4.5.2 Interface, Abort, Requirements.

A.4.5.2.1 An S/R implementation shall implement an interface enabling an ULP to request termination of an active S/R transaction.

A.5 PARAMETERS.

A.5.1 Parameters, Description.

A.5.1.1 The parameters identified below establish processing limits used throughout a S/R implementation. While other entities (e.g., counters, timers, etc.) may be required to fully implement the identified parameters, identification and definition of these entities is deferred to the implementation.

A.5.2 Parameters, Data Segment.

A.5.2.1 Parameters, Data Segment, Description.

A.5.2.1.1 The parameters identified in this section apply to the general processing of DS PDUs. While some of the parameters may be applicable to other PDU types, their primary purpose is for the monitoring and control of DS PDU exchange.

A.5.2.2 Parameters, Data Segment, Hop Count (Originator).

A.5.2.2.1 Parameters, Data Segment, Hop Count (Originator), Description.

A.5.2.2.1.1 Hop Count (HOPCNT) identifies the number of relay points (including the Originator and intermediate relay points) between the Originator and the Destination. This value may not be available in all systems (e.g. systems that do not implement MIL-STD-188-220 Topology Update to maintain Topology Maps).

A.5.2.2.2 Parameters, Data Segment, Hop Count (Originator), Requirements.

A.5.2.2.2.1 When transmitting over a MIL-STD-188-220 network, an S/R Originator shall maintain Hop Count (HOPCNT) as the count of intermediate devices between the Originator and a transaction Destination.

A.5.2.2.2.2 An S/R Originator shall support modification of HOPCNT prior to initiation of the S/R transaction.

A.5.2.2.2.3 An S/R Originator shall hold the value of HOPCNT constant for the duration of the S/R transaction.

A.5.2.2.2.4 An S/R Originator shall set the initial value of HOPCNT to the maximum number of hop counts that can be determined programmatically for each of the potential Destinations.

A.5.2.2.2.5 When a default initial value for HOPCNT cannot be determined programmatically, the S/R Originator shall set the initial value of HOPCNT to one (1).

A.5.2.3 Parameters, Data Segment, Inter-Segment Receive Interval Limit (Destination).

A.5.2.3.1 Parameters, Data Segment, Inter-Segment Receive Interval Limit (Destination), Description.

A.5.2.3.1.1 Inter-Segment Receive Interval Limit (ISRIL) establishes an upper limit on the elapsed time (seconds) between receipt of DS PDUs at a Destination.

Implementation Note: ISRIL can be affected, in addition to the direct effect of network latency, by the number and responsiveness of Destinations for a given S/R transaction.

A.5.2.3.2 Parameters, Data Segment, Inter-Segment Receive Interval Limit (Destination), Requirements.

A.5.2.3.2.1 An S/R Destination shall enforce ISRIL as the upper limit on the number of seconds the Destination will wait for receipt of the next DS PDU after receipt of a DS PDU with P-Bit set to zero (0) in an S/R transaction.

A.5.2.3.2.2 An S/R Destination shall support modification of ISRIL prior to initiation of the S/R transaction.

A.5.2.3.2.3 An S/R Destination shall, when setting the value for ISRIL, enforce a maximum value as identified by Maximum Inter-Segment Receive Interval Limit Value (MAX_ISRIL_VALUE).

A.5.2.3.2.4 An S/R Destination shall update a transaction's ISRIL, subject to a maximum value as identified by MAX_ISRIL_VALUE, based on transaction metrics for receipt of DS PDUs.

A.5.2.3.2.5 An S/R Destination shall enforce ISRIL on receipt of a DS PDU with P-Bit set to zero (0).

A.5.2.3.2.6 An S/R Destination shall initialize ISRIL for an S/R transaction over an IP network to the lesser value of thirty (30) seconds or MAX_ISRIL_VALUE.

A.5.2.3.2.7 An S/R Destination shall initialize ISRIL for an S/R transaction over a MIL-STD-188-220 network where a Type 2 Acknowledgment Timer (T2AT) is available, to the lesser of either MAX_ISRIL_VALUE or the value derived using the equation:

ISRIL(Initial) = (HOPCNT) * (T2AT)

Note: Originators on the same network can use this as a default value. This calculation is performed when the net is enabled based on the net’s configuration. The default value for the net may be modified by the operator.)

Note: T2AT refers to the Acknowledgment Timer used in MIL-STD-188-220 Type 2 (i.e., connection-oriented) processing.

A.5.2.3.2.8 An S/R Destination shall initialize ISRIL for an S/R transaction over a MIL-STD-188-220 network, when a MIL-STD-188-220 T2AT is not available but Number of Stations (NS) on the network is available, to the lesser of either MAX_ISRIL_VALUE or the value derived using the equation:

ISRIL(Initial) = (HOPCNT) * (NS) * (3 sec).

A.5.2.3.2.9 An S/R Destination shall initialize ISRIL for an S/R transaction over a MIL-STD-188-220 network, when neither MIL-STD-188-220 T2AT nor NS on the network are available, to the lesser of either MAX_ISRIL_VALUE or the value derived using the equation:

ISRIL(Initial) = (HOPCNT) * (30 sec).

A.5.2.3.2.10 When an S/R transaction's ISRIL is exceeded and the optional Inter-Segment Receive Interval Expirations Limit (ISRIEL) has not been implemented, the Destination shall abort the transaction.

A.5.2.3.2.11 When an S/R transaction's ISRIL is exceeded and the optional ISRIEL has been implemented, the Destination shall reset the ISRIL tracking mechanism.

A.5.2.3.2.12 When an S/R transaction's ISRIL is exceeded and the optional ISRIEL has been implemented, the Destination shall increment ISRIEL by one (1).

A.5.2.4 Parameters, Data Segment, Inter-Segment Receive Interval Expirations Limit (Destination, Optional).

A.5.2.4.1 Parameters, Data Segment, Inter-Segment Receive Interval Expirations Limit (Destination, Optional), Description.

A.5.2.4.1.1 ISRIEL identifies the maximum number of times ISRIL can be exceeded, without receiving additional segments, before the Destination aborts the S/R transaction.

A.5.2.4.2 Parameters, Data Segment, Inter-Segment Receive Interval Expirations Limit (Destination, Optional), Requirements.

A.5.2.4.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce ISRIEL as the upper limit on the number of times an S/R transaction can exceed ISRIL without receipt of additional DS PDUs before the Destination aborts the transaction.

A.5.2.4.2.2 When an S/R Destination implements the optional ISRIEL, the Destination shall support modification of ISRIEL prior to initiation of an S/R transaction.

A.5.2.4.2.3 When an S/R Destination implements the optional ISRIEL, the Destination shall hold the value of ISRIEL constant for the duration of an S/R transaction.

A.5.2.4.2.4 When an S/R Destination implements the optional ISRIEL, the minimum value of ISRIEL shall be one (1).

A.5.2.4.2.5 When an S/R Destination implements the optional ISRIEL, the maximum value of ISRIEL shall be one thousand (1000).

A.5.2.4.2.6 When an S/R Destination implements the optional ISRIEL, the default value of ISRIEL shall be ten (10).

A.5.2.4.2.7 When an S/R Destination implements the optional ISRIEL, the Destination shall transmit an ABR PDU, with P-Bit set to zero (0), to the transaction Originator when ISRIEL is breached.

A.5.2.4.2.8 When an S/R Destination implements the optional ISRIEL, the Destination shall abort the S/R transaction when ISRIEL is breached.

A.5.2.5 Parameters, Data Segment, Inter-Segment Send Interval Limit (Originator, Optional).

A.5.2.5.1 Parameters, Data Segment, Inter-Segment Send Interval Limit (Originator, Optional), Description.

A.5.2.5.1.1 Inter-Segment Send Interval Limit (ISSIL) identifies a minimum timer interval between transmission of DS PDUs by an Originator, establishing an upper bound on S/R PDU transmission rate over a network. Large ISSIL values, with respect to the network’s bandwidth, will slow down S/R transactions, and will normally have a greater impact on the rate-of-exchange than SCL or SRCL. Small ISSIL values, with respect to the network’s bandwidth, will normally have less impact on the transaction’s rate-of-exchange than SCL or SRCL.

A.5.2.5.1.2 ISSIL smooths out segment transmission rates, avoiding "burstiness" that can occur when the SCL and SRCL congestion controls are used without ISSIL. ISSIL contributes to "fairness" between stations on a shared network by limiting the amount of bandwidth each station utilizes to a value that is less than the maximum bandwidth available. ISSIL can also be used to limit the rate at which segments are sent to stations that are unable to send PA PDUs in a timely manner as required for the SCL and SRCL congestion control mechanisms to function effectively.

A.5.2.5.2 Parameters, Data Segment, Inter-Segment Send Interval Limit (Originator, Optional), Requirements.

A.5.2.5.2.1 It shall be a system option to implement functionality for an S/R Originator to enforce Inter-Segment Send Interval Limit (ISSIL) as the minimum number of seconds the Originator must wait between transmissions of DS PDUs to a transaction Destination.

A.5.2.5.2.2 When an S/R Originator implements the optional ISSIL, the S/R Originator shall support modification of ISSIL prior to initiation of the S/R transaction.

A.5.2.5.2.3 When an S/R Originator implements the optional ISSIL, the S/R Originator shall hold the value of ISSIL constant for the duration of the S/R transaction.

A.5.2.5.2.4 When an S/R Originator implements the optional ISSIL, the Originator shall maintain an ISSIL for each discrete network over which the Originator processes S/R transactions.

A.5.2.6 Parameters, Data Segment, Maximum Inter-Segment Receive Interval Limit Value (Destination).

A.5.2.6.1 Parameters, Data Segment, Maximum Inter-Segment Receive Interval Limit Value (Destination), Description.

A.5.2.6.1.1 Maximum Inter-Segment Receive Interval Limit Value (MAX_ISRIL_VALUE) identifies the maximum amount of time (seconds) that the Destination should wait for receipt of the next segment in an S/R transaction.

A.5.2.6.2 Parameters, Data Segment, Maximum Inter-Segment Receive Interval Limit Value (Destination), Requirements.

A.5.2.6.2.1 An S/R Destination shall set Maximum Inter-Segment Receive Interval Limit Value (MAX_ISRIL_VALUE) to be at least three (3) times the Maximum Request For Acknowledgment Interval Limit Value (MAX_RFAIL_VALUE).

A.5.2.6.2.2 An S/R Destination shall support modification of MAX_ISRIL_VALUE prior to initiation of the S/R transaction.

A.5.2.6.2.3 An S/R Originator shall hold the value of MAX_ISRIL_VALUE constant for the duration of the S/R transaction.

A.5.2.6.2.4 MAX_ISRIL_VALUE value shall be constrained to the inclusive range of 90-2400.

A.5.2.6.2.5 When it is not possible to programmatically determine a valid value for MAX_ISRIL_VALUE, an S/R Destination shall assign a default value of 210.

A.5.2.7 Parameters, Data Segment, Missing Segment Range Limit (Destination, Optional).

A.5.2.7.1 Parameters, Data Segment, Missing Segment Range Limit (Destination, Optional), Description.

A.5.2.7.1.1 MSRL identifies the maximum difference between the Segment Number values of the highest number received segment and lowest number missing segment. When this limit is reached, the Destination will send a PA PDU to the Originator (i.e., there is an assumption that the Originator requires prompting to re-transmit the missing, lower numbered segments).

A.5.2.7.2 Parameters, Data Segment, Missing Segment Range Limit (Destination, Optional), Requirements.

A.5.2.7.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce MSRL as the upper limit on the difference of the Segment Numbers of the highest-numbered received and the lowest-numbered missing DS PDUs.

A.5.2.7.2.2 When an S/R Destination implements the optional MSRL, the Destination shall support modification of MSRL prior to initiation of the S/R transaction.

A.5.2.7.2.3 When an S/R Destination implements the optional MSRL, the Destination shall hold the value of MSRL constant for the duration of the S/R transaction.

A.5.2.7.2.4 When an S/R Destination implements the optional MSRL, the minimum value for MSRL shall be one (1).

A.5.2.7.2.5 When an S/R Destination implements the optional MSRL, the maximum value for MSRL shall be 3248.

A.5.2.7.2.6 When an S/R Destination implements the optional MSRL, the default value for MSRL shall be three (3).

A.5.2.7.2.7 When an S/R Destination implements the optional MSRL and MSRL is breached, the S/R Destination shall send a PA PDU to the transaction Originator.

A.5.2.8 Parameters, Data Segment, Number of Missing Segments Limit (Destination, Optional).

A.5.2.8.1 Parameters, Data Segment, Number of Missing Segments Limit (Destination, Optional), Description.

A.5.2.8.1.1 Number of Missing Segments Limit (NOMSL) is specific to S/R transactions operating under the End of Data Transfer (EDT) Acknowledgment Required scheme, utilizing the Type 0 DS PDU (DS with End of Data Transfer Acknowledgment Required). NOMSL identifies the maximum number of missing DSs (i.e., with Segment Numbers less than the highest numbered segment received). NOMSL supports Destination-side logic to independently send PAs, instead of only sending PAs in response to a request from the originator. The objective for this Destination behavior is to avoid the condition where the Originator reaches the SCL and initial segment transmissions are suspended.

A.5.2.8.2 Parameters, Data Segment, Number of Missing Segments Limit (Destination, Optional), Requirements.

A.5.2.8.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce NOMSL as the upper limit on the number of missing DS PDUs, with Segment Numbers lower than the highest-received Segment Number, allowed before the Destination independently sends a PA PDU to the transaction's Originator.

A.5.2.8.2.2 When an S/R Destination implements the optional NOMSL, the S/R Originator/Destination shall support modification of NOMSL prior to initiation of the S/R transaction.

A.5.2.8.2.3 When an S/R Destination implements the optional NOMSL, the S/R Destination shall hold the value of NOMSL constant for the duration of the S/R transaction.

A.5.2.8.2.4 When an S/R Destination implements the optional NOMSL, the minimum value for NOMSL shall be one (1).

A.5.2.8.2.5 When an S/R Destination implements the optional NOMSL, the maximum value for NOMSL shall be 3248.

A.5.2.8.2.6 When an S/R Destination implements the optional NOMSL, the default value for NOMSL shall be two (2).

A.5.2.8.2.7 When an S/R Destination implements the optional NOMSL, the Destination shall determine the number of missing segments as the count of unreceived DS PDUs with Segment Numbers lower than that of the highest received DS PDU.

A.5.2.8.2.8 When an S/R Destination implements the optional NOMSL and NOMSL is exceeded for an active S/R transaction, the S/R Destination shall send a PA PDU to the transaction Originator.

A.5.2.9 Parameters, Data Segment, Received Segments Count Limit (Destination, Optional).

A.5.2.9.1 Parameters, Data Segment, Received Segments Count Limit (Destination, Optional), Description.

A.5.2.9.1.1 Received Segments Count Limit (RSCL) is an optional parameter that establishes an upper bound on the number of DS PDUs, with Type equal to zero (0), that can be received before a Destination independently transmits a PA PDU against the transaction.

A.5.2.9.2 Parameters, Data Segment, Received Segments Count Limit (Destination, Optional), Requirements.

A.5.2.9.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce RSCL as the upper limit on the number of DS PDUs, with Type equal to zero (0), that a Destination can receive between PA PDU transmissions to the transaction Originator.

A.5.2.9.2.2 When an S/R Destination implements the optional RSCL, the S/R Destination shall support modification of RSCL prior to initiation of the S/R transaction.

A.5.2.9.2.3 When an S/R Destination implements the optional RSCL, the S/R Destination shall hold the value of RSCL constant for the duration of the S/R transaction.

A.5.2.9.2.4 When an S/R Destination implements the optional RSCL and RSCL is reached while processing an incomplete transaction with End of Data Transfer Acknowledgment Required semantics, the S/R Destination shall send a PA PDU to the transaction Originator.

A.5.2.10 Parameters, Data Segment, Reassembly Time Expiration Count Limit (Destination, Optional).

A.5.2.10.1 Parameters, Data Segment, Reassembly Time Expiration Count Limit (Destination, Optional), Description.

A.5.2.10.1.1 When an S/R transaction is operating under End of Data Transfer Acknowledgment Not Required mode, Reassembly Time Expiration Count Limit (RTECL) identifies the maximum number of times Reassembly Time Limit (RTL) can be exceeded before the Destination aborts the S/R transaction.

A.5.2.10.2 Parameters, Data Segment, Reassembly Time Expiration Count Limit (Destination, Optional), Requirements.

A.5.2.10.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce RTECL as the upper limit on the number of consecutive times RTL is allowed to expire.

A.5.2.10.2.2 When an S/R Destination implements the optional RTECL, the Destination shall support modification of RTECL prior to initiation of an S/R transaction.

A.5.2.10.2.3 When an S/R Destination implements the optional RTECL, the Destination shall hold the value of RTECL constant for the duration of an S/R transaction.

A.5.2.10.2.4 When an S/R Destination implements the optional RTECL, the minimum value of RTECL shall be zero (0).

A.5.2.10.2.5 When an S/R Destination implements the optional RTECL, the maximum value of RTECL shall be 1000.

A.5.2.10.2.6 When an S/R Destination implements the optional RTECL, the default value of RTECL shall be ten (10).

A.5.2.10.2.7 When an S/R Destination implements the optional RTECL, the value of RTECL shall be user configurable.

A.5.2.10.2.8 When an S/R Destination implements the optional RTECL, the Destination shall terminate the S/R transaction when RTECL is breached.

A.5.2.11 Parameter, Data Segment, Reassembly Time Limit (Destination, Optional).

A.5.2.11.1 Parameter, Data Segment, Reassembly Time Limit (Destination, Optional), Description.

A.5.2.11.1.1 RTL is the upper limit on the amount of time allowed for successful receipt of all S/R transaction data segments, with Type equal to zero (0), at the Destination.

A.5.2.11.2 Parameter, Data Segment, Reassembly Time Limit (Destination, Optional), Requirements.

A.5.2.11.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce RTL as the upper limit on the time allowed for successful receipt of a transaction's ALPDU using DS PDUs with Type equal to zero (0).

A.5.2.11.2.2 When an S/R Destination implements the optional RTL, the S/R Originator/Destination shall support modification of RTL prior to initiation of the S/R transaction.

A.5.2.11.2.3 When an S/R Destination implements the optional RTL and RTL is reached, the S/R Destination shall calculate a new RTL value.

A.5.2.11.2.4 When an S/R Destination implements the optional RTL, the S/R Destination shall monitor RTL separately for each S/R transaction.

A.5.2.11.2.5 When an S/R Destination implements the optional RTL and RTL is reached while processing an incomplete S/R transaction, the S/R Destination shall send a PA PDU to the transaction Originator.

A.5.2.12 Parameters, Data Segment, Segment Credit Limit (Originator).

A.5.2.12.1 Parameters, Data Segment, Segment Credit Limit (Originator), Description.

A.5.2.12.1.1 SCL identifies the maximum number of outstanding (i.e., sent but unacknowledged) DS PDUs that can exist for an ALPDU. The maximum value for SCL is limited by the maximum size of the bit mask field of the PA PDU. Once SCL is reached, no additional segments can be sent by the Originator until one-or-more of the outstanding segments are acknowledged.

A.5.2.12.1.2 SCL should be large enough to keep the network busy transmitting segments, but small enough to avoid discards. For MIL-STD-188-220 nets, SCL should be selected so that the Queue Size Octets is not exceeded (i.e., consider the MSS being used for the exchange).

A.5.2.12.2 Parameters, Data Segment, Segment Credit Limit (Originator), Requirements.

A.5.2.12.2.1 An S/R Originator shall enforce SCL as the maximum number of DS PDUs that can be in a "transmitted but not acknowledged" state.

A.5.2.12.2.2 An S/R Originator shall support modification of SCL prior to initiation of the S/R transaction.

A.5.2.12.2.3 An S/R Originator shall hold the value of SCL constant for the duration of the S/R transaction.

A.5.2.12.2.4 An S/R Originator shall enforce SCL when processing a Unicast transaction.

A.5.2.12.2.5 An S/R Originator shall constrain SCL values to the inclusive range of 1-16.

A.5.2.12.2.6 An S/R Originator shall assign a default value of five (5) to SCL when it is not possible to programmatically determine a valid value.

A.5.2.12.2.7 An S/R Originator shall prohibit transmission of a DS PDU if the transmission will cause the transaction's SCL to be exceeded.

A.5.2.12.3 Parameters, Data Segment, Segment Credit Limit (Originator, Optional), Requirements.

A.5.2.12.3.1 It shall be a system option for an S/R Originator to support an inclusive upper limit of 3248 for SCL values.

A.5.2.13 Parameters, Data Segment, Segment Size (Originator).

A.5.2.13.1 Parameters, Data Segment, Segment Size (Originator), Description.

A.5.2.13.1.1 Segment Size identifies the maximum number of bytes contained as the payload of a DS PDU. This value is also the minimum size for all data segments except the last.

A.5.2.13.2 Parameters, Data Segment, Segment Size (Originator), Requirements.

A.5.2.13.2.1 An S/R Originator shall enforce Segment Size as the maximum number of bytes contained in the data payload of a DS PDU.

A.5.2.13.2.2 An S/R Originator shall support modification of Segment Size prior to initiation of the S/R transaction.

A.5.2.13.2.3 An S/R Originator/Destination shall hold the value of Segment Size constant for the duration of the S/R transaction.

A.5.2.13.2.4 An S/R Originator shall constrain the value of Segment Size to the inclusive range of three (3) through MSS.

A.5.2.13.2.5 The S/R parameter Segment Size shall be user configurable.

A.5.2.13.2.6 If a valid value for Segment Size cannot be programmatically determined, an S/R Originator shall assign a default value of MSS.

A.5.2.14 Parameters, Data Segment, Segment Retry Count Limit (Originator).

A.5.2.14.1 Parameters, Data Segment, Segment Retry Count Limit (Originator), Description.

A.5.2.14.1.1 SRCL identifies the number of times that an S/R Originator should retransmit a DS, without acknowledgment, to an S/R Destination before the Originator should abort the S/R transaction with the non-responding Destination.

A.5.2.14.2 Parameters, Data Segment, Segment Retry Count Limit (Originator), Requirements.

A.5.2.14.2.1 An S/R Originator shall enforce SRCL as the upper limit on the number of re-transmissions for any given DS PDU to a transaction Destination.

A.5.2.14.2.2 An S/R Originator shall support modification of SRCL prior to initiation of an S/R transaction.

A.5.2.14.2.3 An S/R Originator shall hold the value of SRCL constant for the duration of the S/R transaction.

A.5.2.14.2.4 An S/R Originator shall constrain SRCL values to the inclusive range of 0-5.

A.5.2.14.2.5 When it is not possible to programmatically determine a valid value for SRCL, an S/R Originator shall assign a default value of two (2).

A.5.2.14.2.6 When re-transmission of a DS PDU will cause a Destination's SRCL to be exceeded, the S/R Originator shall abort the transaction for that Destination.

A.5.2.14.3 Parameters, Data Segment, Segment Retry Count Limit (Originator, Optional), Requirements.

A.5.2.14.3.1 It shall be a system option for an S/R Originator to support an inclusive upper limit of 1000 for SRCL values.

A.5.2.14.3.2 When an S/R Originator supports the optional SRCL value range of 1-1000, the default value of SRCL shall be five (5).

A.5.2.15 Parameters, Data Segment, Sent Segments Count Limit (Originator, Optional).

A.5.2.15.1 Parameters, Data Segment, Sent Segments Count Limit (Originator, Optional), Description.

A.5.2.15.1.1 Sent Segments Count Limit (SSCL) identifies the number of S/R DSs, per ALPDU Identifier, that can be sent or resent before the Originator issues an AR. SSCL ensures that Originators request acknowledgments often enough that the SCL will not be reached.

A.5.2.15.2 Parameters, Data Segment, Sent Segments Count Limit (Originator, Optional), Requirements.

A.5.2.15.2.1 It shall be a system option to implement functionality for an S/R Originator to enforce SSCL as the upper limit on the number of DS PDU transmissions, including re-transmissions, that can occur before the Originator must issue an AR PDU.

A.5.2.15.2.2 When an S/R Originator implements the optional SSCL, the S/R Originator shall support modification of SSCL prior to initiation of the S/R transaction.

A.5.2.15.2.3 When an S/R Originator implements the optional SSCL, the S/R Originator shall hold the value of SSCL constant for the duration of an S/R transaction.

A.5.2.15.2.4 When an S/R Originator implements the optional SSCL, the minimum value for SSCL shall be one (1).

A.5.2.15.2.5 When an S/R Originator implements the optional SSCL the maximum value for SSCL shall be 3248.

A.5.2.15.2.6 When an S/R Originator implements the optional SSCL the default value for SSCL shall be four (4) for transactions using DS PDUs with Type equal to zero (0).

A.5.2.15.2.7 When an S/R Originator implements the optional SSCL, the default value for SSCL shall be two (2) for transactions using DS PDUs with Type equal to two (2).

A.5.2.16 Parameters, Data Segment, Segment Send Rate Limit Per Originator (Originator, Optional).

A.5.2.16.1 Parameters, Data Segment, Segment Send Rate Limit Per Originator (Originator, Optional), Description.

A.5.2.16.1.1 Segment Send Rate Limit Per Originator (SSRLPO) identifies a maximum rate at which an Originator should send segments over a network, assuming a single transmitting node on the network.

A.5.2.16.1.2 For MIL-STD-188-220 radio nets and other slow radio nets, SSRLPO is used to calculate the Inter-Segment Send Interval Limit (ISSIL), which supports enforcement of a minimum time interval between transmission of DSs.

A.5.2.16.2 Parameters, Data Segment, Segment Send Rate Limit Per Originator (Originator, Optional), Requirements.

A.5.2.16.2.1 It shall be a system option to implement functionality for an S/R Originator to enforce SSRLPO as the minimum timer interval between transmission of DS PDUs by an Originator.

A.5.2.16.2.2 When an S/R Originator implements the optional SSRLPO, the S/R Originator shall support modification of SSRLPO prior to initiation of the S/R transaction.

A.5.2.16.2.3 When an S/R Originator implements the optional SSRLPO, the S/R Originator shall hold the value of SSRLPO constant for the duration of an S/R transaction.

A.5.2.16.2.4 When an S/R Originator implements the optional SSRLPO, the minimum value of SSRLPO shall be zero (0) bits-per-second (bps).

A.5.2.16.2.5 When an S/R Originator implements the optional SSRLPO, the maximum value of SSRLPO shall be 1,000,000 bits-per-second (bps).

A.5.2.16.2.6 When an S/R Originator implements the optional SSRLPO, the default value of SSRLPO shall be 1800 bits-per-second (bps).

A.5.2.17 Parameters, Data Segment, Transaction Completion Limit (Originator, Optional).

A.5.2.17.1 Parameters, Data Segment, Transaction Completion Limit (Originator, Optional), Description.

A.5.2.17.1.1 Transaction Completion Limit (TCL), identifies the maximum time allocated for completion of the S/R transaction, is supplied by the ULP initiating the S/R transaction.

A.5.2.17.2 Parameters, Data Segment, Transaction Completion Limit (Originator, Optional), Requirements.

A.5.2.17.2.1 It shall be a system option to implement functionality for an S/R Originator to enforce TCL as the upper limit on the time allowed for the successful completion of an S/R transaction.

A.5.2.17.2.2 When an S/R Originator implements the optional TCL, the S/R Originator shall set the value of TCL as indicated by the invoking ULP initiating the S/R transaction.

A.5.2.17.2.3 When an S/R Originator implements the optional TCL, the S/R Originator shall terminate the S/R transaction when TCL is exceeded.

A.5.3 Parameters, Acknowledgment.

A.5.3.1 Parameters, Acknowledgment, Description.

A.5.3.1.1 The parameters identified in this section apply to the general processing of PDUs associated with the acknowledgment process. These PDUs are the AR PDU, Complete Acknowledgment (CA) PDU, and PA PDU.

A.5.3.1.2 Another, indirect, request PDU is the DS PDU with P-Bit set to one (1). This format is used to avoid having to send a separate AR PDU, and is treated by the recipient as an AR PDU.

A.5.3.2 Parameters, Acknowledgment, Complete Acknowledgment Retry Limit (Destination, Optional).

A.5.3.2.1 Parameters, Acknowledgment, Complete Acknowledgment Retry Limit (Destination, Optional), Description.

A.5.3.2.1.1 Complete Acknowledgment Retry Limit (CARL) establishes an upper bound on the number of times a CA PDU is sent/resent to an Originator. CA PDUs may be re-sent for a variety of reasons, but, ultimately, retransmissions are an indication that the Originator is not successfully receiving/processing the acknowledgment.

A.5.3.2.2 Parameters, Acknowledgment, Complete Acknowledgment Retry Limit (Destination, Optional), Requirements.

A.5.3.2.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce CARL as the upper limit on the number of CA PDUs the S/R Destination will send in response to acknowledgment requests from the transaction Originator against a successfully completed transaction.

A.5.3.2.2.2 When an S/R Destination implements the optional CARL, the S/R Destination shall support modification of CARL prior to initiation of the S/R transaction.

A.5.3.2.2.3 When an S/R Destination implements the optional CARL, the S/R Destination shall hold the value of CARL constant for the duration of the S/R transaction.

A.5.3.2.2.4 When an S/R Destination implements the optional CARL, the S/R Destination shall cease transmitting CA PDUs against a transaction when the associated CARL is exceeded.

A.5.3.3 Parameters, Acknowledgment, Estimated Round Trip Delay (Originator).

A.5.3.3.1 Parameters, Acknowledgment, Estimated Round Trip Delay (Originator), Description.

A.5.3.3.1.1 Estimated Round Trip Delay (ERTD) identifies an upper limit on the expected elapsed time from when a Request For Acknowledgment (either an AR PDU or a DS PDU with P-Bit set to one (1)) is sent until a corresponding acknowledgment is received from the S/R Destination.

A.5.3.3.2 Parameters, Acknowledgment, Estimated Round Trip Delay (Originator), Requirements.

A.5.3.3.2.1 An S/R Originator shall enforce ERTD as an upper limit on the number of seconds elapsed between the sending of any Request For Acknowledgment and receipt of the corresponding response.

A.5.3.3.2.2 An S/R Originator shall support modification of ERTD prior to initiation of the S/R transaction.

A.5.3.3.2.3 An S/R Originator shall update ERTD based on actual round trip delay metrics.

A.5.3.3.2.4 An S/R Originator shall maintain ERTD independently for each transaction Destination.

A.5.3.3.2.5 An S/R Originator, on an IP network, shall set the initial value of ERTD to thirty (30) seconds.

A.5.3.3.2.6 An S/R Originator, on a 188/220 network where a T2AT is available, shall set the initial value of ERTD using the equation:

ERTD(Initial) = (HOPCNT) * (Type 2 Acknowledgment Timer)

A.5.3.3.2.7 An S/R Originator, on a 188/220 network where a T2AT is not available but NS is, shall set the initial value of ERTD using the equation:

ERTD(Initial) = (HOPCNT) * (NS) * (2 seconds)

A.5.3.3.2.8 An S/R Originator, on a 188/220 network where neither a T2AT nor NS are available, shall set the initial value of ERTD using the equation:

ERTD(Initial) = (HOPCNT) * (30 seconds)

A.5.3.3.3 Parameters, Acknowledgment, Estimated Round Trip Delay (Originator, Optional), Requirements.

A.5.3.3.3.1 It shall be a system option to implement functionality for an S/R Originator to retransmit unacknowledged data segments when ERTD is exceeded.

A.5.3.3.3.2 It shall be a system option to implement functionality for an S/R Originator to maintain ERTD for an S/R Destination across multiple transactions.

A.5.3.4 Parameters, Acknowledgment, Immediate Acknowledgment Request Limit (Destination, Optional).

A.5.3.4.1 Parameters, Acknowledgment, Immediate Acknowledgment Request Limit (Destination, Optional), Description.

A.5.3.4.1.1 Immediate Acknowledgment Request Count Limit (IARL) identifies an upper limit on the number of requests for acknowledgment (either an Acknowledgment Request (AR) PDU or DS PDU with P-Bit set to one (1)) that a Destination can receive before being required to send a PA to ensure the Originator does not abort the exchange due to a lack of acknowledgments from the Destination.

A.5.3.4.2 Parameters, Acknowledgment, Immediate Acknowledgment Request Limit (Destination, Optional), Requirements.

A.5.3.4.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce IARL as the upper limit on the number of acknowledgment requests (i.e., an AR PDU or a DS PDU with P-Bit set to one (1)) a Destination can receive from the transaction Originator before responding with either a PA PDU or CA PDU.

A.5.3.4.2.2 When an S/R Destination implements the optional IARL, the Destination shall support modification of IARL prior to initiation of an S/R transaction.

A.5.3.4.2.3 When an S/R Destination implements the optional IARL, the Destination shall hold the value of IARL constant for the duration of an S/R transaction.

A.5.3.4.2.4 When an S/R Destination implements the optional IARL, the minimum value of IARL shall be 0.

A.5.3.4.2.5 When an S/R Destination implements the optional IARL, the maximum value of IARL shall be 1000.

A.5.3.4.2.6 When an S/R Destination implements the optional IARL, the default value of IARL shall be one-third the value of Request For Acknowledgment Retry Limit (RFARL) rounded up to the next integer.

A.5.3.4.2.7 When an S/R Destination implements the optional IARL, the Destination shall transmit a PA PDU when IARL is exceeded.

A.5.3.5 Parameters, Acknowledgment, Maximum Request for Acknowledgment Interval Limit Value (Originator).

A.5.3.5.1 Parameters, Acknowledgment, Maximum Request for Acknowledgment Interval Limit Value (Originator), Description.

A.5.3.5.1.1 MAX_RFAIL_VALUE identifies the maximum amount of time (seconds) that an S/R Originator should wait for a Destination's response to a Request For Acknowledgment (i.e., AR PDU or DS PDU with P-Bit set to one (1)).

A.5.3.5.2 Parameters, Acknowledgment, Maximum Request for Acknowledgment Interval Limit Value (Originator), Requirements.

A.5.3.5.2.1 An S/R Originator shall support modification of MAX_RFAIL_VALUE prior to initiation of the S/R transaction.

A.5.3.5.2.2 An S/R Originator shall hold the value of MAX_RFAIL_VALUE constant for the duration of the S/R transaction.

A.5.3.5.2.3 An S/R Originator shall constrain MAX_RFAIL_VALUE values to the inclusive range of thirty (30) to six hundred (600) seconds.

A.5.3.5.2.4 When it is not possible to programmatically determine a valid value for MAX_RFAIL_VALUE, an S/R Originator shall assign a default value of sixty (60) seconds.

A.5.3.6 Parameters, Acknowledgment, Partial Acknowledgment Interval Limit (Destination, Optional).

A.5.3.6.1 Parameters, Acknowledgment, Partial Acknowledgment Interval Limit (Destination, Optional), Description.

A.5.3.6.1.1 Partial Acknowledgment Interval Limit (PAIL) identifies a minimum time (seconds) required to elapse between transmission of acknowledgments by an S/R Destination.

A.5.3.6.2 Parameters, Acknowledgment, Partial Acknowledgment Interval Limit (Destination, Optional), Requirements.

A.5.3.6.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce PAIL as the lower limit on the time between transmission of an acknowledgment, either a PA PDU or CA PDU, by the Destination to the transaction Originator.

A.5.3.6.2.2 When an S/R Destination implements the optional PAIL, the S/R Destination shall support modification of PAIL prior to initiation of the S/R transaction.

A.5.3.6.2.3 When an S/R Destination implements the optional PAIL, the S/R Destination shall hold the value of PAIL constant for the duration of the S/R transaction.

A.5.3.6.2.4 When an S/R Destination implements the optional PAIL, the S/R Destination shall delay transmitting a PA PDU for an S/R transaction being processed using DS PDUs with Type equal to zero (0) until PAIL has elapsed.

A.5.3.6.2.5 When an S/R Destination implements the optional PAIL, the S/R Destination shall monitor PAIL separately for each active S/R transaction.

A.5.3.7 Parameters, Acknowledgment, Partial Acknowledgment Retry Limit (Destination, Optional).

A.5.3.7.1 Parameters, Acknowledgment, Partial Acknowledgment Retry Limit (Destination, Optional), Description.

A.5.3.7.1.1 When processing an S/R transaction under End of Data Transfer Acknowledgment Required mode (i.e., using DS PDU's where Type is equal to zero (0)), Partial Acknowledgment Retry Limit (PARL) identifies the maximum number of consecutive PAs an S/R Destination should send, without a subsequent receipt of a DS PDU, before aborting the transaction.

A.5.3.7.2 Parameters, Acknowledgment, Partial Acknowledgment Retry Limit (Destination, Optional), Requirements.

A.5.3.7.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce PARL as the upper limit on the number of consecutive PA PDUs a Destination can send, when processing an S/R transaction using DS PDUs with Type equal to zero (0), to the transaction Originator without subsequent receipt of a DS PDU.

A.5.3.7.2.2 When an S/R Destination implements the optional PARL, the value of PARL shall be configurable.

A.5.3.7.2.3 When an S/R Destination implements the optional PARL, the S/R Destination shall support modification of PARL prior to initiation of an S/R transaction.

A.5.3.7.2.4 When an S/R Destination implements the optional PARL, the S/R Destination shall hold the value of PARL constant for the duration of an S/R transaction.

A.5.3.7.2.5 When an S/R Destination implements the optional PARL, the minimum value of PARL shall be zero (0).

A.5.3.7.2.6 When an S/R Destination implements the optional PARL, the maximum value of PARL shall be 1000.

A.5.3.7.2.7 When an S/R Destination implements the optional PARL, the default value of PARL shall be ten (10).

A.5.3.7.2.8 When an S/R Destination implements the optional PARL and PARL is exceeded, the S/R Destination shall terminate the S/R transaction.

A.5.3.8 Parameters, Acknowledgment, Request For Acknowledgment Interval Limit (Originator).

A.5.3.8.1 Parameters, Acknowledgment, Request For Acknowledgment Interval Limit (Originator), Description.

A.5.3.8.1.1 Request For Acknowledgment Interval Limit (RFAIL) is used by an S/R Originator to predict when a response to a Request For Acknowledgment (either an AR PDU or a DS PDU with P-Bit set to one (1)) should be received.

A.5.3.8.2 Parameters, Acknowledgment, Request For Acknowledgment Interval Limit (Originator), Requirements.

A.5.3.8.2.1 An S/R Originator shall enforce RFAIL as the upper limit for the elapsed time the Originator will wait for a response to a Request for Acknowledgment.

A.5.3.8.2.2 An S/R Originator shall support modification of RFAIL prior to initiation of the S/R transaction.

A.5.3.8.2.3 RFAIL shall be implemented as the lesser of MAX_RFAIL_VALUE or a calculated ERTD.

A.5.3.8.2.4 When RFAIL is exceeded without receipt of a valid response, the S/R Originator shall re-send the Request For Acknowledgment to the non-responsive Destination.

A.5.3.9 Parameters, Acknowledgment, Request For Acknowledgment Retry Limit (Originator).

A.5.3.9.1 Parameters, Acknowledgment, Request For Acknowledgment Retry Limit (Originator), Description.

A.5.3.9.1.1 RFARL identifies the maximum number of consecutive, unacknowledged request for acknowledgments an Originator should send before aborting the S/R transaction. Unacknowledged is defined as not receiving an acknowledgment response within the time period established by RFAIL.

A.5.3.9.2 Parameters, Acknowledgment, Request For Acknowledgment Retry Limit (Originator), Requirements.

A.5.3.9.2.1 An S/R Originator shall enforce RFARL as the upper limit on the number of consecutive times an AR PDU is sent to a non-responsive Destination.

A.5.3.9.2.2 An S/R Originator shall support modification of RFARL prior to initiation of the S/R transaction.

A.5.3.9.2.3 An S/R Originator shall hold the value of RFARL constant for the duration of an S/R transaction.

A.5.3.9.2.4 An S/R Originator shall constrain RFARL values to the inclusive range of 1-10.

A.5.3.9.2.5 When it is not possible to programmatically determine a valid value for RFARL, the S/R Originator shall assign a default value of three (3).

A.5.3.9.2.6 When RFARL is exceeded for an S/R transaction Destination, the transaction Originator shall abort the transaction for the non-responding Destination.

A.5.3.9.3 Parameters, Acknowledgment, Request For Acknowledgment Retry Limit (Originator, Optional), Requirements.

A.5.3.9.3.1 It shall be a system option to implement support for a maximum RFARL value of 1000.

A.5.3.9.3.2 When the maximum value of RFARL is enforced as 1000, the default value of RFARL shall be ten (10).

A.5.3.10 Parameters, Acknowledgment, Received Segment Count Limit (Destination, Optional).

A.5.3.10.1 Parameters, Acknowledgment, Received Segment Count Limit (Destination, Optional), Description.

A.5.3.10.1.1 RSCL identifies the maximum number of End of Data Transfer Acknowledgment Required (Type 0) DS PDUs received (new or duplicate) by the Destination per ALPDU Identifier before a PA must be sent. RSCL supports Destination-side logic to independently send PAs, instead of only sending PAs in response to a poll/request from the Originator. The objective for this Destination behavior is to avoid a condition where the Originator reaches the SCL and initial segment transmissions are suspended.

A.5.3.10.2 Parameters, Acknowledgment, Received Segment Count Limit (Destination, Optional), Requirements.

A.5.3.10.2.1 It shall be a system option to implement functionality for an S/R Destination to enforce RSCL as the upper limit on the number of DS PDUs, with Type equal to zero (0), that can be received at the Destination before a PA PDU must be sent to the transaction Originator.

A.5.3.10.2.2 When an S/R Destination implements the optional RSCL, the S/R Destination shall support modification of RSCL prior to initiation of the S/R transaction.

A.5.3.10.2.3 When an S/R Destination implements the optional RSCL, the S/R Destination shall hold the value of RSCL constant for the duration of the S/R transaction.

A.5.3.10.2.4 When an S/R Destination implements the optional RSCL, the minimum value for RSCL shall be one (1).

A.5.3.10.2.5 When an S/R Destination implements the optional RSCL, the maximum value for RSCL shall be 3248.

A.5.3.10.2.6 When an S/R Destination implements the optional RSCL, the default value for RSCL shall be two (2).

A.5.4 Parameters, Abort.

A.5.4.1 Parameters, Abort, Description.

A.5.4.1.1 The parameters identified in this section apply to the general processing of PDUs associated with the abort process. These PDUs are the ABR PDU and ABC PDU.

A.5.4.2 Parameters, Abort, Abort Confirm Retry Limit (Optional).

A.5.4.2.1 Parameters, Abort, Abort Confirm Retry Limit (Optional), Description.

A.5.4.2.1.1 Abort Confirm Retry Limit (ABCRL) identifies the maximum number of times an ABC PDU, with F-Bit set to one (1), should be re-sent (i.e., based on receipt of an ABR PDU with P-Bit set to one (1)) before abandoning the transmission.

A.5.4.2.2 Parameters, Abort, Abort Confirm Retry Limit (Optional), Requirements.

A.5.4.2.2.1 It shall be a system option to implement functionality to enforce ABCRL as the upper limit on the number of times an ABC PDU, with F-Bit set to one (1), is sent in response to receipt of an ABR PDU.

A.5.4.2.2.2 When an S/R implementation implements the optional ABCRL, the S/R implementation shall support modification of ABCRL prior to initiation of the S/R transaction.

A.5.4.2.2.3 When an S/R implementation implements the optional ABCRL, the S/R implementation shall hold the value of ABCRL constant for the duration of the S/R transaction.

A.5.4.2.2.4 When an S/R implementation implements the optional ABCRL and ABCRL is exceeded for an S/R transaction, the S/R node transmitting ABC PDUs shall ignore subsequent ABR PDUs against the S/R transaction.

A.5.4.3 Parameters, Abort, Abort Request Retry Limit (Optional).

A.5.4.3.1 Parameters, Abort, Abort Request Retry Limit (Optional), Description.

A.5.4.3.1.1 Abort Request Retry Limit (ABRRL) identifies the maximum number of times an ABR, with P-Bit set to one (1), should be re-sent (i.e., based on non-receipt of a corresponding ABC response) before an S/R node abandons the transmission.

A.5.4.3.2 Parameters, Abort, Abort Request Retry Limit (Optional), Requirements.

A.5.4.3.2.1 It shall be a system option to implement functionality to enforce ABRRL as the upper limit on the number of times an ABR PDU, with P-Bit set to one (1), is sent to a non-responsive S/R node.

A.5.4.3.2.2 When an S/R implementation implements the optional ABRRL, the S/R implementation shall support modification of ABRRL prior to initiation of an S/R transaction.

A.5.4.3.2.3 When an S/R implementation implements the optional ABRRL, the S/R implementation shall hold the value of ABRRL constant for the duration of an S/R transaction.

A.5.4.3.2.4 When an S/R implementation implements the optional ABRRL the minimum value shall be one (1).

A.5.4.3.2.5 When an S/R implementation implements the optional ABRRL, the maximum value shall be ten (10).

A.5.4.3.2.6 When an S/R implementation implements the optional ABRRL, the default value shall be two (2).

A.5.4.3.2.7 When an S/R implementation implements the optional ABRRL and ABRRL is exceeded for an S/R transaction, the transmitting S/R node shall cease sending ABR PDUs to the non-responsive recipient.

A.5.4.4 Parameters, Abort, Abort Request Interval Limit (Optional).

A.5.4.4.1 Parameters, Abort, Abort Request Interval Limit (Optional), Description.

A.5.4.4.1.1 Abort Request Interval Limit (ABRIL) is used by the sender of an ABR PDU to predict when an ABC PDU should be received from the transmission target.

A.5.4.4.2 Parameters, Abort, Abort Request Interval Limit (Optional), Requirements.

A.5.4.4.2.1 It shall be a system option to implement functionality to enforce ABRIL as the upper limit on the time allowed for receipt of an ABC PDU in response to an ABR PDU transmitted with P-Bit set to one (1).

A.5.4.4.2.2 When an S/R implementation implements the optional ABRIL, the S/R implementation shall support modification of ABRIL prior to initiation of the S/R transaction.

A.5.4.4.2.3 When an S/R implementation implements the optional ABRIL, the S/R implementation shall hold the value of ABRIL constant for the duration of the S/R transaction.

A.5.4.4.2.4 When an S/R implementation implements the optional ABRIL and ABRIL is exceeded, the sending node shall re-send the ABR PDU.

A.6 S/R HEADER.

A.6.1 S/R Header, Description.

A.6.1.1 The following sections identify the format, content, and requirements for the S/R Header. The S/R Header is common to all S/R PDUs.

A.6.2 S/R Header, Format.

A.6.2.1 S/R Header, Format, Description.

A.6.2.1.1 FIGURE A-1 depicts the S/R Header elements common to all S/R PDUs.

FIGURE A-1 S/R Header

S/R Header	Octet 0								Octet 1								Octet 2								Octet 3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Header Fields	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Source Port (16 bits)																Destination Port (16 bits)															
S/R Header	Octet 4								Octet 5								Octet 6								Octet 7							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Header Fields	2	1	0	11	10	9	8	7	6	5	4	3	2	1	0	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Type (3 bits)			Header Length (HLEN) (12 bits)													Serial Number (16 bits)															
	P/F Bit (1 bit)																															

A.6.2.2 S/R Header, Format, Requirements.

A.6.2.2.1 Byte order within S/R PDUs shall be Big Endian.

A.6.2.2.2 Bit order within S/R PDUs shall be Most Significant Bit (MSB) first.

A.6.2.3 S/R Header, Format, Source Port.

A.6.2.3.1 S/R Header, Format, Source Port, Description.

A.6.2.3.1.1 This 16-bit number identifies the application process sending the ALPDU being transported by S/R. Source Port's value is established by the Source Port parameter that is passed by the ULP on the S/R service interface sending the request.

A.6.2.3.2 S/R Header, Format, Source Port, Requirements.

A.6.2.3.2.1 Bits 0-15 of the S/R PDU Header shall contain a 16-bit value identifying Source Port.

A.6.2.3.2.2 An S/R implementation processing S/R PDUs with MIL-STD-2045-47001 payloads over UDP shall set the value of S/R Source Port designated by the ULP.

A.6.2.3.2.3 An S/R implementation processing S/R PDUs with MIL-STD-2045-47001 payloads via MIL-STD-188-220 NLPT shall set the value of S/R Source Port to a value designated by the ULP.

A.6.2.4 S/R Header, Format, Destination Port.

A.6.2.4.1 S/R Header, Format, Destination Port, Description.

A.6.2.4.1.1 This 16-bit number identifies the application process that will receive the ALPDU being transported by S/R.

A.6.2.4.2 S/R Header, Format, Destination Port, Requirements.

A.6.2.4.2.1 Bits 16-31 of the S/R PDU Header shall contain a 16-bit value identifying Destination Port.

A.6.2.4.2.2 An S/R implementation processing S/R PDUs with MIL-STD-2045-47001 payloads over UDP shall set the value of S/R Destination Port to 1581.

A.6.2.4.2.3 An S/R implementation processing S/R PDUs with MIL-STD-2045-47001 payloads via MIL-STD-188-220 NLPT shall set the value of S/R Destination Port to 1581.

A.6.2.5 S/R Header, Format, Header Length (HLEN).

A.6.2.5.1 S/R Header, Format, Header Length (HLEN), Description.

A.6.2.5.1.1 This 12-bit field indicates the total length of the complete S/R PDU Header (i.e., including header fields for specific S/R PDU types) in 32-bit words. The maximum value for Header Length (HLEN) is 104.

A.6.2.5.2 S/R Header, Format, Header Length (HLEN), Requirements.

A.6.2.5.2.1 Bits 35-46 of the S/R PDU Header shall contain a 12-bit value for HLEN.

A.6.2.5.2.2 An S/R implementation shall set the value of HLEN to the length of the complete S/R PDU Header in 32-bit words.

A.6.2.5.2.3 When sending a DS PDU, an S/R Originator shall set HLEN to 3.

A.6.2.5.2.4 When sending an S/R AR PDU, HLEN shall be set to three (3).

A.6.2.5.2.5 When sending an S/R CA PDU, HLEN shall be set to two (2).

A.6.2.5.2.6 When sending an S/R PA PDU, HLEN shall be set using the equation:

HLEN = 3 + Number of 32-bit-extensions of Acknowledgment Segments Bit Mask

A.6.2.5.2.7 When sending an S/R ABR PDU, HLEN shall be set to two (2).

A.6.2.5.2.8 When sending an S/R ABC PDU, HLEN shall be set to two (2).

A.6.2.6 S/R Header, Format, Type.

A.6.2.6.1 S/R Header, Format, Type, Description.

A.6.2.6.1.1 This 3-bit field identifies the S/R PDU type (e.g., DS PDU, ABR PDU, etc.). The S/R PDU types and their associated decimal values are shown in Table A-IV.

TABLE A - IV Types of S/R PDUs

S/R PDU Type	Decimal Value
Data Segment with End of Data Transfer Acknowledgment Required (DSEDTAR)	0
Data Segment with End of Data Transfer Acknowledgment not required (DSEDTANR)	2
Partial Acknowledgment (PA)	4
Complete Acknowledgment (CA)	6
Abort Request (ABR)	1
Abort Confirm (ABC)	5
Acknowledgment Request (AR)	3
Reserved - Will be used for future S/R capabilities (e.g., the optional exchange/negotiation of S/R parameters over all types of IP networks (i.e., not just MIL-STD-188-220 nets)).	7

A.6.2.6.2 S/R Header, Format, Type, Requirements.

A.6.2.6.2.1 Bits 32-34 of the S/R PDU Header shall contain a 3-bit value for Type (i.e., PDU Type).

A.6.2.6.2.2 When transmitting DS PDUs for an S/R transaction, an S/R Originator shall use the same Type field value for all DS PDUs within the S/R transaction (i.e., same acknowledgment scheme for all segments with a common Serial Number).

A.6.2.6.2.3 When transmitting a DS PDU with End of Data Transfer Acknowledgment Required (EDTAR), the S/R Header field Type shall be set to a value of zero (0).

A.6.2.6.2.4 When transmitting a DS PDU with End of Data Transfer Acknowledgment Not Required (EDTANR), the S/R Header field Type shall be set to a value of two (2).

A.6.2.6.2.5 When transmitting a PA PDU, the S/R Header field Type shall be set to a value of four (4).

A.6.2.6.2.6 When transmitting a CA PDU, the S/R Header field Type shall be set to a value of six (6) to identify a CA PDU.

A.6.2.6.2.7 When transmitting an ABR PDU, the S/R Header field Type shall be set to a value of one (1).

A.6.2.6.2.8 When transmitting an ABC PDU, the S/R Header field Type shall be set to a value of five (5).

A.6.2.6.2.9 When transmitting an AR PDU, the S/R Header field Type shall be set to a value of three (3).

A.6.2.6.2.10 The S/R Header field Type value of seven (7) shall be reserved for future use.

A.6.2.7 S/R Header, Format, Poll/Final (P/F).

A.6.2.7.1 S/R Header, Format, Poll/Final (P/F), Description.

A.6.2.7.1.1 This 1-bit field is used to request a response from the recipient of the PDU.

A.6.2.7.1.2 When sending S/R PDUs that may require a response from the recipient, the single-bit P/F field is referred to as the P-Bit (Poll-Bit) field with values of zero (0) and one (1). When P-Bit is set to one (1), the sender is polling for a response, and typically will resend the request until a response is received or retries are exhausted (typically resulting in the transmission attempt being aborted).

A.6.2.7.1.3 When sending S/R PDUs in response to a sender request, the single-bit P/F field is referred to as the F-Bit (Final-Bit) with values of zero (0) and one (1). A response with F-Bit set to one (1) is a receipt acknowledgment to an S/R PDU sent with P-Bit set to one (1).

A.6.2.7.1.4 For AR PDUs, P-Bit is always set to one (1).

A.6.2.7.2 S/R Header, Format, Poll/Final (P/F), Requirements.

A.6.2.7.2.1 Bit 47 of the S/R PDU Header shall contain a 1-bit value for Poll/Final (i.e., P-Bit, F-Bit).

A.6.2.7.2.2 When a response is required from the recipient of an S/R PDU, the sending node shall set Poll/Final (i.e., P-Bit) to one (1).

A.6.2.7.2.3 When a response is not required from the recipient of an S/R PDU, the sending node shall set Poll/Final (i.e., P-Bit) to zero (0).

A.6.2.7.2.4 When an S/R PDU is sent in response to receipt of an S/R PDU with P-Bit set to one (1), F-Bit shall be set to one (1).

A.6.2.7.2.5 Unless otherwise specified, when an S/R PDU is not sent in response to receipt of an S/R PDU with P-Bit set to one (1), F-Bit shall be set to zero (0).

A.6.2.7.2.6 When sending an S/R AR PDU, the Originator shall set P-Bit to one (1).

A.6.2.7.3 S/R Header, Format, Poll/Final (P/F) (Optional).

A.6.2.7.3.1 S/R Header, Format, Poll/Final (P/F) (Optional), Description.

A.6.2.7.3.1.1 This section identifies optional S/R capability for the Poll/Final bit.

A.6.2.7.3.2 S/R Header, Format, Poll/Final (P/F) (Optional), Requirements.

A.6.2.7.3.2.1 When sending an ABR PDU, it shall be a system option to implement functionality to set P-Bit to one (1) to request a response from the receiving node.

A.6.2.8 S/R Header, Format, Serial Number.

A.6.2.8.1 S/R Header, Format, Serial Number, Description.

A.6.2.8.1.1 Serial Number is a 16-bit number assigned by an S/R Originator to uniquely identify the S/R transaction (ALPDU) to which this segment belongs. Because two-or-more Originators may independently assign the same Serial Number, Serial Number is combined with the S/R PDU Source Address to form the ALPDU Identifier, which uniquely identifies a transaction in a network of Originators.

A.6.2.8.2 S/R Header, Format, Serial Number, Requirements.

A.6.2.8.2.1 Bits 48-63 of the S/R PDU Header shall contain a 16-bit value for Serial Number.

A.6.2.8.2.2 S/R Originators shall manage Serial Number to be unique within the scope of the Originator's S/R transactions.

A.6.2.8.2.3 S/R Originators shall maintain the continuity of Serial Number values across execution sessions.

A.7 DATA.

A.7.1 Data, Description.

A.7.1.1 This section addresses requirements associated with the processing of the data payload of S/R PDUs, including the processes and artifacts supporting segmentation, transmittal, and receipt of data under the S/R protocol.

A.7.2 Data, Process.

A.7.2.1 Data, Process, Description.

A.7.2.1.1 Under the S/R protocol, formatted messages (i.e., ALPDUs) larger than a designated Segment Size, are segmented by the Originator prior to transmission, and reassembled at the Destination for delivery to the application. Each segment is transmitted as a separate S/R DS PDU, which is then transmitted in either one UDP PDU (IP network) or one Intranet Layer PDU (CNR 188-220 NLPT network). An acknowledgment mechanism may be employed to ensure reliable delivery of all segments in a connectionless transport environment.

A.7.2.1.2 The Originator and Destination nodes maintain controls to facilitate and control the S/R procedures, regardless of the overall acknowledgment scheme employed. These ensure that data transfer occurs in an efficient manner. These controls regulate the flow of DS PDUs, as well as inter-node communication of transaction status.

A.7.2.1.3 ALPDUs larger than the specified Segment Size are segmented and sent to the destination addressee as the payload of DS PDUs. Although there is only one physical layout for the DS PDU, a DS PDU is categorized as one of two types; Type 0 for End of Data Transfer Acknowledgment Required, and Type 2 for End of Data Transfer Acknowledgment Not Required, indicating whether an EDT acknowledgment is required of the Destination node.

A.7.2.1.4 When an EDT acknowledgment is required, the S/R Destination responds to the Originator with a CA PDU after successfully receiving all DS PDUs for an ALPDU, even if P-Bit is set to zero (0) in the last received DS (i.e., the DS may be received out-of-sequence, so the segment completing the Destination's S/R transaction may not be the last segment transmitted by the Originator).

A.7.2.1.5 Systems may perform one-to-one transmission using S/R, but the S/R protocol also supports one-to-many transmissions in much the same fashion as transmission to a single destination.

A.7.2.1.6 An Originator solicits a response from a Destination by setting P-Bit to one (1) in any DS PDU. This mechanism enables an Originator to explicitly request an acknowledgment from a Destination as part of a DS transmission, without having to send a separate AR PDU.

A.7.2.1.7 When processing an S/R Unicast transaction, the Originator uses SCL, in coordination with other controls, to manage the number of unacknowledged segments being transmitted at any given time within a transaction. This limits segment transmission rates, preventing unnecessary network traffic for non-responsive Destinations.

A.7.2.1.8 In the S/R Protocol, mixed-mode Destination Addresses are handled as separate S/R transactions, one for Unicast Addresses and one for Multicast Addresses. This is done to reduce network flooding based on receiving acknowledgments from potentially large multicast groups or the global address, as the core S/R Protocol does not support guaranteed delivery, and the accompanying transaction status messages that facilitate guaranteed delivery.

A.7.2.1.9 Though multiple S/R transactions can be enacted simultaneously by an Originator, each identified by their ALPDU Identifier, implementations are encouraged to only maintain one S/R transaction due to the complexity of S/R transactions and the increased complexity of managing network traffic levels across multiple transactions.

A.7.2.1.10 Recommended values for selected S/R parameters are shown in Table A-V. Note that these values will not be optimal for all CNR networks.

TABLE A - V Recommended S/R Parameter Values

S/R Parameter Description	Abbreviation	Minimum	Maximum	Default Value
Request For Acknowledgment Retry Limit	RFARL	1	10	3 Retries
Segment Credit Limit	SCL	1	16*	5 Segments
Segment Retry Count Limit	SRCL	0	5	2 Retries
Maximum RFAIL Value	MAX_RFAIL_VALUE	30	600	60 seconds
Maximum ISRIL Value	MAX_ISRIL_VALUE	90	2400	210 seconds

* In a MIL-STD-188-220 environment, total octets (i.e., Segment Size * SCL) should not exceed the Originator queue size (e.g., QSO) specified in the MIL-STD-188-220 Parameter Tables.

A.7.2.1.11 The values of S/R parameters may be recalculated during S/R operation. Modification of these values is based not only on the values defined above, but several S/R parameters that are tracked during operation.

A.7.2.2 Data, Process, Acknowledgment.

A.7.2.2.1 Data, Process, Acknowledgment, Description.

A.7.2.2.1.1 The S/R protocol uses a Selective Retransmission scheme, enabling an Originator to determine which DS PDUs to retransmit based on Destination acknowledgments of receipt of data segments. The Originator only retransmits segments after an implementation-determined period of time has passed without Destination acknowledgment of receipt. Several mechanisms exist for an Originator to solicit acknowledgment of receipt of DS PDUs from the Destination, prior to engaging in retransmissions.

A.7.2.2.2 Data, Process, Acknowledgment (End of Data Transfer Acknowledgment Required), Description.

A.7.2.2.2.1 An S/R Originator elects EDTAR, by setting the value of the S/R Header field Type to zero (0).

A.7.2.2.2.2 The EDTAR acknowledgment scheme requires a Destination to inform the Originator with an unsolicited CA when all data segments have been received. Additionally, an unsolicited PA is required under optional S/R processing if, while data segments are still being received, the Destination’s RTL or Partial Acknowledgment Interval Limit (PAIL) is reached, NOMSL is breached, or RSCL is reached.

A.7.2.2.2.3 It should be noted that, because there is no guaranteed order of receipt for DS PDUs, the last DS PDU received at a Destination to complete the S/R transaction may be any of the DS PDUs within the S/R transaction. Additionally, an S/R Originator may explicitly solicit a Destination response by sending an AR PDU or setting P-Bit to one (1) on a DS PDU.

A.7.2.2.3 Data, Process, Acknowledgment (End of Data Transfer Acknowledgment Required), Requirements.

A.7.2.2.3.1 S/R implementations shall support DS PDUs with Type set to zero (0) (i.e., EDTAR).

A.7.2.2.4 Data, Process, Acknowledgment (End of Data Transfer Acknowledgment Not Required), Description.

A.7.2.2.4.1 An S/R Originator elects EDTANR, by setting the value of the S/R Header field Type to two (2).

A.7.2.2.4.2 The EDTANR acknowledgment scheme does not require unsolicited actions to be taken by the Destination. When the transaction Originator elects EDTANR, transaction Destinations perform no autonomous actions to transmit transaction status to the Originator. To solicit a status response from a transaction Destination, the transaction Originator either sends an AR PDU to the Destination, or sends a DS PDU with P-Bit set to one (1).

A.7.2.2.5 Data, Process, Acknowledgment (End of Data Transfer Acknowledgment Not Required), Requirements.

A.7.2.2.5.1 S/R implementations shall support DS PDUs with Type set to two (2) (i.e., EDTANR).

A.7.2.2.6 Data, Process, Acknowledgment (End of Data Transfer Acknowledgment Not Required, Destination), Requirements.

A.7.2.2.6.1 When processing an S/R transaction using DS PDUs with Type set to two (2) (i.e., EDTANR), an S/R Destination shall transmit PA PDUs only in response to receipt of an AR PDU or DS PDU, with P-Bit set to one (1), from the transaction Originator.

A.7.2.2.6.2 When processing an S/R transaction using DS PDUs with Type set to two (2) (i.e., EDTANR), an S/R Destination shall transmit CA PDUs only in response to receipt of an AR PDU or DS PDU, with P-Bit set to one (1), from the transaction Originator.

A.7.2.3 Data, Process, ALPDU.

A.7.2.3.1 Data, Process, ALPDU, Description.

A.7.2.3.1.1 This section addresses requirements for the ALPDU, which is the data payload for DS PDUs.

A.7.2.3.2 Data, Process, ALPDU, Requirements.

A.7.2.3.2.1 When operating over an IP network, the S/R ALPDU Identifier shall be comprised of the source IP address and the transaction's Serial Number.

A.7.2.3.2.2 When operating over an NLPT network, the S/R ALPDU Identifier shall be comprised of the source data link address and the transaction's Serial Number.

A.7.2.3.3 Data, Process, ALPDU, Transaction History (Optional).

A.7.2.3.3.1 Data, Process, ALPDU, Transaction History (Optional), Description.

A.7.2.3.3.1.1 This section addresses optional requirements for the maintenance of a log of transactional status for ALPDUs (i.e., sent, received, successful, unsuccessful, etc.).

A.7.2.3.3.2 Data, Process, ALPDU, Transaction History (Optional), Requirements.

A.7.2.3.3.2.1 It shall be a system option to implement functionality to maintain a history of the transactional status for generated ALPDUs.

A.7.2.3.3.2.2 It shall be a system option to implement functionality to maintain a history of the transactional status for received ALPDUs.

A.7.2.3.4 Data, Process, ALPDU, Segmentation (Originator).

A.7.2.3.4.1 Data, Process, ALPDU, Segmentation (Originator), Description,

A.7.2.3.4.1.1 This section addresses requirements on an S/R Originator node for the segmentation of an ALPDU.

A.7.2.3.4.2 Data, Process, ALPDU, Segmentation (Originator), Requirements.

A.7.2.3.4.2.1 When an ALPDU exceeds Segment Size, an S/R Originator shall segment the ALPDU.

A.7.2.3.4.2.2 When Segment Size is not specified, an S/R Originator shall segment ALPDUs that exceed MSS.

A.7.2.3.4.2.3 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall assign a unique Serial Number to each ALPDU.

A.7.2.3.4.2.4 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall map the ALPDU into an ordered sequence of segments.

A.7.2.3.4.2.5 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall create segments of MSS if Segment Size is not specified.

A.7.2.3.4.2.6 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall generate all data segments, other than the last data segment, to be Segment Size octets in length.

A.7.2.3.4.2.7 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall generate the last data segment in the transaction to be no larger than Segment Size octets in length.

A.7.2.3.4.2.8 When segmenting an ALPDU for processing as an S/R transaction, data segments shall be unpadded.

A.7.2.3.4.2.9 An S/R Originator shall transmit each data segment of an ALPDU in a separate DS PDU.

A.7.2.3.4.2.10 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall place the ALPDU's Serial Number into the S/R Header of each transaction DS PDU.

A.7.2.3.4.2.11 When segmenting an ALPDU for processing as an S/R transaction, an S/R Originator shall place each data segment's Segment Number into the S/R Header for that segment's DS PDU.

A.7.2.3.5 Data, Process, ALPDU, Notification (Originator).

A.7.2.3.5.1 Data, Process, ALPDU, Notification (Originator), Description.

A.7.2.3.5.1.1 This section addresses requirements on an S/R Originator node to provide notification of status for S/R transactions to the invoking ULP.

A.7.2.3.5.2 Data, Process, ALPDU, Notification (Originator), Requirements.

A.7.2.3.5.2.1 When the transfer of an ALPDU to a Destination is aborted at the originating node, an S/R Originator shall provide an error indication to the invoking ULP.

A.7.2.3.5.2.2 When the transfer of an ALPDU to a Destination is successfully completed, an S/R Originator shall notify the invoking ULP.

A.7.2.3.6 Data, Process, ALPDU, Destination.

A.7.2.3.6.1 Data, Process, ALPDU, Destination, Description.

A.7.2.4.6.1.1 This section identifies S/R process requirements for a Destination node.

A.7.2.3.6.2 Data, Process, ALPDU, Destination, Requirements.

A.7.2.3.6.2.1 An S/R Destination shall monitor UDP Port 1624 for MIL-STD-2045-47001 S/R traffic.

A.7.2.3.6.2.2 An S/R Destination shall establish an S/R transaction's Segment Size based on the length of the DS PDU with Segment Number equal to one (1).

A.7.2.3.6.2.3 An S/R Destination shall instantiate a new S/R transaction on the initial receipt of a DS with a Segment Number value of one (1).

A.7.2.3.6.2.4 An S/R Destination shall reassemble received DS PDUs in ascending Segment Number order, irrespective of the order of receipt.

A.7.2.3.6.2.5 An S/R Destination shall track the receipt status for each transaction DS.

A.7.2.3.6.2.6 When an S/R Destination receives a duplicate DS within a transaction, the Destination shall discard the contained data segment.

A.7.2.3.6.2.7 When a received S/R DS PDU with End of Data Transfer Acknowledgment Required (Type = 0) successfully completes receipt of all transaction DS PDUs, an S/R Destination shall transmit a CA PDU to the transaction Originator.

A.7.2.3.6.2.8 When an S/R Destination successfully receives all transaction DS PDUs, the Destination shall forward the reassembled ALPDU to the ULP.

A.7.2.3.6.3 Data, Process, ALPDU, Destination (Optional), Requirements.

A.7.2.3.6.3.1 It shall be a system option to implement functionality for an S/R Destination to forward incomplete ALPDUs (i.e., transactions completed with missing data segments) to the ULP.

A.7.2.3.6.3.2 When an S/R Destination implements the optional forwarding of an incomplete ALPDU to the ULP, the S/R Destination shall identify the missing Segment Numbers.

A.7.2.3.6.3.3 When an S/R Destination implements the optional forwarding of an incomplete ALPDU to the ULP, the S/R Destination shall zero-fill missing data segments.

A.7.2.3.6.3.4 When an S/R Destination implements the optional forwarding of an incomplete ALPDU to the ULP, the S/R Destination shall, if the last data segment is missing, assume a full-sized data segment when zero-filling for the last data segment.

A.7.2.4 Data, Process, Abort.

A.7.2.4.1 Data, Process, Abort, Description.

A.7.2.4.1.1 This section addresses requirements for the abnormal termination of an active S/R transaction.

A.7.2.4.2 Data, Process, Abort (Originator), Requirements.

A.7.2.4.2.1 When aborting an active S/R Unicast transaction, an S/R Originator shall transmit an ABR PDU, with P-Bit set to zero (0), to the targeted transaction Destination.

A.7.2.4.2.2 Data, Process, Abort (Originator, Optional), Requirements.

A.7.2.4.2.2.1 When aborting an active S/R Unicast transaction, it shall be a system option to implement functionality for an S/R Originator to set P-Bit to one (1) on the ABR PDU to poll for a response from the targeted transaction Destination.

A.7.2.4.3 Data, Process, Abort (Destination), Requirements.

A.7.2.4.3.1 When aborting an active S/R Unicast transaction, an S/R Destination shall transmit an ABR PDU, with P-Bit set to zero (0), to the transaction Originator.

A.7.2.4.3.2 Data, Process, Abort (Destination, Optional), Requirements.

A.7.2.4.3.2.1 When aborting an active S/R Unicast transaction, it shall be a system option to implement functionality for an S/R Destination to set P-Bit to one (1) on the ABR PDU to poll for a response from the transaction Originator.

A.7.2.5 Data, Process, Multicast.

A.7.2.5.1 Data, Process, Multicast (Originator), Description.

A.7.2.5.1.1 This section addresses requirements for processing S/R transactions directed to Multicast addresses, including transmitting to the Global address.

A.7.2.5.1.2 When transmitting to Multicast Addresses using only the mandatory requirements, no timing constraints are placed on the transmission, and Destination responses may be ignored.

A.7.2.5.1.3 The process goal is to send each DS PDU once, and only once, to each Multicast Address. There are no mechanisms for acknowledgments or retries in the mandatory requirements for Multicast Addresses. To account for systems that may implement Data Link Layer concatenation, the first segment of the transaction must be transmitted over the air before additional segments are sent down the protocol stack for transmission. This allows the receiver's timers to be properly initialized.

A.7.2.5.2 Data, Process, Multicast (Originator), Requirements.

A.7.2.5.2.1 When transmitting to a Multicast address, an S/R Originator shall transmit the transaction's DS PDUs without regard to potential Destination response(s).

A.7.2.5.3 Data, Process, Multicast (Originator, Optional), Description.

A.7.2.5.3.1 S/R nodes may, optionally, implement functionality to support guaranteed delivery of ALPDUs to Multicast addresses. To facilitate this, the Destination and Originator handle the transaction as if the target were a Unicast address, while the Originator continues to send DS PDUs to the Multicast address. This behavior allows for one-or-more recipients on the Multicast address to engage the Originator in guaranteed-delivery semantics, while still maintaining the relative efficiency of multicast.

A.7.2.5.4 Data, Process, Multicast (Originator, Optional), Requirements.

A.7.2.5.4.1 It shall be a system option to implement functionality for an S/R Originator, when transmitting to a Multicast address, to process Destination responses to the multicast transmission.

A.7.2.5.4.2 When an S/R Originator implements optional processing of Destination responses to a transmission to a Multicast address, the Originator shall use Unicast transaction processes to manage transmission/acknowledgment of DS PDUs to responding Destinations on the Multicast address.

A.7.2.5.5 Data, Process, Multicast (Destination), Description.

A.7.2.5.5.1 This section addresses requirements on the Destination for receipt/processing of S/R transactions on a Multicast address.

A.7.2.5.6 Data, Process, Multicast (Destination), Requirements.

A.7.2.5.6.1 When an S/R DS PDU is received on a Multicast address and the S/R Destination does not support optional transmission of a PA PDU in response, the Destination shall process the transaction without interacting with the transaction Originator.

A.7.2.5.7 Data, Process, Multicast (Destination, Optional), Description.

A.7.2.5.7.1 This section addresses optional requirements on the Destination for receipt/processing of S/R transactions on a Multicast address.

A.7.2.5.8 Data, Process, Multicast (Destination, Optional), Requirements.

A.7.2.5.8.1 It shall be a system option to implement functionality for an S/R Destination, on receipt of a S/R DS PDU on a Multicast address for a transaction with multiple data segments, to send a PA PDU to the transaction Originator to acknowledge receipt of the initial DS PDU.

A.7.2.5.8.2 When an S/R Destination implements the optional acknowledgment of receipt of DS PDUs received on a Multicast address, the Destination shall use Unicast transaction processes to manage receipt/acknowledgment of DS PDUs.

A.7.3 Data, PDU.

A.7.3.1 Data, PDU, Data Segment.

A.7.3.1.1 Data, PDU, Data Segment, Description.

A.7.3.1.1.1 This section addresses requirements for the DS PDU.

A.7.3.1.2 Data, PDU, Data Segment, Format.

A.7.3.1.2.1 Data, PDU, Data Segment, Format, Description.

A.7.3.1.2.1.1 This section addresses requirements for the format of the DS PDU.

A.7.3.1.3 Data, PDU, Data Segment, Format (S/R Header).

A.7.3.1.3.1 Data, PDU, Data Segment, Format (S/R Header), Description.

A.7.3.1.3.1.1 This section addresses requirements for the S/R Header portion of a DS PDU, shown in FIGURE A-2.

FIGURE A-2 Data Segment PDU

S/R Header	Octet 0								Octet 1								Octet 2								Octet 3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	S/R Header																															
	Octet 4								Octet 5								Octet 6								Octet 7							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	S/R Header																															
Data Segment Fields	Octet 8								Octet 9								Octet 10								Octet 11							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Segment Number (16 bits)																Last Segment Number (16 bits)															
	Octet 12								Octet …								Octet n-1								Octet n							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	Data Segment Payload (1..Maximum Segment Size)																															

A.7.3.1.3.2 Data, PDU, Data Segment, Format (S/R Header), Requirements.

A.7.3.1.3.2.1 Bits 0-63 of the S/R DS PDU shall contain values for the S/R PDU Header.

A.7.3.1.3.2.2 When sending a DS PDU, an S/R Originator shall set Header Length (HLEN) to three (3).

A.7.3.1.3.2.3 An S/R Originator shall use the same Type field value for all DS PDUs within an S/R transaction (i.e., same acknowledgment scheme for all segments with a common "Serial Number").

A.7.3.1.4 Data, PDU, Data Segment, Format (Segment Number (SN)).

A.7.3.1.4.1 Data, PDU, Data Segment, Format (Segment Number (SN)), Description.

A.7.3.1.4.1.1 Segment Number is a 16-bit number (0-65,535) assigned by the transaction Originator to identify a data segment's position in the overall ALPDU. Segment Number is used by the Destination to correctly order received DSs during the reassembly process.

A.7.3.1.4.2 Data, PDU, Data Segment, Format (Segment Number (SN)), Requirements.

A.7.3.1.4.2.1 Bits 64-79 of the S/R DS PDU shall contain the value for the Segment Number field.

A.7.3.1.4.2.2 An S/R Originator shall assign the value for Segment Number when generating a DS PDU.

A.7.3.1.4.2.3 Segment Number for the first DS PDU in an S/R transaction shall be one (1).

A.7.3.1.4.2.4 When segmenting an ALPDU, the Originator shall increment Segment Number by one (1) for each successive DS PDU.

A.7.3.1.5 Data, PDU, Data Segment, Format (Last Segment Number (LSN)).

A.7.3.1.5.1 Data, PDU, Data Segment, Format (Last Segment Number (LSN)), Description.

A.7.3.1.5.1.1 Last Segment Number (LSN) is a 16-bit number (0-65,535) assigned by the transaction Originator identifying the Segment Number of the last data segment for the ALPDU (i.e., total number of data segments in an S/R transaction).

A.7.3.1.5.2 Data, PDU, Data Segment, Format (Last Segment Number (LSN)), Requirements.

A.7.3.1.5.2.1 Bits 80-95 of the S/R DS PDU shall contain the value for the LSN field.

A.7.3.1.5.2.2 LSN shall be equal to the Segment Number of the last data segment within the S/R transaction.

A.7.3.1.6 Data, PDU, Data Segment, Format (Data Segment Payload).

A.7.3.1.6.1 Data, PDU, Data Segment, Format (Data Segment Payload), Description.

A.7.3.1.6.1.1 DS Payload contains the actual data segment being transmitted on the DS PDU.

A.7.3.1.6.2 Data, PDU, Data Segment, Format (Data Segment Payload), Requirements.

A.7.3.1.6.2.1 Bit 96 of the S/R DS PDU shall be the initial bit of the data segment payload.

A.7.3.1.6.2.2 The data segment payload of an S/R DS PDU shall be less than, or equal to, MSS octets in length.

A.7.3.1.7 Data, PDU, Data Segment, Send (Originator).

A.7.3.1.7.1 Data, PDU, Data Segment, Send (Originator), Description.

A.7.3.1.7.1.1 This section addresses Originator requirements associated with the initial transmission of DS PDUs.

A.7.3.1.7.2 Data, PDU, Data Segment, Send (Originator), Requirements.

A.7.3.1.7.2.1 An S/R Originator shall transmit ALPDU segments as the data portion of S/R DS PDUs.

A.7.3.1.7.2.2 When transmitting over an IP network, an S/R Originator shall transmit each DS PDU in one UDP request.

A.7.3.1.7.2.3 When transmitting over a MIL-STD-188-220 NLPT network, an S/R Originator shall transmit each DS PDU in one Intranet Layer request.

A.7.3.1.7.2.4 When a Destination-initiated acknowledgment by an S/R Destination is required on successful completion of an S/R transaction, the S/R Originator shall transmit the data segments using DS PDUs with Type equal to zero (0) (EDTAR).

A.7.3.1.7.2.5 When a Destination-initiated acknowledgment by an S/R Destination is not required on successful completion of an S/R transaction, the S/R Originator shall transmit the data segments using DS PDUs with Type equal to two (2) (EDTANR).

A.7.3.1.7.2.6 An S/R Originator shall track the acknowledgment status of each segment for each transaction Destination.

A.7.3.1.7.2.7 An S/R Originator shall wait for resolution of acknowledgments for the first DS PDU before sending any subsequent DS PDUs for the transaction.

A.7.3.1.7.2.8 An S/R Originator shall set a DS PDU's P-Bit to one (1) for a DS PDU whose transmission will cause SCL to be reached.

A.7.3.1.7.2.9 An S/R Originator shall set a DS PDU's P-Bit to zero (0) for a DS PDU whose transmission will not cause SCL to be reached.

A.7.3.1.7.2.10 An S/R Originator shall transmit all DS PDUs within an S/R transaction (i.e., having the same Serial Number) with the same Data Link Precedence.

A.7.3.1.7.2.11 An S/R Originator shall send DS PDUs in ascending Segment Number order.

A.7.3.1.7.2.12 An S/R Originator shall track the highest Segment Number sent for each active S/R transaction.

A.7.3.1.8 Data, PDU, Data Segment, Send (Originator, Unicast).

A.7.3.1.8.1 Data, PDU, Data Segment, Send (Originator, Unicast), Description.

A.7.3.1.8.1.1 This section identifies requirements specific to the Unicast transmission of DS PDUs by an S/R Originator.

A.7.3.1.8.2 Data, PDU, Data Segment, Send (Originator, Unicast), Requirements.

A.7.3.1.8.2.1 When processing a Unicast S/R transaction, an S/R Originator shall set P-Bit to one (1) for the first DS PDU within an S/R transaction.

A.7.3.1.8.2.2 When an S/R Originator requires a receipt acknowledgment from a S/R Destination in response to a transmitted DS PDU, the S/R Originator shall set the DS PDU's P-Bit to one (1).

A.7.3.1.8.2.3 When an S/R Originator does not require a receipt acknowledgment from a S/R Destination in response to a transmitted DS PDU, the S/R Originator shall set the DS PDU's P-Bit to zero (0).

A.7.3.1.8.2.4 When processing a Unicast S/R transaction, an S/R Originator shall only transmit a DS PDU when the Originator is not waiting on an acknowledgment from the transaction Destination.

A.7.3.1.8.2.5 When processing a Unicast S/R transaction, an S/R Originator shall track the sent/complete status for each transaction data segment.

A.7.3.1.8.2.6 When processing an S/R Unicast transaction using End of Data Transfer Acknowledgment Required DS PDUs (Type = 0), an S/R Originator shall set P-Bit to one (1) for the last DS PDU in the transaction.

A.7.3.1.9 Data, PDU, Data Segment, Send (Originator, Unicast, Window).

A.7.3.1.9.1 Data, PDU, Data Segment, Send (Originator, Unicast, Window), Description.

A.7.3.1.9.1.1 Within the S/R protocol, a "window" refers to the number of DS PDUs that can be transmitted before the Segment Credit Limit is reached. In general implementation, with the exception of an S/R transaction's first DS PDU, DS PDUs are transmitted in groups bounded by SCL.

A.7.3.1.9.2 Data, PDU, Data Segment, Send (Originator, Unicast, Window), Requirements.

A.7.3.1.9.2.1 When processing an S/R Unicast transaction, an S/R Originator shall send the second and subsequent DS PDUs in groups up to SCL in number.

A.7.3.1.10 Data, PDU, Data Segment, Send (Originator, Multicast).

A.7.3.1.10.1 Data, PDU, Data Segment, Send (Originator, Multicast), Description.

A.7.3.1.10.1.1 Within the S/R protocol, a "window" refers to the number of DS PDUs that can be transmitted before the Segment Credit Limit is reached. In general implementation, with the exception of an S/R transaction's first DS PDU, DS PDUs are transmitted in groups bounded by SCL.

A.7.3.1.10.2 Data, PDU, Data Segment, Send (Originator, Multicast), Requirements.

A.7.3.1.10.2.1 When processing a Multicast S/R transaction without support for Destination responses, an S/R Originator shall transmit each DS PDU only once to a Multicast address.

A.7.3.1.10.2.2 When processing a Multicast S/R transaction without support for Destination responses, an S/R Originator shall set P-Bit to zero (0) for all DS PDUs.

A.7.3.1.10.2.3 When processing a Multicast S/R transaction without support for Destination responses, an S/R Originator shall send all DS PDUs with Type set to two (2) (i.e., as End of Data Transfer Acknowledgment Not Required).

A.7.3.1.11 Data, PDU, Data Segment, Send (Originator, Optional).

A.7.3.1.11.1 Data, PDU, Data Segment, Send (Originator, Optional), Description.

A.7.3.1.11.1.1 When an Originator transmits an S/R DS PDU (with Type=0 or Type=2) to a Destination, the value of P-Bit indicates if an acknowledgment is being requested from the Destination. P-Bit is typically set to '1' on the last DS being transmitted within a "transmission window".

A.7.3.1.11.1.2 Transmission of the first DS for a transaction is a special case, as an acknowledgment of receipt for the first DS PDU is required before the remainder of the transaction's DS PDUs will be transmitted. In this case, the first DS PDU of a transaction is both the first and last DS PDU in the transaction's initial transmission window.

A.7.3.1.11.1.3 The optional S/R constraint on sending subsequent DS PDUs until all Destinations have acknowledged receipt of the first segment is intended to avoid situations where multiple segments are sent and/or resent to a destination that is unreachable, resulting in wasted bandwidth. However, exceptions to requesting an acknowledgment for the first segment are permitted (e.g., to account for situations where the latency for communicating back from Destination to the originator is very high, or the destination is not able to communicate back to the originator because it has gone quiet on transmit but can still receive).

Implementation Note: The optional constraint identified is most applicable to Unicast transmissions over MIL-STD-188-220 networks, and may be detrimental to performance when using Unicast UDP transmissions over an IP network.

A.7.3.1.11.1.4 To help avoid S/R PDUs being discarded when lower-layer queues become overfilled, SCL is used to constrain the maximum number of segments that can be outstanding (sent but not yet acknowledged). While SCL typically controls the size of S/R's "transmission window" (i.e., the number of S/R PDUs sent before an acknowledgment is requested), the actual "window size" is constrained by the lesser of SCL and MSRL. Accordingly, MSRL is normally set to a value several times larger than SCL, to ensure that higher numbered segments can continue to be sent when a single lower numbered segment does not get acknowledged promptly (i.e., must be retried one or more times). It should be noted that MSRL also acts as an upper bound on the size of a Bit Mask field in the Partial Acknowledgment PDU.

A.7.3.1.11.1.5 Implementation Discussion for Slow Nets over CNR (Combat Net Radio): For Slow Nets, ISSIL identifies a maximum rate at which segments should be sent, supporting regulation of transmission rates to avoid the "burstiness" (burst of segments sent in a very short time period) that occurs when the SCL and MSRL congestion controls are used without ISSIL. ISSIL can also be used to limit the rate at which segments are sent to a quiet station, which is critical because these stations are unable to send the PA PDUs required for the SCL and MSRL based congestion control mechanisms to function.

A.7.3.1.11.2 Data, PDU, Data Segment, Send (Originator, Optional), Requirements.

A.7.3.1.11.2.1 It shall be a system option to implement functionality for an S/R Originator to require receipt of acknowledgments for the first DS PDU from all transaction Destinations prior to sending any subsequent transaction DS PDUs.

A.7.3.1.12 Data, PDU, Data Segment, Re-Send (Originator, Unicast).

A.7.3.1.12.1 Data, PDU, Data Segment, Re-Send (Originator, Unicast), Description.

A.7.3.1.12.1.1 This section identifies process requirements for retransmitting DS PDUs that are unacknowledged by one-or-more Destinations.

A.7.3.1.12.1.2 In a MIL-STD-188-220 environment (i.e., transmitting over NLPT), retransmitted DS PDUs are transmitted to all active Destinations to prevent destinations from timing out due to inactivity from the Originator (recalling that duplicate segments received by a Destination are discarded).

A.7.3.1.12.2 Data, PDU, Data Segment, Re-Send (Originator, Unicast), Requirements.

A.7.3.1.12.2.1 When one-or-more active transaction Destinations do not acknowledge receipt of a DS PDU for a Unicast S/R transaction, an S/R Originator shall retransmit the DS PDU.

A.7.3.1.12.2.2 An S/R Originator shall re-send unacknowledged DS PDUs before sending unsent DS PDUs.

A.7.3.1.12.2.3 When re-transmitting unacknowledged DS PDUs for an S/R Unicast transaction, an S/R Originator shall set P-Bit to one (1) if the DS PDU's Segment Number is one (1).

A.7.3.1.13 Data, PDU, Data Segment, Re-Send (Originator, Multicast, Optional).

A.7.3.1.13.1 Data, PDU, Data Segment, Re-Send (Originator, Multicast, Optional), Description.

A.7.3.1.13.1.1 This section identifies process requirements for the optional retransmission of DS PDUs.

A.7.3.1.13.2 Data, PDU, Data Segment, Re-Send (Originator, Multicast, Optional), Requirements.

A.7.3.1.13.2.1 It shall be a system option to implement functionality for an S/R Originator to re-transmit DS PDUs to Multicast addresses.

A.7.3.1.14 Data, PDU, Data Segment, Re-Send (Originator, Optional).

A.7.3.1.14.1 Data, PDU, Data Segment, Re-Send (Originator, Optional), Description.

A.7.3.1.14.1.1 The timing of segment retransmissions has a significant impact on S/R reliability and performance. S/R parameters (e.g., ERTD, Inter-Segment Send Interval Limit (ISSIL), Segment Send Rate Limit Per Originator, etc.) support implementation logic to ensure that segments are not resent prematurely (i.e., before the Destination has had a chance to acknowledge receipt of a segment). When implementation logic implies that a segment should have already been acknowledged, this does not exclude the possibility that an acknowledgment was sent-but-not-received. Accordingly, blindly retransmitting segments in the order of original transmission is not the best policy for CNR nets.

Implementation Note for Re-Transmitting DS PDUs on a CNR (i.e., MIL-STD-188-220) Network

Bandwidth constraints and elements specific to transmitting on a MIL-STD-188-220 network warrant additional consideration, especially for retransmission. Logic elements to consider when determining which unacknowledged data segment(s) should be retransmitted on a CNR (i.e., MIL-STD-188-220) network include:

a. Have all data segments been sent at least once?

b. If all data segments have not been sent at least once, has MSRL been breached, indicating that no "new" data segments should be sent until acknowledgments are received on prior DS PDUs (i.e., re-send lower-numbered unacknowledged DS PDU)?

c. Are there any DS PDUs for which there are multiple outstanding acknowledgments?

A.7.3.1.14.1.2 While it is intuitive to re-transmit the least-recently-transmitted unacknowledged DS PDU, the lack of acknowledgment from two-or-more Destinations on a MIL-STD-188-220 network is a strong indicator that the DS PDU will need to be re-sent, providing more time for receipt/acknowledgment of other DS PDUs.

A.7.3.1.14.2 Data, PDU, Data Segment, Re-Send (Originator, Optional), Requirements.

A.7.3.1.14.2.1 It shall be a system option to implement functionality for an S/R Originator, when retransmitting DS PDUs, to retransmit the least recently transmitted DS PDU.

A.7.3.1.15 Data, PDU, Data Segment, Receive (Destination).

A.7.3.1.15.1 Data, PDU, Data Segment, Receive (Destination), Description.

A.7.3.1.15.1.1 An S/R Destination monitors receipt of DS PDUs, using the source address of the Originator, in combination with the Serial Number field value from the S/R header, to uniquely identify all data segments associated with a discrete S/R transaction. Each Destination reassembles received segments in the proper order, regardless of the actual order of reception, tracking which segments have and have not been acknowledged for each ALPDU Identifier, and detecting/ignoring duplicate segments. Once a complete ALPDU is reassembled, it is forwarded to the appropriate/registered ULP.

A.7.3.1.15.1.2 The Destination may also forward reassembled ALPDUs with missing segments to the Upper Layer Protocol, including the reporting of which segments were and were not received when the reassembly attempt terminated.

A.7.3.1.15.2 Data, PDU, Data Segment, Receive (Destination), Requirements.

A.7.3.1.15.2.1 When an S/R Destination receives a DS PDU with P-Bit set to one (1), the Destination shall respond to the transaction Originator with a CA PDU, with F-Bit set to one (1), if all transaction data segments have been successfully received.

A.7.3.1.15.2.2 When an S/R Destination receives a DS PDU with P-Bit set to one (1), the Destination shall respond to the transaction Originator with a PA PDU, with F-Bit set to one (1), if all transaction data segments have not been successfully received.

A.7.3.1.15.2.3 When an S/R Destination receives a DS PDU, with a Segment Number other than one (1) and P-Bit set to one (1), which cannot be associated to an S/R transaction using the ALPDU Identifier, the Destination shall respond to the sender with an ABR PDU with P-Bit set to zero (0).

A.7.3.1.15.2.4 When an S/R Destination receives a DS PDU, with P-Bit set to one (1), against an S/R transaction which is both inactive and incomplete, the Destination shall respond to the sender with an ABR PDU with P-Bit set to zero (0).

A.7.3.1.15.2.5 When an S/R Destination receives a DS PDU, other than the transaction's last DS PDU where the segment length is other than the transaction's defined Segment Size, the Destination shall abort the transaction.

A.7.3.1.15.2.6 When an S/R Destination receives a DS PDU, with a Segment Number of one (1), which cannot be associated to a current S/R transaction using the ALPDU Identifier, the Destination shall establish a new S/R transaction for the ALPDU Identifier.

A.7.3.1.15.2.7 When an S/R Destination receives a duplicate Data Segment PDU, with P-Bit set to zero (0), for an active transaction, the Destination shall discard the contained data segment.

A.7.3.1.15.2.8 When an S/R Destination receives a duplicate DS PDU, with P-Bit set to zero (0), for an active transaction, the Destination shall send a PA PDU to the transaction Originator.

A.7.3.1.15.2.9 When an S/R Destination receives a DS PDU, with the S/R Header field Type set to zero (0) (EDTAR), that completes the ALPDU, the Destination shall send a CA PDU to the transaction Originator.

A.7.3.1.15.2.10 When an S/R Destination receives a DS PDU, with the S/R Header field Type set to zero (0) (EDTAR), against a completed S/R transaction, the Destination shall send a CA PDU to the transaction Originator.

A.7.3.1.15.2.11 When an S/R Destination receives a DS PDU, with the S/R Header field Type set to zero (0) (End of Data Transfer Acknowledgment Required), against an aborted transaction, the Destination shall send an ABR PDU to the transaction Originator.

A.7.3.1.16 Data, PDU, Data Segment, Receive (Destination, Optional).

A.7.3.1.16.1 Data, PDU, Data Segment, Receive (Destination, Optional), Description.

A.7.3.1.16.1.1 This section identifies optional capabilities which may be supported by an S/R Destination.

A.7.3.1.16.2 Data, PDU, Data Segment, Receive (Destination, Optional), Requirements.

A.7.3.1.16.2.1 When an S/R Destination receives a DS PDU from a transaction Originator against an S/R transaction that was aborted by the Destination without confirmation/acknowledgment from the transaction Originator, it shall be a system option to implement Destination functionality to respond to the transaction Originator with an ABR with P-Bit set to one (1).

A.7.3.1.16.2.2 When an S/R Destination receives a DS PDU from a transaction Originator against an S/R transaction that was aborted by the Destination with confirmation/acknowledgment from the transaction Originator, it shall be a system option to implement Destination functionality to respond to the transaction Originator with an ABR with P-Bit set to one (1).

A.7.3.1.16.2.3 When an S/R Destination receives a DS PDU from a transaction Originator against an S/R transaction that was aborted by the Destination and for which the Destination is not waiting for an ABC PDU from the Originator, it shall be a system option to implement Destination functionality to respond to the transaction Originator with an ABR with P-Bit set to one (1).

A.7.3.1.16.2.4 When an S/R Destination receives a DS PDU, with the S/R Header field Type set to two (2), that completes the S/R transaction, it shall be a system option to implement Destination functionality to transmit a CA PDU, with F-Bit set to zero (0), to the transaction Originator.

A.7.3.1.16.2.5 When an S/R Destination receives a DS PDU, with the S/R Header field Type set to zero (0), against an S/R transaction which has already been successfully completed, it shall be a system option to implement Destination functionality to transmit a CA PDU, with F-Bit set to one (1), to the transaction Originator.

A.7.3.1.16.2.6 When an S/R Destination receives a DS PDU, with the S/R Header field Type set to two (2), against an S/R transaction which has already been successfully completed, it shall be a system option to implement Destination functionality to transmit a CA PDU, with F-Bit set to zero (0), to the transaction Originator.

A.7.3.1.16.2.7 When an S/R Destination receives a DS PDU that cannot be associated to an existing S/R transaction using the DS PDU's source address and Serial Number, it shall be a system option to implement Destination functionality to instantiate a new S/R transaction for the ALPDU Identifier.

A.7.3.1.16.2.8 It shall be a system option to implement functionality for an S/R Destination to record the time-of-receipt for DS PDUs.

A.7.3.1.16.2.9 When an S/R Destination receives a duplicate DS PDU, it shall be a system option to implement Destination functionality to send a PA PDU to the transaction Originator.

A.7.3.1.16.2.10 When an S/R Destination receives a duplicate DS PDU, with P-Bit set to one (1), it shall be a system option to implement Destination functionality to send a PA PDU with, F-Bit set to one (1), to the transaction Originator.

A.7.3.1.16.2.11 When an S/R Destination receives a DS PDU, with P-Bit set to one (1), from an Originator against an S/R transaction that was aborted by the Destination without confirmation from the transaction Originator, it shall be a system option to implement Destination functionality to respond to the Originator with an ABR PDU with F-Bit set to one (1).

A.7.3.1.16.2.12 When an S/R Destination receives a DS PDU, with P-Bit set to one (1), from the transaction Originator against an S/R transaction that was aborted with acknowledgment by the Originator, it shall be a system option to implement Destination functionality to transmit an ABR PDU, with F-Bit set to zero (0), to the Originator.

A.8 ACKNOWLEDGMENT.

A.8.1 Acknowledgment, Description.

A.8.1.1 A Request for Acknowledgment can take the form of an AR PDU, or a DS PDU with P-Bit set to one (1). In either case, the S/R Destination should respond with either a CA PDU or PA PDU, dependent on the state of the S/R transaction.

A.8.1.2 This section addresses the three PDUs (AR PDU, CA PDU, and PA PDU) explicitly associated with the acknowledgment process. The case of the DS PDU with P-Bit set to one (1) is addressed as requirements for receipt processing of the DS PDU by the S/R Destination.

A.8.2 Acknowledgment, PDU.

A.8.2.1 Acknowledgment, PDU, Acknowledgment Request.

A.8.2.1.1 Acknowledgment, PDU, Acknowledgment Request, Description.

A.8.2.1.1.1 The AR PDU is used by an S/R Originator to solicit an acknowledgment identifying the receipt status of DS PDUs at the transaction Destination. Upon receiving an AR PDU, the Destination should respond with a PA PDU to the Originator if not all data segments have been received, a CA if all data segments have been received, or an ABR PDU if the receiver wishes to terminate the transfer. The format of the AR PDU is shown in FIGURE A-3.

A.8.2.1.2 Acknowledgment, PDU, Acknowledgment Request, Format.

A.8.2.1.2.1 Acknowledgment, PDU, Acknowledgment Request, Format, Description.

A.8.2.1.2.1.1 This section describes the format of the AR PDU, shown in FIGURE A-3.

FIGURE A-3 Acknowledgment Request PDU

	Octet 0								Octet 1								Octet 2								Octet 3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
S/R Header	S/R Header																															
	Octet 4								Octet 5								Octet 6								Octet 7							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	S/R Header																															
Ack Request Fields	Octet 8								Octet 9								Octet 10								Octet 11							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Last Sent Segment Number (16 bits)																Padding (16 bits)															

A.8.2.1.3 Acknowledgment, PDU, Acknowledgment Request, Format (S/R Header).

A.8.2.1.3.1 Acknowledgment, PDU, Acknowledgment Request, Format (S/R Header), Description.

A.8.2.1.3.1.1 The AR PDU begins with the S/R Header.

A.8.2.1.3.2 Acknowledgment, PDU, Acknowledgment Request, Format (S/R Header), Requirements.

A.8.2.1.3.2.1 Bits 0-63 of the S/R AR PDU shall contain values for the S/R PDU Header fields.

A.8.2.1.3.2.2 When sending an S/R AR PDU, Header Length (HLEN) shall be set to three (3).

A.8.2.1.3.2.3 When sending an S/R AR PDU, the Originator shall set P-Bit to one (1).

A.8.2.1.4 Acknowledgment, PDU, Acknowledgment Request, Format (Last Sent Segment Number).

A.8.2.1.4.1 Acknowledgment, PDU, Acknowledgment Request, Format (Last Sent Segment Number), Description.

A.8.2.1.4.1.1 Last Sent Segment Number (LSSN) is a 16-bit number indicating the highest segment number sent by the transaction Originator at the time the AR PDU is issued.

A.8.2.1.4.2 Acknowledgment, PDU, Acknowledgment Request, Format (Last Sent Segment Number), Requirements.

A.8.2.1.4.2.1 Bits 64-79 of the S/R AR PDU shall contain the value for the AR PDU field LSSN.

A.8.2.1.4.2.2 When sending an S/R AR PDU, the S/R Originator shall enter the Segment Number of the highest sent data segment into the LSSN field.

A.8.2.1.5 Acknowledgment, PDU, Acknowledgment Request, Format (Padding).

A.8.2.1.5.1 Acknowledgment, PDU, Acknowledgment Request, Format (Padding), Description.

A.8.2.1.5.1.1 "Padding" is used to pad the AR PDU to the next 32-bit boundary.

A.8.2.1.5.2 Acknowledgment, PDU, Acknowledgment Request, Format (Padding), Requirements.

A.8.2.1.5.2.1 Bits 80-95 of the S/R AR PDU shall be reserved for "Padding".

A.8.2.1.6 Acknowledgment, PDU, Acknowledgment Request, Send (Originator).

A.8.2.1.6.1 Acknowledgment, PDU, Acknowledgment Request, Send (Originator), Description.

A.8.2.1.6.1.1 This section identifies requirements specific to the transmission of an AR PDU by an S/R Originator.

A.8.2.1.6.2 Acknowledgment, PDU, Acknowledgment Request, Send (Originator), Requirements.

A.8.2.1.6.2.1 An S/R Originator shall send an AR PDU to request the receipt status of transaction DSs from an S/R Destination.

A.8.2.1.6.2.2 An S/R Originator shall set the AR PDU's Padding field to zero (0).

A.8.2.1.7 Acknowledgment, PDU, Acknowledgment Request, Send (Originator, Multicast).

A.8.2.1.7.1 Acknowledgment, PDU, Acknowledgment Request, Send (Originator, Multicast), Description.

A.8.2.1.7.1.1 This section addresses requirements for the transmission of an AR PDU by an S/R Originator.

A.8.2.1.7.2 Acknowledgment, PDU, Acknowledgment Request, Send (Originator, Multicast), Requirements.

A.8.2.1.7.2.1 When an S/R Originator is operating under standard multicast semantics (i.e., without receipt acknowledgment), the S/R Originator shall not send AR PDUs.

A.8.2.1.8 Acknowledgment, PDU, Acknowledgment Request, Send (Originator, Multicast, Optional).

A.8.2.1.8.1 Acknowledgment, PDU, Acknowledgment Request, Send (Originator, Multicast, Optional), Description.

A.8.2.1.8.1.1 This section addresses optional requirements for the transmission of an AR PDU by an S/R Originator, when the Originator supports guaranteed delivery of ALPDUs to multicast destination addresses.

A.8.2.1.8.2 Acknowledgment, PDU, Acknowledgment Request, Send (Originator, Multicast, Optional), Requirements.

A.8.2.1.8.2.1 When an SR Originator is operating under optional multicast semantics for guaranteed delivery (i.e., with receipt acknowledgment), the S/R Originator shall send AR PDUs to Multicast Addresses.

A.8.2.1.9 Acknowledgment, PDU, Acknowledgment Request, Re-Send (Originator).

A.8.2.1.9.1 Acknowledgment, PDU, Acknowledgment Request, Re-Send (Originator), Description.

A.8.2.1.9.1.1 This section addresses requirements for the re-transmission of an AR PDU by an S/R Originator.

A.8.2.1.9.2 Acknowledgment, PDU, Acknowledgment Request, Re-Send (Originator), Requirements.

A.8.2.1.9.2.1 When an S/R Destination fails to respond to an AR PDU within the ERTD, the S/R Originator shall re-send the AR PDU.

A.8.2.1.9.2.2 When an S/R Destination fails to respond to a DS PDU, with P-Bit set to one (1), within the ERTD, the S/R Originator shall re-send the DS PDU, with P-Bit set to one (1).

A.8.2.1.10 Acknowledgment, PDU, Acknowledgment Request, Receive (Destination).

A.8.2.1.10.1 Acknowledgment, PDU, Acknowledgment Request, Receive (Destination), Description.

A.8.2.1.10.1.1 This section identifies actions taken by a Destination when it receives an AR PDU from the transaction Originator.

A.8.2.1.10.2 Acknowledgment, PDU, Acknowledgment Request, Receive (Destination), Requirements.

A.8.2.1.10.2.1 An S/R Destination shall ignore the content of the AR PDU's Padding field.

A.8.2.1.10.2.2 When an S/R Destination receives an AR PDU from the transaction Originator against an active but incomplete transaction, the Destination shall send a PA PDU to the Originator.

A.8.2.1.10.2.3 When an S/R Destination receives an AR PDU from the transaction Originator against a completed transaction, the Destination shall send a CA PDU to the Originator.

A.8.2.1.10.2.4 When an S/R Destination receives an AR PDU from the transaction Originator against an aborted transaction, the Destination shall send an ABR PDU to the Originator.

A.8.2.1.10.2.5 When an S/R Destination receives an AR PDU that cannot be associated to an ALPDU Identifier, the Destination shall instantiate a new S/R transaction.

A.8.2.1.10.2.6 When an S/R Destination receives an AR PDU that cannot be associated to an ALPDU Identifier, the Destination shall respond with a PA PDU, indicating no data segments have been received.

A.8.2.1.10.3 Acknowledgment, PDU, Acknowledgment Request, Receive (Destination, Optional), Requirements.

A.8.2.1.10.3.1 When an S/R Destination receives an AR PDU against an active but incomplete transaction, it shall be a system option to implement Destination functionality to set F-Bit to one (1) in the responding PA PDU.

A.8.2.1.10.3.2 When an S/R Destination receives an AR PDU from an Originator against an S/R transaction that was aborted by the Destination without confirmation from the transaction Originator, it shall be a system option to implement Destination functionality to respond to the Originator with an ABR PDU with F-Bit set to one (1).

A.8.2.1.10.3.3 When an S/R Destination receives an AR PDU from the transaction Originator against an S/R transaction that was aborted with acknowledgment by the Originator, it shall be a system option to implement Destination functionality to transmit an ABR PDU, with F-Bit set to zero (0), to the Originator.

A.8.2.1.10.3.4 When an S/R Destination receives an AR PDU from the transaction Originator against a successfully completed transaction, it shall be a system option to implement Destination functionality to set F-Bit to one (1) in the responding CA PDU.

A.8.2.1.10.3.5 When an S/R Destination receives an AR PDU from the transaction Originator against an aborted S/R transaction for which the Destination is not waiting on an ABC PDU from the Originator, it shall be a system option to implement Destination functionality to transmit an ABR PDU, with P-Bit set to one (1), to the Originator.

A.8.2.2 Acknowledgment, PDU, Complete Acknowledgment.

A.8.2.2.1 Acknowledgment, PDU, Complete Acknowledgment, Description.

A.8.2.2.1.1 The CA PDU is transmitted by an S/R Destination to the transaction's Originator, as notification that all data segments for an ALPDU were received correctly.

A.8.2.2.2 Acknowledgment, PDU, Complete Acknowledgment, Format.

A.8.2.2.2.1 Acknowledgment, PDU, Complete Acknowledgment, Format, Description.

A.8.2.2.2.1.1 This section addresses the format for the CA PDU.

A.8.2.2.2.2 Acknowledgment, PDU, Complete Acknowledgment, Format, Requirements.

A.8.2.2.2.2.1 The S/R CA PDU shall contain no fields other than the S/R Header.

A.8.2.2.3 Acknowledgment, PDU, Complete Acknowledgment, Format (S/R Header).

A.8.2.2.3.1 Acknowledgment, PDU, Complete Acknowledgment, Format (S/R Header), Description.

A.8.2.2.3.1.1 This section addresses requirements for the CA PDUs S/R Header.

A.8.2.2.3.2 Acknowledgment, PDU, Complete Acknowledgment, Format (S/R Header), Requirements.

A.8.2.2.3.2.1 Bits 0-63 of the S/R CA PDU shall contain values for the S/R Header fields.

A.8.2.2.4 Acknowledgment, PDU, Complete Acknowledgment, Format (Data).

A.8.2.2.4.1 Acknowledgment, PDU, Complete Acknowledgment, Format (Data), Description.

A.8.2.2.4.1.1 The CA PDU does not contain any fields, other than the S/R Header.

A.8.2.2.4.2 Acknowledgment, PDU, Complete Acknowledgment, Format (Data), Requirements.

A.8.2.2.4.2.1 No data fields shall be added to an S/R CA PDU.

A.8.2.2.5 Acknowledgment, PDU, Complete Acknowledgment, Send (Destination).

A.8.2.2.5.1 Acknowledgment, PDU, Complete Acknowledgment, Send (Destination), Description.

A.8.2.2.5.1.1 An S/R Destination sends CA PDUs in response to conditions (e.g., receipt of a "completing" DS PDU), receipt of an AR PDU, etc.). Because of this, requirements addressing the conditions under which CA PDUs are sent are documented in the sections associated with the triggering cause.

A.8.2.2.5.2 Acknowledgment, PDU, Complete Acknowledgment, Send (Destination), Requirements.

A.8.2.2.5.2.1 No specific requirements.

A.8.2.2.6 Acknowledgment, PDU, Complete Acknowledgment, Receive (Originator).

A.8.2.2.6.1 Acknowledgment, PDU, Complete Acknowledgment, Receive (Originator), Description.

A.8.2.2.6.1.1 This section identifies process requirements for an Originator receiving a CA PDU.

A.8.2.2.6.2 Acknowledgment, PDU, Complete Acknowledgment, Receive (Originator), Requirements.

A.8.2.2.6.2.1 When an S/R Originator receives a CA PDU, the Originator shall ignore acknowledgments that cannot be associated to an active S/R transaction Destination.

A.8.2.2.6.2.2 When an S/R Originator receives a CA PDU, the Originator shall issue a notification to the ULP that the S/R transaction has successfully completed for the sending Destination.

A.8.2.3 Acknowledgment, PDU, Partial Acknowledgment.

A.8.2.3.1 Acknowledgment, PDU, Partial Acknowledgment, Description.

A.8.2.3.1.1 When processing an S/R transaction, the PA PDU is transmitted by the Destination to acknowledge receipt/non-receipt of DSs to the transaction Originator. The format of the PA is shown in FIGURE A-4. The PA PDU contains no data fields.

FIGURE A-4 Partial Acknowledgment PDU

	Octet 0								Octet 1								Octet 2								Octet 3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
S/R Header	S/R Header																															
	Octet 4								Octet 5								Octet 6								Octet 7							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	S/R Header																															
	Octet 8								Octet 9								Octet 10								Octet 11							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Partial Ack Fields	Starting Segment Number (16 bits)																Acknowledgment Segments Bit Mask (16 bits)															
	Octet 12								Octet 13								Octet 14								Octet 15							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	Acknowledgment Segments Bit Mask, Extension 1																															
	Octet …								Octet …								Octet n-1								Octet n							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	Acknowledgment Segments Bit Mask, Extension n																															

A.8.2.3.2 Acknowledgment, PDU, Partial Acknowledgment, Format (S/R Header).

A.8.2.3.2.1 Acknowledgment, PDU, Partial Acknowledgment, Format (S/R Header), Description.

A.8.2.3.2.1.1 This section addresses requirements for the PA PDUs S/R Header.

A.8.2.3.2.2 Acknowledgment, PDU, Partial Acknowledgment, Format (S/R Header), Requirements.

A.8.2.3.2.2.1 Bits 0-63 of the S/R PA PDU shall contain values for the common S/R Header fields.

A.8.2.3.3 Acknowledgment, PDU, Partial Acknowledgment, Format (Starting Segment Number).

A.8.2.3.3.1 Acknowledgment, PDU, Partial Acknowledgment, Format (Starting Segment Number), Description.

A.8.2.3.3.1.1 Starting Segment Number (SSN) is a 16-bit number identifying the lowest numbered segment that has not yet been received at the Destination (i.e., all segments preceding SSN have been received). SSN is also the Segment Number referenced by the first bit in the Bit Mask field.

A.8.2.3.3.2 Acknowledgment, PDU, Partial Acknowledgment, Format (Starting Segment Number), Requirements.

A.8.2.3.3.2.1 Bits 64-79 of the S/R PA PDU shall contain the 16-bit value for the Partial Acknowledgment PDU field SSN.

A.8.2.3.3.2.2 If no segments have been received at the S/R Destination, SSN shall be set to one (1).

A.8.2.3.4 Acknowledgment, PDU, Partial Acknowledgment, Format (Acknowledgment Segments Bit Mask).

A.8.2.3.4.1 Acknowledgment, PDU, Partial Acknowledgment, Format (Acknowledgment Segments Bit Mask), Description.

A.8.2.3.4.1.1 Acknowledgment Segments Bit Mask (or, Bit Mask), indicates the receipt status of DSs at a Destination. As a form of shorthand, the first bit in Bit Mask corresponds to the status of the DS identified by Starting Segment Number, and is always set to zero (0) (not received). The last bit in Bit Mask corresponds to Highest Numbered Segment Received (HNSR), and is always set to one (1) (received). Any DS prior to SSN is presumed to have been received at the Destination, and any DS following Highest Numbered Segment Received is presumed to have not yet been received at the Destination.

A.8.2.3.4.1.2 Within Bit Mask, a bit set to one (1) indicates that the corresponding DS has been received, while a bit set to zero (0) indicates that the corresponding DS has not been received.

A.8.2.3.4.1.3 Bit Mask's initial size is 16 bits, with the first bit set to zero (0) and corresponding to SSN. Each subsequent bit represents the receipt status of the next DS in Segment Number order, ending at Highest Numbered Segment Received. Bit Mask is extensible, as required, in 32-bit increments.

A.8.2.3.4.2 Acknowledgment, PDU, Partial Acknowledgment, Format (Acknowledgment Segments Bit Mask), Requirements.

A.8.2.3.4.2.1 The Acknowledgment Segments Bit Mask field shall start at bit 80 of the S/R PA PDU.

A.8.2.3.4.2.2 The length of the PA PDU's Acknowledgment Segments Bit Mask field shall be calculated using the equation:

Length (Bit Mask) = Highest Numbered Segment Received – Starting Segment Number + 1.

A.8.2.3.4.2.3 The first bit in an S/R PA PDU's Acknowledgment Segments Bit Mask shall represent the receipt state for the DS PDU identified by Starting Segment Number (SSN).

A.8.2.3.4.2.4 The first bit in an Acknowledgment Segment PDU's Acknowledgment Segments Bit Mask field shall be set to zero (0).

A.8.2.3.4.2.5 The first bit in an S/R PA PDU's Acknowledgment Segments Bit Mask shall be the most significant bit (MSB) of the initial 16-bit field.

A.8.2.3.4.2.6 The second bit, and subsequent bits, of an S/R PA PDU's Bit Mask shall represent the receipt state of DSs of succeeding DSs, in contiguous Segment Number order, after Starting Segment Number.

A.8.2.3.4.2.7 If a DS has been received at the Destination, the corresponding bit in the S/R PA PDU's Acknowledgment Segments Bit Mask shall be set to one (1).

A.8.2.3.4.2.8 If a DS has not been received at the Destination, the corresponding bit in the S/R PA PDU's Acknowledgment Segments Bit Mask shall be set to zero (0).

A.8.2.3.4.2.9 The S/R PA PDU's Acknowledgment Segments Bit Mask field shall, as needed, be extended in 32-bit increments.

A.8.2.3.4.2.10 The maximum size of the S/R PA PDU's Acknowledgment Segments Bit Mask shall be 3248 bits (i.e., the original 16-bits with 101 32-bit "extensions" to accommodate reporting requirements).

A.8.2.3.5 Acknowledgment, PDU, Partial Acknowledgment, Format (Padding).

A.8.2.3.5.1 Acknowledgment, PDU, Partial Acknowledgment, Format (Padding), Description.

A.8.2.3.5.1.1 The "Padding" field is included to force the PA PDU to end on a 32-bit boundary.

A.8.2.3.5.2 Acknowledgment, PDU, Partial Acknowledgment, Format (Padding), Requirements.

A.8.2.3.5.2.1 When generating an S/R PA PDU and the Acknowledgment Segments Bit Mask field does not end on a 32-bit boundary, the Destination shall include the "Padding" field to ensure that the PDU ends on the next 32-bit boundary.

A.8.2.3.5.2.2 When the S/R PA PDU's "Padding" field is included, the "Padding" field shall start at the bit immediately following the Acknowledgment Segments Bit Mask field.

A.8.2.3.5.2.3 When the S/R PA PDU's "Padding" field is included, the "Padding" field shall be zero (0) filled.

A.8.2.3.6 Acknowledgment, PDU, Partial Acknowledgment, Send (Destination).

A.8.2.3.6.1 Acknowledgment, PDU, Partial Acknowledgment, Send (Destination), Description.

A.8.2.3.6.1.1 This section addresses S/R Destination requirements for the sending of a PA PDU.

A.8.2.3.6.2 Acknowledgment, PDU, Partial Acknowledgment, Send (Destination), Requirements.

A.8.2.3.6.2.1 Mandatory requirements for the transmission of PA PDUs are documented as responses to the receipt of DS PDUs or AR PDUs.

A.8.2.3.6.3 Acknowledgment, PDU, Partial Acknowledgment, Send (Destination, Optional), Requirements.

A.8.2.3.6.3.1 It shall be a system option to implement functionality for an S/R Destination to enforce a minimum time interval (seconds), determined by the value of Partial Acknowledgment Interval Limit (PAIL), between transmission of PA PDUs to the transaction Originator.

A.8.2.3.6.3.2 It shall be a system option to implement functionality for an S/R Destination to transmit a PA PDU that is not a response to a poll from the transaction Originator.

A.8.2.3.6.3.3 When an S/R Destination implements the optional transmission of a PA PDU that is not a response to a poll from the transaction Originator, the Destination shall set F-Bit for the PA PDU to zero (0).

A.8.2.3.7 Acknowledgment, PDU, Partial Acknowledgment, Receive (Originator).

A.8.2.3.7.1 Acknowledgment, PDU, Partial Acknowledgment, Receive (Originator), Description.

A.8.2.3.7.1.1 This section identifies process requirements for an S/R Originator receiving a PA PDU.

A.8.2.3.7.2 Acknowledgment, PDU, Partial Acknowledgment, Receive (Originator), Requirements.

A.8.2.3.7.2.1 When an S/R Originator receives a PA PDU, the Originator shall ignore acknowledgments that cannot be associated to an active S/R Destination.

A.8.2.3.7.2.2 When an S/R Originator receives a PA PDU from a transaction Destination, the Originator shall update the acknowledgment status for transaction data segments.

A.8.2.3.7.2.3 When an S/R Originator receives a PA PDU from a Destination for which the Originator has aborted the transaction, the Originator shall respond to the Destination with an ABR PDU, with P-Bit set to zero (0).

A.8.2.3.7.2.4 When an S/R Originator receives a PA PDU from a node not associated with the active transaction, the Originator shall respond to the sender with an ABR PDU, with P-Bit set to zero (0), for the identified ALPDU.

A.8.2.3.7.3 Acknowledgment, PDU, Partial Acknowledgment, Receive (Originator, Optional), Requirements.

A.8.2.3.7.3.1 When an S/R Originator supports the optional capability of guaranteed delivery over multicast transactions and receives a PA PDU from an unrecognized Destination in response to transmission of the first DS PDU to a multicast address, to the Originator shall add the Destination to the "list of Destinations" for the S/R transaction.

A.9 ABORT.

A.9.1 Abort, Description.

A.9.1.1 This section addresses the processes and S/R PDUs associated with the abnormal termination of an S/R transaction.

A.9.2 Abort, Process.

A.9.2.1 Abort, Process, Description.

A.9.2.1.1 Abnormal termination of an S/R transaction may be initiated by either the Originator or Destination nodes. The conditions under which a node many initiate abnormal termination of an S/R transaction are identified elsewhere in this document.

A.9.2.2 Abort, Process (Originator), Requirements.

A.9.2.2.1 When an S/R Originator aborts a transaction for a transaction Destination, the scope of impact shall be constrained to the targeted Destination.

A.9.2.2.2 When an S/R Originator terminates a Unicast transaction, the Originator shall provide notification to the ULP identifying the Destination for which the transaction was terminated.

A.9.3 Abort, PDU.

A.9.3.1 Abort, PDU, Abort Request.

A.9.3.1.1 Abort, PDU, Abort Request, Description.

A.9.3.1.1.1 Initiated by either the S/R transaction Originator or Destination, the ABR PDU is used to notify the recipient that the sender is terminating the transfer of an S/R ALPDU. When sending an ABR PDU, the sender sets P-Bit to one (1) if an ABC PDU is desired from the recipient.

A.9.3.1.1.2 When an S/R Destination receives an ABR PDU from an Originator, any received segments associated with the S/R transaction are discarded. When an S/R Originator receives an ABR PDU from a Destination, the Originator stops transmitting segments to that Destination and reports a failed transmission, as appropriate, to the ULP.

A.9.3.1.2 Abort, PDU, Abort Request, Requirements.

A.9.3.1.2.1 When an S/R node initiates abnormal termination of a transaction, the initiating node shall transmit an ABR PDU as notification to the recipient that the sending node is terminating the transaction.

A.9.3.1.3 Abort, PDU, Abort Request, Format.

A.9.3.1.3.1 Abort, PDU, Abort Request, Format, Description.

A.8.3.1.3.1.1 This section addresses the format of the ABR PDU.

A.9.3.1.4 Abort, PDU, Abort Request, Format (S/R Header).

A.9.3.1.4.1 Abort, PDU, Abort Request, Format (S/R Header), Description.

A.9.3.1.4.1.1 The ABR PDU begins with the S/R Header.

A.9.3.1.4.2 Abort, PDU, Abort Request, Format (S/R Header), Requirements.

A.9.3.1.4.2.1 Bits 0-63 of the S/R ABR PDU shall contain values for the S/R Header fields.

A.9.3.1.5 Abort, PDU, Abort Request, Format (Data).

A.9.3.1.5.1 Abort, PDU, Abort Request, Format (Data), Description.

A.9.3.1.5.1.1 The ABR PDU does not contain any fields, other than the S/R Header.

A.9.3.1.5.2 Abort, PDU, Abort Request, Format (Data), Requirements.

A.9.3.1.5.2.1 No data fields shall be added to an S/R ABR PDU.

A.9.3.1.6 Abort, PDU, Abort Request, Send.

A.9.3.1.6.1 Abort, PDU, Abort Request, Send, Description.

A.9.3.1.6.1.1 This section addresses the transmission of an ABR PDU.

A.9.3.1.6.2 Abort, PDU, Abort Request, Send, Requirements.

A.9.3.1.6.2.1 ABR PDUs are sent in response to conditions encountered while processing a transaction. Accordingly, requirements for the sending of ABR PDUs are documented in the sections identifying the triggering error conditions.

A.9.3.1.6.3 Abort, PDU, Abort Request, Send (Destination, Optional), Requirements.

A.9.3.1.6.3.1 When an S/R Destination sends an ABR PDU to the transaction Originator, it shall be a system option to implement Destination functionality to generate a notification to the invoking ULP identifying receipt status for transaction data segments.

A.9.3.1.7 Abort, PDU, Abort Request, Receive.

A.9.3.1.7.1 Abort, PDU, Abort Request, Receive, Description.

A.9.3.1.7.1.1 This section addresses the receipt of an ABR PDU.

A.9.3.1.7.2 Abort, PDU, Abort Request, Receive, Requirements.

A.9.3.1.7.2.1 When an S/R node receives an ABR PDU with P-Bit set to one (1), the recipient shall respond with an ABC PDU with F-Bit set to one (1).

A.9.3.1.7.3 Abort, PDU, Abort Request, Receive (Destination), Requirements.

A.9.3.1.7.3.1 When an S/R Destination receives an ABR PDU from the transaction Originator, the Destination shall terminate the identified S/R transaction.

A.9.3.1.7.4 Abort, PDU, Abort Request, Receive (Originator), Requirements.

A.9.3.1.7.4.1 When an S/R Originator receives an ABR PDU from a transaction Destination, the Originator shall terminate the identified S/R transaction for the sending Destination.

A.9.3.1.7.4.2 When an S/R Originator receives an ABR PDU from a transaction Destination, the Originator shall, as appropriate, provide notification of the failed transaction to the ULP.

A.9.3.1.7.4.3 When an S/R Originator receives an ABR PDU from an active transaction Destination for a Unicast transaction, and at least one transaction Destination is still active, the Originator shall update the status of transmitted data segments to reflect termination of the transaction for the sending Destination.

A.9.3.2 Abort, PDU, Abort Confirm.

A.9.3.2.1 Abort, PDU, Abort Confirm, Description.

A.9.3.2.1.1 This section addresses the ABC PDU.

A.9.3.2.2 Abort, PDU, Abort Confirm, Format.

A.9.3.2.2.1 Abort, PDU, Abort Confirm, Format, Description.

A.9.3.2.2.1.1 This section identifies format requirements for the ABC PDU.

A.9.3.2.3 Abort, PDU, Abort Confirm, Format (S/R Header).

A.9.3.2.3.1 Abort, PDU, Abort Confirm, Format (S/R Header), Description.

A.9.3.2.3.1.1 The ABC PDU begins with the S/R Header.

A.9.3.2.3.2 Abort, PDU, Abort Confirm, Format (S/R Header), Requirements.

A.9.3.2.3.2.1 Bits 0-63 of the S/R ABC PDU shall contain values for the S/R Header fields.

A.9.3.2.4 Abort, PDU, Abort Confirm, Format (Data).

A.9.3.2.4.1 Abort, PDU, Abort Confirm, Format (Data), Description.

A.9.3.2.4.1.1 The ABC PDU does not contain any fields, other than the S/R Header.

A.9.3.2.4.2 Abort, PDU, Abort Confirm, Format (Data), Requirements.

A.9.3.2.4.2.1 No data fields shall be added to an S/R ABC PDU.

A.9.3.2.5 Abort, PDU, Abort Confirm, Send.

A.9.3.2.5.1 Abort, PDU, Abort Confirm, Send, Description.

A.9.3.2.5.1.1 This section addresses the transmission of an ABC PDU.

A.9.3.2.5.2 Abort, PDU, Abort Confirm, Send, Requirements.

A.9.3.2.5.2.1 The ABC PDU is sent in response to a transaction state encountered during the exchange of S/R PDUs. Accordingly, requirements for the sending of the ABC PDU are captured in the "receipt requirements" for the triggering S/R PDU(s).

A.10 TRANSACTION.

A.10.1 Transaction, Addressing.

A.10.1.1 Transaction, Addressing, Description.

A.10.1.1.1 This section addresses addressing requirements for S/R transactions. It should be noted that, though any given S/R transaction consists of only one type of transmission (i.e., Unicast or Multicast), it is possible for an implementation to accept both types of addresses on a single call, and partition the addresses into address-appropriate transactions.

A.10.1.2 Transaction, Addressing, Requirements.

A.10.1.2.1 An S/R Unicast transaction shall only contain Unicast destination addresses.

A.10.1.2.2 An S/R Multicast transaction shall only contain Multicast destination addresses.

A.10.1.3 Transaction, Addressing (Optional), Description.

A.10.1.3.1 This section explicitly codifies the capability to process multiple transmission types as part of a single S/R transaction. Note that this does not constrain an implementation to processing all address types in a single transaction instance (i.e., the addresses can still be partitioned into separate sub-transactions to facilitate processing logic).

A.10.1.4 Transaction, Addressing (Optional), Requirements.

A.10.1.4.1 It shall be a system option to implement functionality for an S/R Originator to process S/R transactions containing any combination of Unicast and Multicast addresses, including the Global address.

A.10.2 Transaction, IP TOS.

A.10.2.1 Transaction, IP TOS, Description.

A.10.2.1.1 Table A-VI identifies the IP TOS (Internet Protocol Type Of Service) values assigned by S/R Originators to transmitted S/R PDUs, based on the precedence identified by the ULP initiating the exchange. For effective use of IP TOS precedence, large transfers using the S/R protocol are normally assigned a Precedence value of Routine by the initiating application, and all DS PDUs within an S/R transaction will have the same IP TOS precedence value.

A.10.2.1.2 The IP TOS values assigned by S/R Destinations are shown in Table A-VII. Smaller, control-related S/R PDUs whose timely exchange is critical to the success of Routine exchanges are assigned higher precedence values, supporting a lower probability of discard at lower layers as the supporting network becomes saturated.

A.10.2.1.3 Support for large, multi-segment S/R data exchanges at a precedence of Flash or higher are optional, due to the operationally unacceptable delays that it will cause for exchanging small, higher precedence safety and mission related ALPDUs as networks become saturated. When S/R data exchanges at Flash-and-higher precedence are supported, the Destination will determine the precedence of the exchange by interrogating the transport header for the IP TOS value.

A.10.2.2 Transaction, IP TOS, Requirements.

A.10.2.2.1 No specific requirements.

A.10.2.3 Transaction, IP TOS (Originator, Optional), Requirements.

A.10.2.3.1 It shall be a system option to implement functionality for an S/R Originator to enforce IP TOS, based on the ULP-identified message precedence, in accordance with Table A-VI Originator Assigned IP TOS Precedence by S/R PDU Type.

TABLE A - VI Originator Assigned IP TOS Precedence By S/R PDU Type

Initiating Application Assigned Precedence	IP TOS for Type 0 or Type 2 - Data Segments	IP TOS for Type 1 - Abort Request	IP TOS for Type 3, P-Bit = "0" - Ack Request	IP TOS for Type 3, P-Bit = "1" - Ack Request	IP TOS for Type 5 - Abort Confirm
Routine	Routine	Immediate	Routine	Immediate	Immediate
Priority	Priority	Immediate	Priority	Immediate	Immediate
Immediate	Immediate	Immediate	Immediate	Immediate	Immediate
Flash	Flash	Flash	Flash	Flash	Flash
Flash Override	Flash Override	Flash Override	Flash Override	Flash Override	Flash Override
Critic/ECP	Critic/ECP	Critic/ECP	Critic/ECP	Critic/ECP	Critic/ECP

A.10.2.4 Transaction, IP TOS (Destination), Requirements.

A.10.2.4.1 When an S/R Destination does not support the optional mapping of IP TOS based on the IP TOS of the received DS PDU, the Destination shall transmit all transaction responses (i.e., PA PDUs, CA PDUs, ABR PDUs, ABC PDUs) with the same Data Link Precedence as the S/R PDU being responded to.

A.10.2.5 Transaction, IP TOS (Destination, Optional), Requirements.

A.10.2.5.1 It shall be a system option to implement functionality for an S/R Destination to enforce IP TOS based on the IP TOS setting of the first DS PDU received for the transaction, in accordance with Table A-VII.

TABLE A - VII Destination Assigned IP TOS Precedence By S/R PDU Type

Receiving Application Reported Precedence Base On First Segment Content	IP TOS for Type 1 - Abort Request	IP TOS for Type 4 - Partial Ack	IP TOS for Type 5 - Abort Confirm	IP TOS for Type 6 - Complete Ack
Routine	Immediate	Immediate	Immediate	Immediate
Priority	Immediate	Immediate	Immediate	Immediate
Immediate	Immediate	Immediate	Immediate	Immediate
Flash	Flash	Flash	Flash	Flash
Flash Override	Flash Override	Flash Override	Flash Override	Flash Override
Critic/ECP	Critic/ECP	Critic/ECP	Critic/ECP	Critic/ECP

A.10.2.5.2 When an S/R Destination implements the optional setting of IP TOS values based on the IP TOS setting of the DS PDU, the Destination shall determine the transaction's IP TOS by interrogating the UDP header's Type Of Service value.

A.10.3 Transaction, Node Status.

A.10.3.1 Transaction, Node Status, Description.

A.10.3.1.1 Node Status addresses the concept of an S/R node's transactional state (i.e., is the node actively participating in a transaction, or is the node no longer participating (either due to completion of the transaction, or termination by either the sending or receiving node)).

A.10.3.2 Transaction, Node Status (Originator), Requirements.

A.10.3.2.1 An S/R Originator shall track the transactional status of each transaction Destination for the duration of the S/R transaction.

A.10.3.3 Transaction, Node Status (Originator, Optional), Requirements.

A.10.3.3.1 When an S/R Originator implements optional guaranteed-delivery functionality for multicast destination addresses, the Originator shall track the transactional status of each identified transaction Destination for the duration of the S/R transaction.

A.10.3.4 Transaction, Node Status (Destination), Requirements.

A.10.3.4.1 An S/R Destination shall track the transactional status of the transaction Originator for the duration of the S/R transaction.

Appendix A

A.11 SUPPLEMENTAL INFORMATION.

A.11.1 Supplemental Information, Description.

A.11.1.1 The following information provides additional context to assist in the understanding of the functionality identified by the requirements. This information is descriptive and/or explanatory, but is neither requirements nor constraints.

A.11.2 Supplemental Information, Unicast Transaction.

A.11.2.1 The sequence diagram FIGURE A-5 depicts the behavior and interaction between nodes in a unicast S/R transaction.

A.11.2.2 This diagram does not depict any optional behavior/interaction, nor any error states that may occur during a transaction. A narrative description of the behaviors and interactions follows.

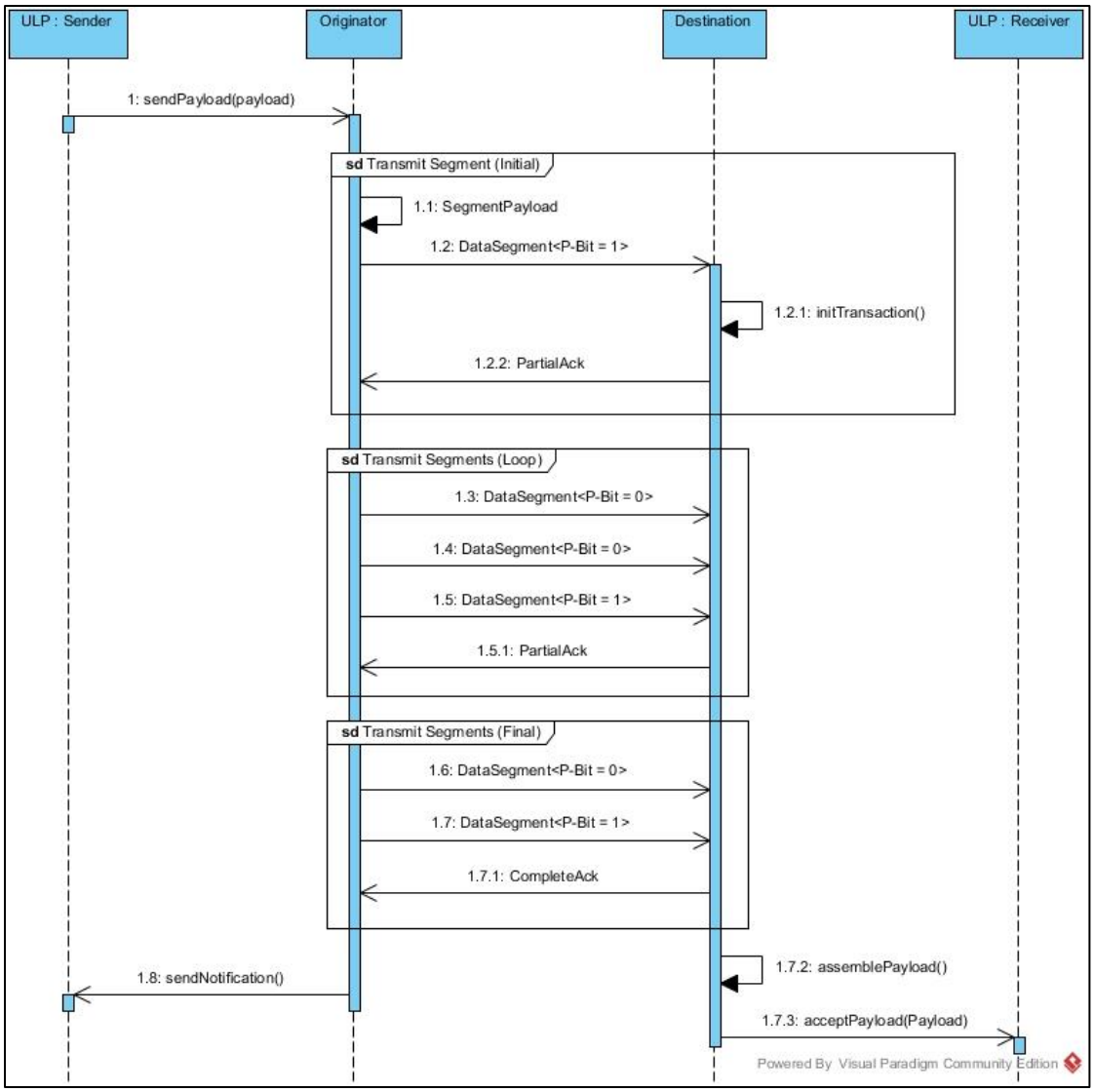

FIGURE A-5 Unicast S/R Transaction

a) Sender, Send Payload (1) - The Sender (i.e., payload source) requests transmission of a supplied payload.

b) Transmit Segment (Initial) - Steps 1.1 through 1.2.2 depict the transmission of the initial transaction segment.

Note: The Originator requires a Destination acknowledgment of the initial segment before any subsequent segments may be transmitted.

c) Originator, Segment Payload (1.1) - The Originator makes a determination to send the payload using S/R, and segments the payload for transmission.

d) Originator, Send Initial DS (1.2) - After segmenting the payload, the Originator sends the first transaction segment to initiate an S/R transaction with the Destination.

e) Destination, Initialize Transaction (1.2.1) - On receipt of the initial segment, the Destination initializes an S/R transaction to receive and process the remaining transaction segments.

f) Destination, Send PA (1.2.2) - The Destination sends a PA PDU for the initial transaction segment to the Originator.

Note: In the case of a transaction with only one (1) segment (i.e., S/R is being used for the acknowledgment mechanism), the Destination would send a CA PDU at this step.

g) Transmit Segments (Loop) - Steps 1.3 through 1.5.1 depict the transmission of non-terminal transaction segments.

h) Originator, Send DS (1.3, 1.4) - The Originator sends transaction segments with the S/R Header field Poll/Final Bit set to zero (0), indicating no acknowledgment is required from the Destination.

Note: Setting of the Poll/Final Bit value is based on the parameter Segment Credit Limit, which the Originator uses to define a "Transmission Window". When sending a transaction segment does not cause Segment Credit Limit to be reached, Poll/Final Bit is set to zero (0). When sending a transaction segment causes Segment Credit Limit to be reached, the Originator sets Poll/Final Bit to one (1) to close the Transmission Window.

i) Originator, Send DS (1.5)- The Originator sends the last transaction segment of the Transmission Window with the S/R Header field Poll/Final Bit set to one (1), indicating an acknowledgment is required from the Destination.

j) Destination, Send PA (1.5.1) - On receipt of the transaction segment with Poll/Final Bit set to one (1), the Destination sends a PA PDU to the Originator, indicating the receipt status of transaction segments.

Note: If the PA PDU indicates that any sent transaction segments have not been received, the Originator will need to re-send those segments.

k) Transmit Segments (Final) - Steps 1.6 through 1.7.1 depict the transmission of the terminal segment for the transaction. It is possible for other, non-terminal segments to be included in the same Transmission Window (i.e., unlike the initial transaction segment, there is no requirement to send the terminal segment in its own Transmission Window).

l) Originator, Send Data Segment (1.6) - This step is representative of one-or-more non-terminal transaction segments in the Transmission Window, as transmission of the terminal transaction is reactive vice predictive. The Poll/Final Bit for these segments is set to zero (0).

m) Originator, Send Final DS (1.7) - By definition, the terminal segment for a transaction is the last segment for the Transmission Window, and its Poll/Final Bit field is set to one (1).

n) Destination, Send CA (1.7.1) - On receipt of the terminal segment for the transaction, the Destination acknowledges receipt and completion of the transaction by sending a Complete Transaction PDU to the Originator.

Note: The Destination should, on receipt of the terminal segment for the transaction, transmit a PA PDU if all transaction segments have not been successfully received.

o) Originator, Notify Sender (1.8) - On completion of the S/R transaction, the Originator notifies the Sender of the transaction's status, completing the transaction at the Originator node.

Note: The Originator should also notify the Sender if the S/R transaction was terminated before completion, by either the Originator or Destination nodes.

p) Destination, Reassemble Payload (1.7.2) - On successful receipt of all transaction segments, the Destination reassembles the segment payloads, re-generating the original payload.

q) Destination, Forward Payload (1.7.3) - To complete the S/R transaction at the Destination node, the Destination forwards the reassembled payload to the Receiver.

A.11.3 Supplemental Information, Multicast Transaction (Standard).

A.11.3.1 The sequence diagram FIGURE A-6 depicts the behavior and interaction between nodes in a standard multicast S/R transaction (i.e., without support for guaranteed delivery).

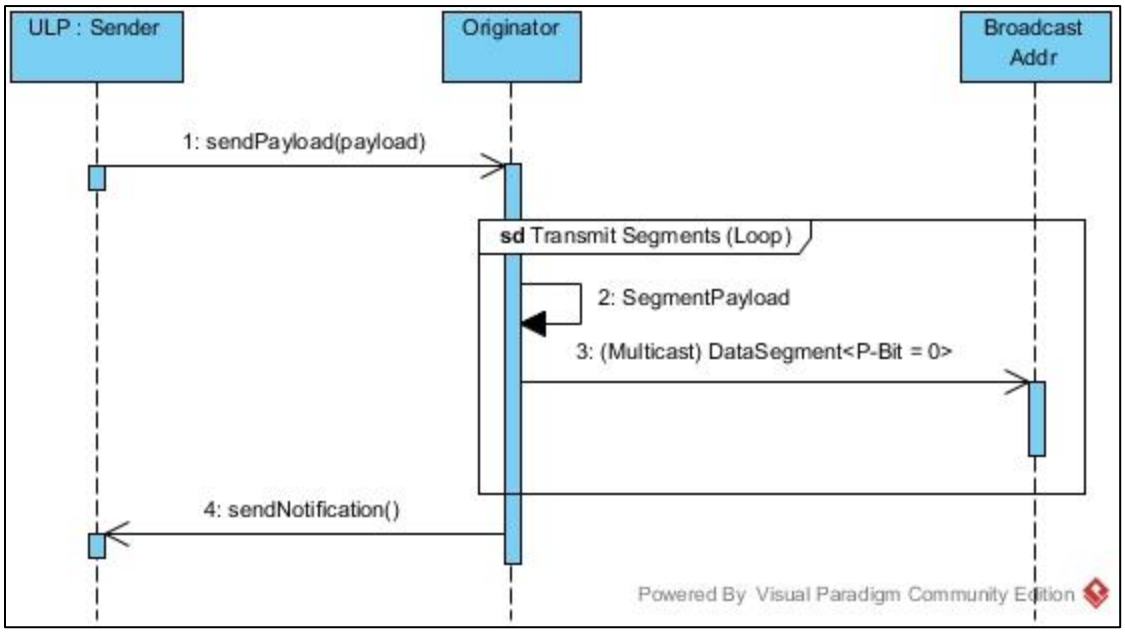

FIGURE A-6 Multicast S/R Transaction (w/out guaranteed delivery)

A.11.3.2 This diagram is included primarily to demonstrate the difference between S/R transactions that support guaranteed delivery, requiring feedback from the Destination, and the fire-and-forget semantics when guaranteed delivery is not supported.

A.11.3.3 As an implementation note, consideration should be given to ensuring that the transmission loop incorporates a mechanism to avoid flooding the network.

A.11.4 Supplemental Information, Multicast Transaction (Guaranteed Delivery).

A.11.4.1 The sequence diagram FIGURE A-7 depicts the behavior and interaction between nodes in a multicast S/R transaction supporting guaranteed delivery.

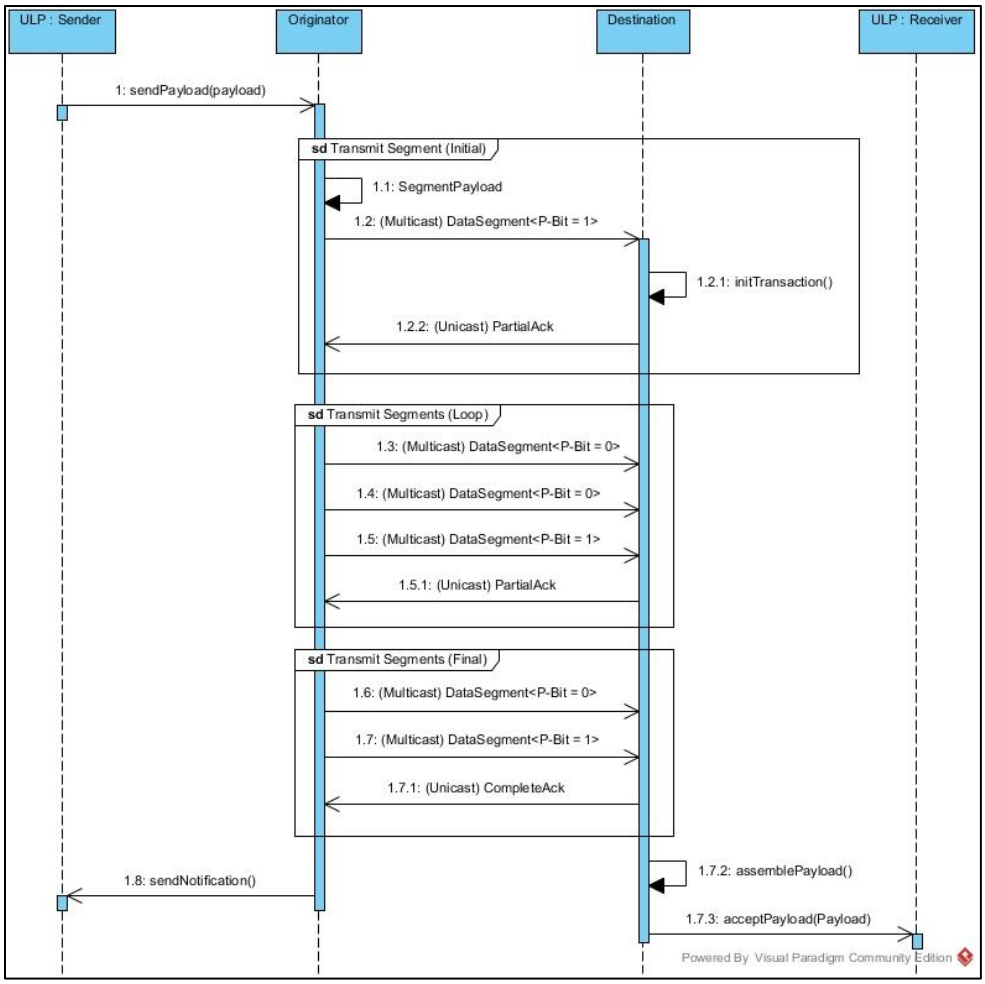

FIGURE A-7 Multicast S/R Transaction (with guaranteed delivery)

A.11.4.2 It should be noted that this is the same sequence as that for a unicast S/R transaction, with one significant difference; all Originator S/R PDUs are sent as multicast transmissions. Destination nodes still respond via unicast, enabling the Originator to identify and track responses on a per-node basis.

A.11.4.3 Implementation note: Additional logic should be anticipated at the Originator node to aggregate Destination responses for sending re-transmissions as a single multicast S/R PDU.

A.11.5 Supplemental Information, Multicast Transactions.

A.11.5.1 This activity diagram shown in FIGURE A-8 depicts the potential interactions between S/R nodes implementing mandatory and optional capabilities. While it is possible for nodes of differing capabilities to co-exist on a network, it is important to note that nodes implementing optional capabilities should have a mechanism for gracefully degrading these capabilities when expected responses (i.e., from other nodes implementing optional capabilities) are not detected.

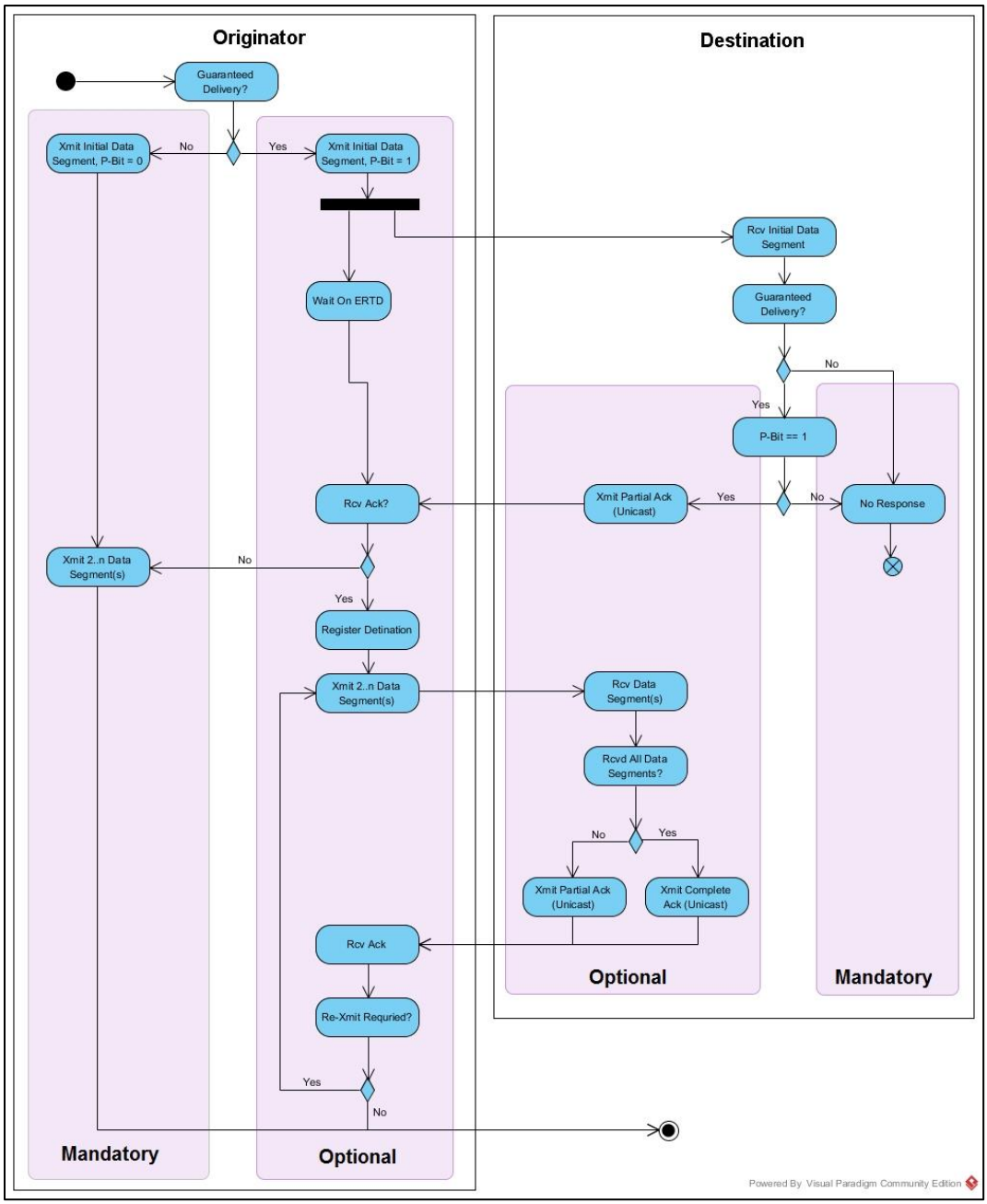

FIGURE A-8 Interactions between S/R nodes implementing mandatory and optional capabilities

A.11.5.2 The activity diagram is segmented into Originator activities and Destination activities. These are further segmented into Mandatory and Optional activities. The important elements to note are the points in the diagram where a node, capable of supporting optional behavior, degrades into a mode using only mandatory behavior.

A.11.5.3 At the Originator node, this occurs if no acknowledgments are received against the initial transaction segment. At this point, the Originator degrades from attempting to guarantee delivery for the multicast transaction to a straight multicast of all transaction segments, without attempting to confirm receipt.

A.11.5.4 It should be noted that, in the case where one-or-more Destination nodes respond with acknowledgments, subsequent multicasts will be received by all Destinations, whether or not they support the required optional behaviors. While the optional behavior guarantees delivery to acknowledging Destinations, non-acknowledging Destinations may also receive the transmitted segments.

A.11.5.5 At the Destination node, the graceful degradation occurs on inspection of the S/R Header field Poll/Final Bit. If the Originator implements behavior for guaranteed delivery for multicast transactions, the Originator will set this value to one (1) on the initial transaction segment. If this value is not set to one (1), it is most likely due to the Originator not implementing optional behavior supporting guaranteed delivery for multicast transactions. While this is not a prohibition against a Destination attempting to engage the Originator in optional behavior (i.e., sending a PA PDU to attempt re-transmission of missing transaction segments), there should not be an expectation of success.

A.11.6 Supplemental Information, PDU Bit Order.

A.11.6.1 Table A-VIII is an example of the bit order and masking for filling an AR PDU

TABLE A - VIII PDU Bit Order (AR PDU)

FIELD				OCTET BUFFER/STREAM			
			VALUE (Binary)	FIELD FRAGMENTS	OCTET VALUE (Binary)		
TITLE	LENGTH (Bits)	VALUE (Dec)	MSB 2^n LSB 2^0	MSB 2^7 LSB 2^0	MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET#
Source Port	16	5000	0001001110001000	00010011	00010011	0x13	0
				10001000	10001000	0x88	1
Destination Port	16	1581	0000011000101101	00000110	00000110	0x06	2
				00101101	00101101	0x2D	3
Type	3	3	011	011xxxxx			
HLEN	12	3	000000000011	xxx00000	01100000	0x60	4
				0000011x			
P/F	1	1	1	xxxxxxx1	00000111	0x07	5
Serial Number	16	16000	0011111010000000	00111110	00111110	0x3E	6
				10000000	10000000	0x80	7
Last Sent Segment Number	16	260	0000000100000100	00000001	00000001	0x01	8
				00000100	00000100	0x04	9

TABLE A - VIII PDU Bit Order (AR PDU)

FIELD				OCTET BUFFER/STREAM			
			VALUE (Binary)	FIELD FRAGMENTS	OCTET VALUE (Binary)		
TITLE	LENGTH (Bits)	VALUE (Dec)	MSB 2^n LSB 2^0	MSB 2^7 LSB 2^0	MSB 2^7 LSB 2^0	OCTET VALUE (Hex)	OCTET#
Padding	16	0	0000000000000000	00000000	00000000	0x00	10
				00000000	00000000	0x00	11

Appendix B

DATA ELEMENT DICTIONARY

B.1 SCOPE

This document contains the data elements used in MIL-STD-2045-47001E. The data elements are uniquely specified by two numbers, the Data Field Identifier (DFI) and its Data Use Identifier (DUI). The DFI includes a single concept and is the generic representation of the DUIs grouped under it. The DUIs, which are representative of the DFI concept, contain the Data Items (DIs) used to compose the data element. The DFIs are listed in numerical sequence. Alphabetical and numerical indexes of the DFIs and DUIs are included before the first DFI.

B.2 APPLICABLE DOCUMENTS

B.2.1 The following specifications, standards, and handbooks form a part of this Appendix to the extent specified herein.

B.2.2 Federal:

FIPS 10-4	COUNTRIES, DEPENDENCIES, AREAS OF SPECIAL SOVEREIGNTY, AND THEIR PRINCIPAL ADMINISTRATIVE DIVISIONS
FIPS 180-4	SECURE HASH STANDARD (SHS) https://doi.org/10.6028/nist.fips.180-4

B.2.3 Other:

LEMPEL-ZIV-WELCH	"A TECHNIQUE FOR HIGH PERFORMANCE DATA COMPRESSION", TERRY A. WELCH, IEEE COMPUTER, VOL. 17, NO. 6, PP. 8-19, JUNE 1984.
LEMPEL-ZIV 1977	"A UNIVERSAL ALGORITHM FOR SEQUENTIAL DATA COMPRESSION", J. ZIV AND A. LEMPEL, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL IT-23, NO. 3, PP 337-343, MAY 1977. https://ieeexplore.ieee.org/xplore/home.jsp
W3C EXI	"EFFICIENT XML INTERCHANGE (EXI) FORMAT 1.0 (SECOND EDITION)", J. SCHNEIDER, T. KAMIYA, D. http://www.w3.org/TR/2014/REC-exi-20140211/

B.3 DEFINITIONS

The definitions in the Main Body of this standard apply to this appendix.

B.4 GENERAL REQUIREMENTS PERTAINING TO THIS APPENDIX

B.4.1 General DFI, DUI, and DI Rules and Conventions.

a. This section describes the structure and use of DFIs, DUIs, and DIs as well as the related data to be used in developing data elements.

b. Only readily understood terms will be used.

c. Acronyms used as part of a name will have their meaning spelled out in the definition or explanation.

d. DFI and DUI names will be as short as possible.

B.4.2 DFI Specific Rules.

a. Special characters used in the formatting of a DFI will have a predetermined meaning.

b. All DFIs must have at least one associated DUI.

c. Chained DFIs will not be used.

B.4.2.1 DFI Name Rules.

a. Each DFI name will be unique.

b. The DFI name will identify a single concept.

c. The DFI name will be a generic representation of the contained DUIs.

d. Group words (type, category, degree, designator, etc.) in DFI names will follow modifying words and phrases, e.g., "Keying Material ID Length" rather than "Length of Keying Material ID" will be used. B.4.2.2 DFI Definition Rules.

a. The DFI definition will be provided only when necessary for amplification.

b. The DFI definition will be a generic definition of the concept represented by the associated DUIs.

c. The DFI definition will be based on a review of all appropriate definition sources.

B.4.3 DUI Specific Rules.

All DUIs must have associated DIs.

B.4.3.1 DUI Name Rules.

a. Each DUI name will be unique.

b. Parallelism of phraseology of all DUI names within the DFI will be preserved.

c. DUI names will be representative of the DFI concept.

B.4.3.2 DUI Field Descriptor.

The field descriptor is an abbreviation used in place of the full DUI name when it will not fit in the allocated field space of a computer-generated message map.

B.4.3.3 DUI Explanation.

a. A DUI explanation will exist for each DUI only when necessary for amplification.

b. A DUI explanation will not be a restatement of the name unless it is spelling out an acronym.

c. A DUI explanation will not be solely an example.

B.4.4 DI Specific Rules.

B.4.4.1 DI Name.

a. Within a DUI, each DI will have a specific name and meaning.

b. DIs will be consistent with the explanation of the DUI.

B.4.4.2 DI Bit Codes.

a. Bit codes will be expressed in decimal with the exception of DIs that are displayed to the operator in octal. When the bit code is octal, a notation will be made to indicate that octal values are used.

b. Within a DUI, each DI will be represented by a unique bit code and have a specific meaning.

B.4.4.3 DI Explanations.

a. The DI explanation will be provided only when necessary for amplification.

b. The DI explanation will attempt to use explanations from previously accepted standards.

c. The DI explanation will be based upon a review of all appropriate sources.

d. The DI explanation will not be a restatement of the name unless it is spelling out an acronym.

e. When a DI name is "NUMERIC," the DI explanation must contain a description of what the DI represents. Literal data item explanations will indicate any ASCII character exceptions (i.e., illegal values). The following are examples:

Data Item	Bit Code	Explanation
ILLEGAL	0	
NUMERIC	1 THROUGH 4095	IN 1 OCTET INCREMENTS.

f. In expressing numerical quantities, the following are the type of entries required.

Data Item	Bit Code	Explanation
0 THROUGH 511 3/4 DATA MILES	0 THROUGH 2047	DISTANCE IN 1/4 DATA MILE INCREMENTS.
NO STATEMENT	2048	
-511 3/4 THROUGH -1/4 DATA MILES	2049 THROUGH 4095	DISTANCE IN 1/4 DATA MILE INCREMENTS.

B.4.4.4 Generic Data Items Entries.

TERM	MEANING
DISUSED	A DI value that was previously named but is no longer valid. A DISUSED value cannot be renamed without determining if coordinated implementation is required.
UNDEFINED	A term used to describe a bit code that has no currently assigned value but may have a value assigned in the future. (This occurs in logically coded items (DUIs) in which all the DIs in the DUI do not have assigned values.)
ILLEGAL	A term used to describe a bit code that is not a permissible entry into the tactical data system(s) supporting interface. (For example, a 9-bit DUI called HEADING that has legal values of 0-359 that represents degrees has illegal values of 360-511.)
NO STATEMENT	A data item that indicates that no information on this DUI is being transmitted. (This does not necessarily indicate that the originator does not have the information.) The procedure to transmit a no statement value is to set the presence indicator to zero. Receipt of a presence indicator set to zero will be interpreted as no statement.
UNKNOWN	A data item that indicates that other values available for this DUI have not been determined by the originator.
TO BE DETERMINED	This indicates that the data item design is incomplete. (DI names and bit codes will be specified at a later time.)

B.4.4.5 No Statement Assignment.

When two options are shown, the binary value 0 will be used as NO STATEMENT except when the binary value 0 has a valid numeric value, in which case the highest binary value will be used.

B.4.5 Definition of Symbols that can be Used in DFI and DUI Name.

a. Hyphen (-) will be used in compound terms.

b. Virgule (/) will be used with bona fide acronyms and in the expression "and/or" only.

c. Parentheses () will be used to enclose an acronym when both title and acronym are included in name.

d. A comma (,) will be used in its normal sense.

e. No other symbols will be used.

B.4.6 ASCII Character Usage.

a. TABLE B-I lists the ASCII characters used in MIL-STD 2045-47001. The ASCII character set is made up of: 26 upper case alphabetic characters, 26 lower case alphabetic characters, 10 numeric characters, 8 special characters (characters that are not alphabetic, numeric, or space characters), 3 non-printing ASCII control codes (horizontal tab, carriage return, line feed), 24 extended special characters (characters that are not an alphabetic, numeric, special, or space character) and the End of Literal Field Marker (ASCII Delete Character).

b. To aid the automated processing of ASCII encodings and their conversion to XML, the data item descriptions for literal fields include a Regular Expression (REGEX) specifying the field's legal content and format. The REGEX syntax used here is compliant to the formal W3C recommendation on regular expressions at http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/.

c. Regular expressions include both characters and metacharacters. For MIL-STD-2045-47001, the characters are the ASCII characters specified in TABLE B-I. Metacharacters are characters that have both their character meaning as defined in the table and additional meaning used to specify the format of a character string. The metacharacters needed to support MIL-STD-2045-47001 are:

1) * Indicates zero or more occurrences of the immediately preceding characters or set of characters.

2) + Indicates one or more occurrences of the immediately preceding characters or set of characters.

3) ? Indicates one or one of the immediately preceding characters or set of characters.

4) [ ] Set indicator. Specifies one character from the set of included characters. E.g.: [A-Za-z0-9] Specifies any single upper case alpha, lower case alpha, or numeric character. Equivalent to ALN, above.

5) {n} Count indicator. E.g.: [A-Z]{3} Specifies three upper case alpha characters as in AAA, ABC, ZZZ, etc.

6) {n,m} Range count indicator. E.g.: [a-z]{2,5} Specifies at least two but not more than five lower case alpha characters.

7) | Option indicator, used as OR. E.g.: [A-Z]|[0-9] Specifies one upper case alpha OR one numeric character.

8) ( ) Grouping indicator. Treat the expression between (and) as a group. E.g.: (b|f|l|m)oot yields boot, foot, loot, or moot.

9) ^ Multipurpose metacharacter. When used as first metacharacter in pattern, it indicates beginning of a line. E.g.: ^[A-Z] specifies first character on line. [^0-9] specifies any non-numeric character. MIL-STD-2045-47001 does not use this metacharacter. It is included only for completeness.

10) . Any character indicator. Used to specify/match any single character. MIL-STD-2045-47001 does not use this metacharacter. It is included only for completeness.

11) \ Escape character. Used to turn a metacharacter into a regular character, a regular character into a metacharacter, or as part of octal or hexadecimal indicator. E.g.: \. Makes the metacharacter "." a normal period. When specified in a set like [:,.+], most metacharacters act like normal characters. However,], ^ and – retain their metacharacter meaning inside sets. They have unique handling requirements. Place] at the beginning of a set to override its metacharacter status. Similarly place - at the beginning of a set to override its metacharacter status. Place ^ anywhere after the first character in a set to override the metacharacter status of this code. If these placements cannot be accommodated, override the metacharacter with the escape character. E.g.: in [-:,+] and [:,\-+] the – is treated as a normal literal dash.

12) \nnn Octal character. Any character can be represented by its octal equivalent. E.g.: \040 specifies space. \177 (decimal 127) specifies the ASCII delete character.

13) \xnn Hexadecimal indicator. Any character can be represented by its hexadecimal equivalent. E.g.: \x20 specifies space. \x7F (decimal 127) specifies the ASCII delete character.

14) \t Horizontal tab character, ASCII 9.

15) \n Newline (linefeed) character, ASCII 10.

16) \r Carriage return character, ASCII 13.

d. Examples:

1) THE 21 BITS OF THIS DUI ARE DIVIDED INTO 3 GROUPS OF 7 BITS EACH REPRESENTING ASCII SET: ABN. REGEX: [A-Z0-9\040]{3}

2) THE 448 BITS OF THIS DUI ARE DIVIDED INTO 64 GROUPS OF 7 BITS EACH REPRESENTING ASCII SET: ALBNSED.
REGEX: [-A-Za-z0-9\040!"#$%&'*+;<=>@[\\\]^_`{|}~(),./:?]{64}|[-A-Za-z0-9\040!"#$%&'*+;<=>@[\\\]^_`{|}~(),./:?]{1,63}\177

3) THE 28 BITS OF THIS DUI ARE DIVIDED INTO 4 GROUPS OF 7 BITS, EACH REPRESENTING ASCII SET: ABN. THESE CHARACTERS MUST BE ARRANGED IN THE SEQUENCE ALPHABETIC/NUMERIC/ALPHABETIC/SPACE OR ALPHABETIC/NUMERIC/NUMERIC/ALPHABETIC, AS IN A1A(SPACE) OR A12A.
REGEX: [A-Z][0-9][A-Z]\040|[A-Z][0-9]{2}[A-Z]

4) THE 28 BITS OF THESE DUIS ARE DIVIDED INTO 3 GROUPS. THE FIRST 2 GROUPS ARE 7 BITS EACH AND REPRESENT ASCII SET: A. THE LAST GROUP IS 14 BITS AND REPRESENTS A DECIMAL VALUE OF 0000 THROUGH 9999, 10000 THROUGH 16383 ARE ILLEGAL. STRUCTURE OF THE TARGET NUMBER IS CONTAINED IN QSTAG 221, TARGET NUMBERING SYSTEM. REGEX: [A-Z]{2}[0-9]{4}

Note: This last example is the data item description for Target Number, which is a composite field consisting of both literal and numeric parts. Because the numeric part of Target Number is a number and not a literal, the REGEX for this data item will not correctly generate the desired binary representation. Consequently, composite fields require special processing.

B.4.7 End of Literal Field Marker (1111111_2).

The End of Literal Field Marker is the ASCII value 1111111_2 (Delete). It will be used to indicate end of field for free text, character-based, literal fields only. The maximum literal field size is specified in the data element dictionary by the second value, {m,n}, of the variable length range indicator. The message processing software will be capable of recognizing either the End of Literal Field Marker indicating end of field (no zero padding required) or the field maximum length indicating the end of literal field.

TABLE B-I ASCII Character Set Definition

Code	Character Type	Definition	Decimal
A	Uppercase Alphabetic Character	One of the upper case letters from A to Z.	65 - 90
B	Blank Character	A space (or blank) text character.	32
C	Non-Printing ASCII Control Codes	• Horizontal Tab • Line Feed • Carriage Return	9 10 13
D	End of Literal Field Marker (ASCII Delete)	Refer to paragraph B.3.7	127
E	Extended Special Character	! exclamation point " quote # number symbol $ dollar sign % percent sign & ampersand ' apostrophe * asterisk + plus sign ; semicolon < less than symbol = equal sign > greater than symbol @ at symbol [left bracket \ backward slant] right bracket ^ caret _ underscore ` backward accent { left brace | vertical bar } right brace ~ tilde	33 34 35 36 37 38 39 42 43 59 60 61 62 64 91 92 93 94 95 96 123 124 125 126
L	Lowercase Alphabetic Character	One of the lower case letters from a to z.	97 - 122
N	Numeric Character	One of the digits from 0 to 9.	48 - 57
S	Special Character	(left parenthesis) right parenthesis , comma - minus sign . period / forward slant : colon ? question mark	40 41 44 45 46 47 58 63

B.5 INDEX OF DFIS AND DUIS.

To assist in using this standard, four listings immediately follow this page. The first list, TABLE B-II, is ordered alphabetically by DFI name, the second list, TABLE B-III, is ordered numerically by DFI number, the third, TABLE B-IV, is ordered alphabetically by DUI name, and the fourth, TABLE B-V, is ordered numerically by DUI number.

TABLE B-II ALPHABETICAL LIST OF DATA FIELD IDENTIFIERS (DFIS)

DFI NAME	DFI NO.
ACTIVITY IDENTIFICATION	6010
DAY OF MONTH	4019
FILE NAME	6006
FUNCTIONAL AREA DESIGNATOR	4081
HOUR	792
NUMBER	4085
MINUTE	797
MONTH	4099
PRESENCE INDICATOR	4014
RECURRENCE INDICATOR	4045
SECOND	380
SECURITY PARAMETER LENGTH INDICATORS	6009
SECURITY PARAMETERS	6008
MILITARY IDENTIFICATION	4004
USER DATA MESSAGE DATA DESIGNATOR	6001
USER DATA MESSAGE HANDLING COMMENTS	6004
USER DATA MESSAGE HANDLING DESIGNATOR	6002
USER DATA MESSAGE HEADER 1-BIT INDICATOR	6007
USER DATA MESSAGE HEADER NUMBER	6005
USER DATA MESSAGE PROCESSING DESIGNATOR	6003
VARIABLE LENGTH NUMERIC	6011
YEAR	4098

TABLE B-III NUMERICAL LIST OF DATA FIELD IDENTIFIERS (DFIS)

DFI NAME	DFI NO.
SECOND	380
HOUR	792
MINUTE	797
MILITARY IDENTIFICATION	4004
PRESENCE INDICATOR	4014
DAY OF MONTH	4019
RECURRENCE INDICATOR	4045
FUNCTIONAL AREA DESIGNATOR	4081
NUMBER	4085
YEAR	4098
MONTH	4099
USER DATA MESSAGE DATA DESIGNATOR	6001
USER DATA MESSAGE HANDLING DESIGNATOR	6002
USER DATA MESSAGE PROCESSING INDICATOR	6003
USER DATA MESSAGE HANDLING COMMENTS	6004
USER DATA MESSAGE HEADER NUMBER	6005
FILE NAME	6006
USER DATA MESSAGE HEADER 1-BIT INDICATOR	6007
SECURITY PARAMETERS	6008
SECURITY PARAMETER LENGTH INDICATORS	6009
ACTIVITY IDENTIFICATION	6010
VARIABLE LENGTH NUMERIC	6011

TABLE B-IV ALPHABETICAL LIST OF DATA USE IDENTIFIERS (DUIS)

DUI NAME	DFI NO.	DUI NO.
AUTHENTICATION DATA (A)	6008	005
AUTHENTICATION DATA (A) LENGTH	6009	004
AUTHENTICATION DATA (B)	6008	006
AUTHENTICATION DATA (B) LENGTH	6009	005
CANTCO REASON	6003	002
CANTPRO REASON	6003	005
CONTROL/RELEASE MARKING	6002	005
CRYPTOGRAPHIC INITIALIZATION	6008	003
CRYPTOGRAPHIC INITIALIZATION LENGTH	6009	002
DATA COMPRESSION TYPE	6001	010
DAY OF MONTH	4019	001
DTG EXTENSION	6005	002
FILE NAME	6006	001
FPI	4014	002
FRI	4045	002
FUNCTIONAL AREA DESIGNATOR	4081	001
GPI	4014	001
GRI	4045	001
GROUP SIZE	6005	004
HEADER SIZE	6005	003
HEADER VERSION	6001	006
HEADER ZERO PADDING	6011	001
HOUR	792	001
KEY TOKEN	6008	004
KEY TOKEN LENGTH	6009	003
KEYING MATERIAL ID	6008	002
KEYING MATERIAL ID LENGTH	6009	001
MACHINE ACKNOWLEDGE REQUEST INDICATOR	6007	001
MESSAGE NUMBER	4085	019
MINUTE	797	004
MONTH	4099	001
OPERATION INDICATOR	6001	005
OPERATOR ACKNOWLEDGE REQUEST INDICATOR	6007	002
OPERATOR REPLY REQUEST INDICATOR	6007	003
REPLY AMPLIFICATION	6004	001
RETRANSMIT INDICATOR	6007	004
SECOND	380	001
SECURITY PARAMETERS INFORMATION	6008	001
SIGNED ACKNOWLEDGE REQUEST INDICATOR	6008	007

TABLE B-IV ALPHABETICAL LIST OF DATA USE IDENTIFIERS (DUIS) (CONTINUED)

DUI NAME	DFI NO.	DUI NO.
USER DATA MESSAGE RECEIPT/COMPLIANCE	6003	001
USER DATA MESSAGE SECURITY CLASSIFICATION	6002	002
UNIT NAME	6010	013
URN	4004	012
USER DATA MESSAGE FORMAT	6001	012
USER DATA MESSAGE STANDARD VERSION	6001	011
USER DATA MESSAGE PRECEDENCE	6002	006
USER DATA MESSAGE SECURITY PADDING	6008	008
USER DATA MESSAGE SECURITY PADDING LENGTH	6009	006
USER DATA MESSAGE SIZE	6005	001
USER DATA MESSAGE VERSION	6001	014
VMF MESSAGE SUBTYPE	6001	013
YEAR	4098	001

TABLE B-V NUMERICAL LIST OF DATA USE IDENTIFIERS (DUIS)

DUI NAME	DFI NO.	DUI NO.
SECOND	380	001
HOUR	792	001
MINUTE	797	004
URN	4004	012
GPI	4014	001
FPI	4014	002
DAY OF MONTH	4019	001
GRI	4045	001
FRI	4045	002
FUNCTIONAL AREA DESIGNATOR	4081	001
MESSAGE NUMBER	4085	019
YEAR	4098	001
MONTH	4099	001
OPERATION INDICATOR	6001	005
HEADER VERSION	6001	006
DATA COMPRESSION TYPE	6001	010
USER DATA MESSAGE STANDARD VERSION	6001	011
USER DATA MESSAGE FORMAT	6001	012
VMF MESSAGE SUBTYPE	6001	013
USER DATA MESSAGE VERSION	6001	014
USER DATA MESSAGE SECURITY CLASSIFICATION	6002	002
CONTROL/RELEASE MARKING	6002	005
USER DATA MESSAGE PRECEDENCE	6002	006
USER DATA MESSAGE RECEIPT/COMPLIANCE	6003	001
CANTCO REASON	6003	002
CANTPRO REASON	6003	005
REPLY AMPLIFICATION	6004	001
USER DATA MESSAGE SIZE	6005	001
DTG EXTENSION	6005	002
HEADER SIZE	6005	003
GROUP SIZE	6005	004
FILE NAME	6006	001
MACHINE ACKNOWLEDGE REQUEST INDICATOR	6007	001
OPERATOR ACKNOWLEDGE REQUEST INDICATOR	6007	002
OPERATOR REPLY REQUEST INDICATOR	6007	003
RETRANSMIT INDICATOR	6007	004
SECURITY PARAMETERS INFORMATION	6008	001
KEYING MATERIAL ID	6008	002
CRYPTOGRAPHIC INITIALIZATION	6008	003
KEY TOKEN	6008	004

TABLE B-V NUMERICAL LIST OF DATA USE IDENTIFIERS (DUIS) (CONTINUED)

DUI NAME	DFI NO.	DUI NO.
AUTHENTICATION DATA (A)	6008	005
AUTHENTICATION DATA (B)	6008	006
SIGNED ACKNOWLEDGE REQUEST INDICATOR	6008	007
USER DATA MESSAGE SECURITY PADDING	6008	008
KEYING MATERIAL ID LENGTH	6009	001
CRYPTOGRAPHIC INITIALIZATION LENGTH	6009	002
KEY TOKEN LENGTH	6009	003
AUTHENTICATION DATA (A) LENGTH	6009	004
AUTHENTICATION DATA (B) LENGTH	6009	005
USER DATA MESSAGE SECURITY PADDING LENGTH	6009	006
UNIT NAME	6010	013
HEADER ZERO PADDING	6011	001

DFI	NAME	DEFINITION
380	SECOND	A UNIT OF TIME.

DUI	NAME	EXPLANATION
001	SECOND [6 BIT]	THE SECOND OF THE MINUTE.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
0 THROUGH 59 SECONDS	0 THROUGH 59	IN ONE SECOND INCREMENTS.
ILLEGAL	60 THROUGH 62	
NO STATEMENT	63	

DFI	NAME	DEFINITION
792	HOUR	EXPRESSES TIME OF DAY OR A PERIOD OF TIME IN HOURS.

DUI	NAME	EXPLANATION
001	HOUR [5 BIT]	EXPRESSES TIME OF DAY OR A PERIOD OF TIME IN HOURS.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
0 HOUR	0	
1 THROUGH 23 HOURS	1 THROUGH 23	IN 1 HOUR INCREMENTS.
ILLEGAL	24 THROUGH 30	
NO STATEMENT	31	

DFI	NAME	DEFINITION
797	MINUTE	EXPRESSES THE MINUTE OF THE HOUR.

DUI NAME	EXPLANATION
004 MINUTE [6 BIT]	THE MINUTE OF THE HOUR.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 004 -----		
0 THROUGH 59 MINUTES	0 THROUGH 59	IN ONE MINUTE INCREMENTS.
ILLEGAL	60 THROUGH 62	
NO STATEMENT	63	

DFI	NAME	DEFINITION
4004	MILITARY IDENTIFICATION	A SHORT SERIES OF ALPHABETIC OR NUMERIC CHARACTERS ASSIGNED TO UNIQUELY IDENTIFY THE MILITARY UNIT WHICH WILL FUNCTION AS A LINKAGE TO THE LONG ACTUAL MILITARY UNIT IDENTIFICATION.

DUI	NAME	EXPLANATION
012	URN [24 BIT]	A REFERENCE NUMBER USED BY UNITS A VMF INTERFACE TO UNIQUELY IDENTIFY FRIENDLY MILITARY UNITS, BROADCAST NETWORKS, AND MULTICAST GROUPS. UNIT REFERENCE NUMBER (URN) WILL BE ASSIGNED IN ACCORDANCE WITH INTERFACE OPERATING PROCEDURES.

----- FOR DUI 012 -----

0 THROUGH 1,999,999	0 THROUGH 1999999	U.S. ARMY URN BLOCK.
2,000,000 THROUGH 2,999,999	2000000 THROUGH 2999999	U.S. MARINE CORPS URN BLOCK.
3,000,000 THROUGH 3,999,999	3000000 THROUGH 3999999	U.S. AIR FORCE URN BLOCK.
4,000,000 THROUGH 4,999,999	4000000 THROUGH 4999999	U.S. NAVY URN BLOCK.
5,000,000 THROUGH 7,999,999	5000000 THROUGH 7999999	COCOM/MULTI-NATIONAL/INTERAGENCY URN BLOCK.
8,000,000 THROUGH 8,028,159	8000000 THROUGH 8028159	URN BLOCK FOR DYNAMIC ASSIGNMENT TO UNITS WITH SOURCE TRACK NUMBER ASSIGNMENTS 11000 THROUGH 77777 (OCTAL).
8,028,160 THROUGH 8,032,767	8028160 THROUGH 8032767	URN BLOCK FOR DYNAMIC ASSIGNMENT TO UNITS WITH SOURCE TRACK NUMBER ASSIGNMENTS 00000 THROUGH 10777 (OCTAL).
8,032,768 THROUGH 16,777,212	8032768 THROUGH 16777212	ACTIVE, NOT PRE-BLOCKED.
16,777,213	16777213	DISUSED.
16,777,214	16777214	INTELLIGENCE REPORT.
16,777,215	16777215	BROADCAST URN.

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

DUI	NAME	EXPLANATION
001	GPI [1 BIT]	GROUP PRESENCE INDICATOR (GPI) THAT INDICATES THE PRESENCE OR ABSENCE OF THE ASSOCIATED INFORMATION GROUP FOLLOWING THE GPI.
002	FPI [1 BIT]	FIELD PRESENCE INDICATOR (FPI) THAT INDICATES THE PRESENCE OR ABSENCE OF THE ASSOCIATED INFORMATION FIELD FOLLOWING THE FPI.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUIS 001 AND 002 -----		
NOT PRESENT	0	INFORMATION ASSOCIATED WITH THE INDICATOR IS OMITTED.
PRESENT	1	INFORMATION ASSOCIATED WITH THE INDICATOR IS PRESENT.

DFI	NAME	DEFINITION
4019	DAY	A 24-HOUR PERIOD RESERVED FOR A CERTAIN ACTIVITY.

DUI	NAME	EXPLANATION
001	DAY OF MONTH [5 BIT]	ONE OF 24 HOUR PERIODS OF A MONTH AS DEFINED BY THE GREGORIAN CALENDAR.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
ILLEGAL	0	
DAY 1 THROUGH 31	1 THROUGH 31	THE SPECIFIC DAY OF THE MONTH.

DFI	NAME	DEFINITION
4045	RECURRENCE INDICATOR	FOR USE WITHIN A MESSAGE TO INDICATE RECURRENCE.

DUI	NAME	EXPLANATION
001	GRI [1 BIT]	GROUP RECURRENCE INDICATOR (GRI) INDICATES THAT THE ASSOCIATED GROUP INFORMATION FOLLOWING THE GRI IS REPEATED.
002	FRI [1 BIT]	FIELD RECURRENCE INDICATOR (FRI) INDICATES THAT THE ASSOCIATED FIELD INFORMATION FOLLOWING THE FRI IS REPEATED.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUIS 001 AND 002 -----		
NOT REPEATED	0	INDICATES THIS IS THE LAST RECURRENCE OF INFORMATION ASSOCIATED WITH THE INDICATOR.
REPEATED	1	INDICATES THAT AT LEAST 1 MORE RECURRENCE OF INFORMATION IS ASSOCIATED WITH THE INDICATOR.

DFI	NAME	DEFINITION
4081	FUNCTIONAL AREA DESIGNATOR	PROVIDES THE NUMBERING CONVENTION FOR VARIABLE MESSAGE FORMAT.

DUI	NAME	EXPLANATION
001	FUNCTIONAL AREA DESIGNATOR [4 BIT]	IDENTIFIES THE FUNCTIONAL AREA OF A SPECIFIC VMF MESSAGE.

----- FOR DUI 001 -----

NETWORK CONTROL	0
GENERAL INFORMATION EXCHANGE	1
FIRE SUPPORT OPERATIONS	2
AIR OPERATIONS	3
INTELLIGENCE OPERATIONS	4
LAND COMBAT OPERATIONS	5
MARITIME OPERATIONS	6
COMBAT SERVICE SUPPORT	7
SPECIAL OPERATIONS	8
JTF OPERATIONS CONTROL	9
AIR DEFENSE/AIR SPACE CONTROL	10
UNDEFINED	11 THROUGH 15

DFI	NAME	DEFINITION
4085	NUMBER	AN IDENTIFIER OF AN ENTITY, COMMONLY CONSIDERED TO BE, OR REFERRED TO AS, A "NUMBER".

DUI	NAME	EXPLANATION
019	MESSAGE NUMBER [7 BIT]	A NUMBER WHICH IDENTIFIES A SPECIFIC MESSAGE WITHIN A FUNCTIONAL AREA.
	----- FOR DUI 019 -----	
	ILLEGAL	0
	NUMERIC	1 THROUGH 127

DFI	NAME	DEFINITION
4098	YEAR	A PERIOD OF EITHER 365 OR 366 DAYS AS DEFINED BY THE GREGORIAN CALENDAR.

DUI	NAME	EXPLANATION
001	YEAR [7 BIT]	A PERIOD OF EITHER 365 OR 366 DAYS AS DEFINED BY THE GREGORIAN CALENDAR.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 ----		
2000 THROUGH 2094	0 THROUGH 94	IN 1 YEAR INCREMENTS.
1995 THROUGH 1999	95 THROUGH 99	IN 1 YEAR INCREMENTS.
UNDEFINED	100 THROUGH 127	

DFI	NAME	DEFINITION
4099	MONTH	ONE OF TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY THE GREGORIAN CALENDAR.

DUI	NAME	EXPLANATION
001	MONTH [4 BIT]	ONE OF TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY THE GREGORIAN CALENDAR.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
ILLEGAL	0	
JANUARY	1	
FEBRUARY	2	
MARCH	3	
APRIL	4	
MAY	5	
JUNE	6	
JULY	7	
AUGUST	8	
SEPTEMBER	9	
OCTOBER	10	
NOVEMBER	11	
DECEMBER	12	
ILLEGAL	13 THROUGH 15	

DFI	NAME	DEFINITION
6001	USER DATA MESSAGE DATA DESIGNATOR	INDICATES SELECTION FROM AN ITEMIZED LIST

DUI	NAME	EXPLANATION
005	OPERATION INDICATOR [2 BIT]	USED TO INDICATE THAT THE USER DATA MESSAGE IS USED IN SUPPORT OF EITHER AN OPERATION, EXERCISE, TEST OR SIMULATION.
006	HEADER VERSION [4 BIT]	SPECIFIES THE VERSION OF THE MIL-STD-2045-47001 HEADER BEING USED FOR THE APPLICATION LAYER PROTOCOL DATA UNIT.
010	DATA COMPRESSION TYPE [2 BIT]	INDICATES THE TYPE OF COMPRESSION USED TO COMPRESS THE USER DATA MESSAGE.
011	USER DATA MESSAGE STANDARD VERSION [4 BIT]	CONTAINS A FOUR BIT BINARY CODEWORD THAT REPRESENTS THE VERSION OF THE MESSAGE STANDARD THAT IS USED TO CREATE THE USER DATA PORTION AND HAS ASSOCIATION WITH THE USE DATA MESSAGE FORMAT FIELD.
012	USER DATA MESSAGE FORMAT [4 BIT]	INDICATES THE FORMAT OF THE DATA CONTAINED IN THE USER DATA PORTION OF THE APPLICATION LAYER PROTOCOL DATA UNIT.
013	VMF MESSAGE SUBTYPE [7 BIT]	REPRESENTS THE NUMBER THAT IDENTIFIES A SPECIFIC CASE WITHIN A VMF MESSAGE. THE CASE DEPENDS ON THE SETTING OF THE USER MESSAGE FORMAT FIELD, THE FUNCTIONAL AREA DESIGNATOR FIELD, AND THE VMF MESSAGE NUMBER FIELD.
014	USER DATA MESSAGE VERSION [10 BIT]	IDENTIFIES THE VERSION OF THE USER DATA MESSAGE BEING TRANSMITTED IN THE USER DATA PORTION OF THE APPLICATION LAYER PROTOCOL DATA UNIT.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 005 -----		
OPERATION	0	
EXERCISE	1	
SIMULATION	2	
TEST	3	

DFI NAME
6001 USER DATA MESSAGE DATA DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
----- FOR DUI 006 -----		
MIL-STD-2045-47001	0	
MIL-STD-2045-47001B	1	
MIL-STD-2045-47001C	2	
MIL-STD-2045-47001D	3	
MIL-STD-2045-47001D Change 1	4	
MIL-STD-2045-47001E	5	
UNDEFINED	6 THROUGH 14	
VERSION SENT NOT IMPLEMENTED	15	USED IN RESPONSE TO AN APPLICATION LAYER PROTOCOL DATA UNIT IN WHICH THE VERSION FIELD IS SET TO VALUE 2 (47001C).
----- FOR DUI 010 -----		
UNIX COMPRESS/UNCOMPRESS	0	LEMPEL-ZIV-WELCH COMPRESSION ALGORITHM, WELCH 1984.
GZIP	1	LEMPEL-ZIV COMPRESSION ALGORITHM LEMPEL-ZIV 1977.
EXI	2	EFFICIENT XML INTERCHANGE (EXI).
UNDEFINED	3	
----- FOR DUI 011 -----		
---------- FOR LINK 16 UDMF = 0 ----------		
MIL-STD-6016	0	
MIL-STD-6016A	1	
MIL-STD-6016B	2	
MIL-STD-6016C	3	
MIL-STD-6016D	4	
MIL-STD-6016E	5	
MIL-STD-6016F	6	

DFI NAME
6001 USER DATA MESSAGE DATA DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
MIL-STD-6016G	7	
MIL-STD-6016H	8	
MIL-STD-6016I	9	
MIL-STD-6016C CHG1	10	
UNDEFINED	11 THROUGH 15	

FOR BINARY FILE		
UDMF = 1		

NOT PRESENT		

FOR VMF UDMF = 2		

VMF TIDP-TE R2	0	
VMF TIDP-TE R3	1	
VMF TIDP-TE R4	2	
VMF TIDP-TE R5	3	
VMF TIDP-FTE R6	4	
MIL-STD-6017	5	
MIL-STD-6017A	6	
MIL-STD-6017B	7	
MIL-STD-6017C	8	
MIL-STD-6017D	9	
MIL-STD-6017E	10	
RESERVED	11 THROUGH 14	RESERVED FOR FUTURE VERSIONS OF VMF.
USE USER DATA MESSAGE VERSION	15	ASSOCIATED WITH VMF.

FOR NITFS UDMF = 3		

V2.0	0	
V2.1	1	
UNDEFINED	2 THROUGH 15	

DFI NAME
6001 USER DATA MESSAGE DATA DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
FOR REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT UDMF = 4		
DISUSED		
FOR USMTF UDMF = 5		
MIL-STD-6040 Baseline 1993	0	
MIL-STD-6040 Baseline 1995	1	
MIL-STD-6040 Baseline 1997	2	
MIL-STD-6040 Baseline 1998	3	
MIL-STD-6040 Baseline 1999	4	
MIL-STD-6040 Baseline 2000	5	
MIL-STD-6040 Baseline 2001	6	
MIL-STD-6040 Baseline 2002	7	
MIL-STD-6040 Baseline 2003	8	
MIL-STD-6040 Baseline 2004	9	
MIL-STD-6040 Baseline 2005	10	
MIL-STD-6040 Baseline 2006	11	
MIL-STD-6040 Baseline 2007	12	
2008 (MIL-STD-6040A)	13	
2009 (MIL-STD-6040B)	14	
USE USER DATA MESSAGE VERSION	15	
FOR UDMF = 6		
DISUSED		

DFI NAME
6001 USER DATA MESSAGE DATA DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
FOR XML-MTF UDMF = 7		
UNDEFINED	0 THROUGH 5	
MIL-STD-6040 Baseline 2001	6	
MIL-STD-6040 Baseline 2002	7	
MIL-STD-6040 Baseline 2003	8	
MIL-STD-6040 Baseline 2004	9	
MIL-STD-6040 Baseline 2005	10	
MIL-STD-6040 Baseline 2006	11	
MIL-STD-6040 Baseline 2007	12	
2008 (MIL-STD-6040A)	13	
2009 (MIL-STD-6040B)	14	
USE USER DATA MESSAGE VERSION	15	
FOR VML UDMF = 8		
UNDEFINED	0 THROUGH 2	
VMF TIDP-TE R5	3	
VMF TIDP-FTE R6	4	
MIL-STD-6017	5	
MIL-STD-6017A	6	
MIL-STD-6017B	7	
MIL-STD-6017C	8	
MIL-STD-6017D	9	
MIL-STD-6017E	10	
RESERVED	11 THROUGH 14	RESERVED FOR FUTURE VERSIONS OF VMF.
USE USER DATA MESSAGE VERSION	15	

DFI NAME
6001 USER DATA MESSAGE DATA DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
----- FOR DUI 012 -----		
LINK 16	0	J-SERIES MESSAGE.
BINARY FILE	1	
VARIABLE MESSAGE FORMAT (VMF)	2	K-SERIES MESSAGE.
NATIONAL IMAGERY TRANSMISSION FORMAT SYSTEM (NITFS)	3	
REDISTRIBUTED APPLICATION LAYER PROTOCOL DATA UNIT	4	
UNITED STATES MESSAGE TEXT FORMAT (USMTF)	5	
DISUSED	6	
EXTENSIBLE MARKUP LANGUAGE MESSAGE TEXT FORMAT (XML-MTF)	7	
VARIABLE MESSAGE FORMAT MARKUP LANGUAGE (VML)	8	
UNDEFINED	9 THROUGH 15	
----- FOR DUI 013 -----		
ILLEGAL	0	
CASES 1.1 THROUGH 1.127	1 THROUGH 127	
----- FOR DUI 014 -----		
NUMERIC	0 THROUGH 1023	IDENTIFIES THE VERSION OF THE USER DATA MESSAGE BEING TRANSMITTED IN THE USER DATA PORTION OF THE APPLICATION LAYER PROTOCOL DATA UNIT.

DFI	NAME	DEFINITION
6002	USER DATA MESSAGE HANDLING DESIGNATOR	SPECIFIES RULES FOR HANDLING USER DATA MESSAGES

DUI	NAME	EXPLANATION
002	USER DATA MESSAGE SECURITY CLASSIFICATION [2 BIT]	A CATEGORY ASSIGNED TO CLASSIFIED MESSAGE INFORMATION OR MATERIAL TO SHOW THE DEGREE OF DAMAGE TO THE INTERESTS OF NATIONAL DEFENSE WHICH COULD RESULT FROM ITS UNAUTHORIZED DISCLOSURE AND TO SHOW THE STANDARD OF PROTECTION REQUIRED TO GUARD AGAINST UNAUTHORIZED DISCLOSURE.
005	CONTROL/RELEASE MARKING [9 BIT]	A FIXED LENGTH, NINE BIT INTEGER THAT IDENTIFIES A GEOGRAPHIC ENTITY OR COUNTRY AND THE DIGRAPH (BASED ON FIPS PUB 10-4) ASSIGNED TO THAT ENTITY TO WHICH THE USER DATA MESSAGE MAY BE RELEASED. THIS ESTABLISHES THE RESTRICTIONS OR REQUIREMENTS FOR SPECIAL HANDLING, ACCESS CONTROL, AND RELEASABILITY OF THE USER DATA MESSAGE.
006	USER DATA MESSAGE PRECEDENCE [3 BIT]	INDICATES THE PRECEDENCE OF A USER DATA MESSAGE.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 002 -----		
UNCLASSIFIED	0	
CONFIDENTIAL	1	
SECRET	2	
TOP SECRET	3	
----- FOR DUI 005 -----		
NO STATEMENT	0	
AFGHANISTAN (AF)	1	
ALBANIA (AL)	2	
ALGERIA (AG)	3	
AMERICAN SOMOA (AQ)	4	
ANDORRA (AN)	5	
ANGOLA (AO)	6	
ANGUILLA (AV)	7	
ANTARCTICA (AY)	8	
ANTIGUA AND BARBUDA (AC)	9	
ARGENTINA (AR)	10	
ARMENIA (AM)	11	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
AUSTRIA (AU)	15	
ARUBA (AA)	12	
ASHMORE AND CARTER ISLANDS (AT)	13	
AUSTRALIA (AS)	14	
AZERBAIJAN (AJ)	16	
BAHAMAS, THE (BF)	17	
BAHRAIN (BA)	18	
BAKER ISLAND (FQ)	19	
BANGLADESH (BG)	20	
BARBADOS (BB)	21	
BASSAS DA INDIA (BS)	22	BASSAS DA INDIA, EUROPA ISLAND, GLORIOSO ISLANDS, JUAN DE NOVA ISLANDS, AND TORMELIN ISLAND ARE CONTROLLED BY FRANCE AND ARE ADMINISTERED FROM REUNION.
BELARUS (BO)	23	
BELGIUM (BE)	24	
BELIZE (BH)	25	
BENIN (BN)	26	
BERMUDA (BD)	27	
BHUTAN (BT)	28	
BOLIVIA (BL)	29	
BOZNIA AND HERZEGOVINA (BK)	30	FORMER YUGOSLAV REPUBLIC.
BOTSWANA (BC)	31	
BOUVET ISLAND (BV)	32	
BRAZIL (BR)	33	
BRITISH INDIAN OCEAN TERRITORY (IO)	34	CHAGOS ARCHIPELAGO (INCLUDING DIEGO GARCIA).
BRITISH VIRGIN ISLANDS (VI)	35	
BRUNEI (BX)	36	
BULGARIA (BU)	37	
BURKINA FASO (UV)	38	FORMERLY UPPER VOLTA.
BURMA (BM)	39	LOCAL LONG FORM NAME TRANSLATED BY THE BURMESE AS "UNION OF MYANMAR."

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
BURUNDI (BY)	40	
CAMBODIA (CB)	41	
CAMEROON (CM)	42	
CANADA (CA)	43	
CAPE VERDE (CV)	44	
CAYMAN ISLANDS (CJ)	45	
CENTRAL AFRICAN REPUBLIC (CT)	46	
CHAD (CD)	47	
CHILE (CI)	48	
CHINA (CH)	49	WITH THE ESTABLISHMENT OF DIPLOMATIC RELATIONS WITH CHINA ON JANUARY 1, 1979, THE US GOVERNMENT RECOGNIZED THE PEOPLE'S REPUBLIC OF CHINA AS THE SOLE GOVERNMENT OF CHINA AND ACKNOWLEDGED THE CHINESE POSITION THAT THERE IS ONLY ONE CHINA AND THAT TAIWAN IS PART OF CHINA.
CHRISTMAS ISLAND (KT)	50	
CLIPPERTON ISLAND (IP)	51	
COCOS (KEELING) ISLANDS (CK)	52	
COLOMBIA (CO)	53	
COMOROS (CN)	54	
CONGO (CF)	55	
CONGO (DEMOCRATIC REPUBLIC OF THE) (CG)	56	CONGO IS THE OFFICIAL SHORT-FORM NAME FOR BOTH THE REPUBLIC OF THE CONGO AND THE DEMOCRATIC REPUBLIC OF THE CONGO (FORMERLY ZAIRE). TO DISTINGUISH ONE FROM THE OTHER, US DEPARTMENT OF STATE ADDS THE CAPITAL IN PARENTHESES (BRAZZAVILLE AND KINSHASA, RESPECTIVELY). THIS PRACTICE IS UNOFFICIAL AND PROVISIONAL.

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
COOK ISLANDS (CW)	57	
CORAL SEA ISLANDS (CR)	58	
COSTA RICA (CS)	59	
COTE D'IVOIRE (IV)	60	FORMERLY IVORY COAST.
CROATIA (HR)	61	FORMER YUGOSLAVIA REPUBLIC.
CUBA (CU)	62	
CYPRUS (CY)	63	
CZECH REPUBLIC (EZ)	64	
DENMARK (DA)	65	
DJIBOUTI (DJ)	66	
DOMINICA (DO)	67	
DOMINICAN REPUBLIC (DR)	68	
EAST TIMOR (TT)	69	
ECUADOR (EC)	70	
EGYPT (EG)	71	
EL SALVADOR (ES)	72	
EQUATORIAL GUINEA (EK)	73	
ERITREA (ER)	74	
ESTONIA (EN)	75	
ETHIOPIA (ET)	76	
EUROPA ISLAND (EU)	77	BASSAS DA INDIA, EUROPA ISLAND, GLORIOSO ISLANDS, JUAN DE NOVA ISLANDS, AND TORMELIN ISLAND ARE CONTROLLED BY FRANCE AND ARE ADMINISTERED FROM REUNION.
FALKLAND ISLANDS (FK)	78	FORMERLY INCLUDED SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS.
FAROE ISLANDS (FO)	79	
FIJI (FJ)	80	
FINLAND (FI)	81	
FRANCE (FR)	82	
FRENCH GUIANA (FG)	83	
FRENCH POLYNESIA (FP)	84	

DFI 6002 NAME: USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
FRENCH SOUTHERN AND ANTARCTIC LANDS (FS)	85	INCLUDES ILE AMSTERDAM, ILE SAINT-PAUL, ILES CROZET, AND ILES KERGUELEN IN THE SOUTHERN INDIAN OCEAN, ALONG WITH THE FRENCH-CLAIMED SECTOR OF ANTARCTICA, "TERRE ADELIE."
GABON (GB)	86	
GAMBIA, THE (GA)	87	
GAZA STRIP (GZ)	88	
GEORGIA (GG)	89	
GERMANY (GM)	90	
GHANA (GH)	91	
GIBRALTAR (GI)	92	
GLORIOSO ISLANDS (GO)	93	BASSAS DA INDIA, EUROPA ISLAND, GLORIOSO ISLANDS, JUAN DE NOVA ISLANDS, AND TORMELIN ISLAND ARE CONTROLLED BY FRANCE AND ARE ADMINISTERED FROM REUNION.
GREECE (GR)	94	
GREENLAND (GL)	95	
GRENADA (GJ)	96	
GUADELOUPE (GP)	97	
GUAM (GQ)	98	
GUATEMALA (GT)	99	
GUERNSEY (GK)	100	
GUINEA (GV)	101	
GUINEA-BISSAU (PU)	102	
GUYANA (GY)	103	
HAITI (HA)	104	
HEARD ISLAND AND MCDONALD ISLANDS (HM)	105	
HONDURAS (HO)	106	
HONG KONG (HK)	107	
HOWLAND ISLAND (HQ)	108	
HUNGARY (HU)	109	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
ICELAND (IC)	110	
INDIA (IN)	111	
INDONESIA (ID)	112	
IRAN (IR)	113	
IRAQ (IZ)	114	
IRELAND (EI)	115	
ISRAEL (IS)	116	
ITALY (IT)	117	
JAMAICA (JM)	118	
JAN MAYEN (JN)	119	
JAPAN (JA)	120	
JARVIS ISLAND (DQ)	121	
JERSEY (JE)	122	
JOHNSTON ATOLL (JQ)	123	
JORDAN (JO)	124	
JUAN DE NOVA ISLAND (JU)	125	BASSAS DA INDIA, EUROPA ISLAND, GLORIOSO ISLANDS, JUAN DE NOVA ISLANDS, AND TORMELIN ISLAND ARE CONTROLLED BY FRANCE AND ARE ADMINISTERED FROM REUNION.
KAZAKHSTAN (KZ)	126	
KENYA (KE)	127	
KINGMAN REEF (KQ)	128	
KIRIBATI (KR)	129	
KOREA, DEMOCRATIC PEOPLES REPUBLIC OF (KN)	130	
KOREA, REPUBLIC OF (KS)	131	
KUWAIT (KU)	132	
KYRGYZSTAN (KG)	133	
LAOS (LA)	134	
LATVIA (LG)	135	
LEBANON (LE)	136	
LESOTHO (LT)	137	
LIBERIA (LI)	138	
LIBYA (LY)	139	
LIECHTENSTEIN (LS)	140	
LITHUANIA (LH)	141	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
LUXEMBOURG (LU)	142	
MACAU (MC)	143	
MACEDONIA (MK)	144	
MADAGASCAR (MA)	145	
MALAWI (MI)	146	
MALAYSIA (MY)	147	
MALDIVES (MV)	148	
MALI (ML)	149	
MALTA (MT)	150	
MAN, ISLE OF (IM)	151	
MARSHALL ISLANDS (RM)	152	
MARTINIQUE (MB)	153	
MAURITANIA (MR)	154	
MAURITIUS (MP)	155	
MAYOTTE (MF)	156	
MEXICO (MX)	157	
MICRONESIA, FEDERATED STATES OF (FM)	158	
MIDWAY ISLANDS (MQ)	159	
MOLDOVA (MD)	160	
MONACO (MN)	161	
MONGOLIA (MG)	162	
MONTSERRAT (MH)	163	
MOROCCO (MO)	164	
MOZAMBIQUE (MZ)	165	
NAMIBIA (WA)	166	
NAURU (NR)	167	
NAVASSA ISLAND (BQ)	168	
NEPAL (NP)	169	
NETHERLANDS (NL)	170	
NETHERLANDS ANTILLES (NT)	171	
NEW CALEDONIA (NC)	172	
NEW ZEALAND (NZ)	173	
NICARAGUA (NU)	174	
NIGER (NG)	175	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
NIGERIA (NI)	176	
NIUE (NE)	177	
NORFOLK ISLAND (NF)	178	
NORTHERN MARIANA ISLANDS (CQ)	179	
NORWAY (NO)	180	
OMAN (MU)	181	
OTHER COUNTRY (OO)	182	
PAKISTAN (PK)	183	
PALAU (PS)	184	
PALMYRA ATOLL (LQ)	185	
PANAMA (PM)	186	
PAPUA NEW GUINEA (PP)	187	
PARACEL ISLANDS (PF)	188	SOUTH CHINA SEA ISLANDS OCCUPIED BY CHINA BUT CLAIMED BY VIETNAM.
PARAGUAY (PA)	189	
PERU (PE)	190	
PHILIPPINES (RP)	191	
PITCAIRN ISLANDS (PC)	192	
POLAND (PL)	193	
PORTUGAL (PO)	194	
PUERTO RICO (RQ)	195	
QATAR (QA)	196	
REUNION (RE)	197	BASSAS DA INDIA, EUROPA ISLAND, GLORIOSO ISLANDS, JUAN DE NOVA ISLANDS, AND TORMELIN ISLAND ARE CONTROLLED BY FRANCE AND ARE ADMINISTERED FROM REUNION.
ROMANIA (RO)	198	
RUSSIA (RS)	199	
RWANDA (RW)	200	
ST. KITTS AND NEVIS (SC)	201	FORMERLY ST. CHRISTOPHER AND NEVIS.
ST. HELENA (SH)	202	
ST. LUCIA (ST)	203	
ST. PIERRE AND MIQUELON (SB)	204	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
ST. VINCENT AND THE GRENADINES (VC)	205	
SAMOA (WS)	206	
SAN MARINO (SM)	207	
SAO TOME AND PRINCIPE (TP)	208	
SAUDI ARABIA (SA)	209	
SENEGAL (SG)	210	
SEYCHELLES (SE)	211	
SIERRA LEONE (SL)	212	
SINGAPORE (SN)	213	
SLOVAKIA (LO)	214	WITH THE COLLAPSE OF SOVIET AUTHORITY IN 1989, CZECHOSLOVAKIA REGAINED ITS FREEDOM THROUGH A PEACEFUL "VELVET REVOLUTION." ON 1 JANUARY 1993, THE COUNTRY UNDERWENT A "VELVET DIVORCE" INTO ITS TWO NATIONAL COMPONENTS, THE CZECH REPUBLIC AND SLOVAKIA.
SLOVENIA (SI)	215	FORMER YUGOSLAV REPUBLIC.
SOLOMON ISLANDS (BP)	216	
SOMALIA (SO)	217	
SOUTH AFRICA (SF)	218	
SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS (SX)	219	DEPENDENT TERRITORY OF THE UNITED KINGDOM (ALSO CLAIMED BY ARGENTINA).
SPAIN (SP)	220	
SPRATLY ISLANDS (PG)	221	
SRI LANKA (CE)	222	
SUDAN (SU)	223	
SURINAME (NS)	224	
SVALBARD (SV)	225	
SWAZILAND (WZ)	226	
SWEDEN (SW)	227	
SWITZERLAND (SZ)	228	
SYRIA (SY)	229	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
TAIWAN (TW)	230	WITH THE ESTABLISHMENT OF DIPLOMATIC RELATIONS WITH CHINA ON JANUARY 1, 1979, THE US GOVERNMENT RECOGNIZED THE PEOPLE'S REPUBLIC OF CHINA AS THE SOLE GOVERNMENT OF CHINA AND ACKNOWLEDGED THE CHINESE POSITION THAT THERE IS ONLY ONE CHINA AND THAT TAIWAN IS PART OF CHINA.
TAJIKISTAN (TI)	231	
TANZANIA (TZ)	232	
THAILAND (TH)	233	
TOGO (TO)	234	
TOKELAU (TL)	235	
TONGA (TN)	236	
TRINIDAD AND TOBAGO (TD)	237	
TROMELIN ISLAND (TE)	238	
TUNISIA (TS)	239	
TURKEY (TU)	240	
TURKMENISTAN (TX)	241	
TURKS AND CAICOS ISLANDS (TK)	242	
TUVALU (TV)	243	
UGANDA (UG)	244	
UKRAINE (UP)	245	
UNITED ARAB EMIRATES (AE)	246	
UNITED KINGDOM (UK)	247	
UNITED STATES (US)	248	
URUGUAY (UY)	249	
UZBEKISTAN (UZ)	250	
VANUATU (NH)	251	FORMERLY NEW HEBRIDES.
VATICAN CITY (VT)	252	
VENEZUELA (VE)	253	
VIETNAM (VM)	254	
VIRGIN ISLANDS, US (VQ)	255	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
WAKE ISLAND (WQ)	256	
WALLIS AND FUTUNA (WF)	257	
WEST BANK (WE)	258	
WESTERN SAHARA (WI)	259	
YEMEN (YM)	260	
YUGOSLAVIA (YI)	261	
ZAMBIA (ZA)	262	
ZIMBABWE (ZI)	263	
EXERCISE BLACK COUNTRY (OA)	264	
EXERCISE BLACK FORCES (OB)	265	USED IN REPORTING OF INTELLIGENCE ON FORMER WARSAW PACT EXERCISES TO DENOTE THOSE UNITS REPRESENTING FORMER WARSAW PACT FORCES DURING SUCH EXERCISES.
EXERCISE BLUE COUNTRY (OC)	266	FRIENDLY COUNTRIES DURING EXERCISES.
EXERCISE BLUE FORCE (OD)	267	THOSE FORCES USED IN A FRIENDLY ROLE DURING EXERCISES.
EXERCISE FRIENDLY COUNTRY (YC)	268	NATIONAL GEOGRAPHIC ENTITY POSITIVELY IDENTIFIED AS FRIENDLY.
EXERCISE FRIENDLY FORCE (YY)	269	AIR, SEA, OR GROUND UNIT(S), POSITIVELY IDENTIFIED AS FRIENDLY.
EXERCISE HOSTILE COUNTRY (XC)	270	NATIONAL GEOGRAPHIC ENTITY POSITIVELY IDENTIFIED AS HOSTILE.
EXERCISE HOSTILE FORCE (XX)	271	AIR, SEA, OR GROUND UNIT(S), POSITIVELY IDENTIFIED AS HOSTILE.
EXERCISE NEUTRAL COUNTRY (ZC)	272	NATIONAL GEOGRAPHIC ENTITY POSITIVELY IDENTIFIED AS NEUTRAL.
EXERCISE NEUTRAL FORCE (ZZ)	273	AIR, SEA, OR GROUND UNIT(S), POSITIVELY IDENTIFIED AS NEUTRAL.
EXERCISE ORANGE COUNTRY (OJ)	274	ENEMY COUNTRIES DURING EXERCISES.
EXERCISE ORANGE FORCE (OK)	275	THOSE FORCES USED IN AN ENEMY ROLE DURING EXERCISES.

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
EXERCISE RED COUNTRY (OR)	276	
EXERCISE RED FORCE (OE)	277	
EXERCISE WHITE COUNTRY (ON)	278	FRIENDLY NON-COMBATANT COUNTRIES AND CERTAIN THIRD WORLD UNITS.
EXERCISE NATO FORCE (OT)	279	THOSE FORCES MADE AVAILABLE TO NATO BY MEMBER NATIONS.
EXERCISE PURPLE FORCE (OL)	280	THOSE FORCES USED TO OPPOSE BOTH BLUE AND ORANGE FORCES IN EXERCISES. THIS IS USUALLY APPLICABLE TO SUBMARINES AND AIRCRAFT.
EXERCISE SPARE NUMBER ONE (XA)	281	
EXERCISE SPARE NUMBER TWO (XB)	282	
EXERCISE UNITED NATIONS FORCE (UU)	283	THOSE FORCES MADE AVAILABLE TO NATO BY MEMBER NATIONS.
EXERCISE FORMER WARSAW PACT FORCE (OW)	284	THOSE FORCES MADE AVAILABLE BY FORMER WARSAW PACT MEMBER NATIONS.
NAT/ALL-1 THROUGH NAT/ ALL-28	285 THROUGH 312	NATIONAL (NAT)/ALLIANCE (ALL).
SPANISH NORTH AFRICA (SQ)	313	
ABKHAZIA (AB)	314	ONE OF TWO SEPARATIST REGIONS IN GEORGIA (ABKHAZIA AND SOUTH OSSETIA).
AZORES (AZ)	315	
BOPHUTHATSWANA (BW)	316	PART OF SOUTH AFRICA.
CARIBBEAN (EXCLUDING ANTIGUA AND BARBUDA) (CC)	317	
CRIMEA (CX)	318	PART OF UKRAINE.
DISUSED	319	
EASTERN CARIBBEAN COUNTRIES (EA)	320	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
EASTERN EUROPEAN COUNTRIES (PW)	321	
FALKLAND ISLAND DEPENDENCIES (FL)	322	
FAR EAST COUNTRIES (FE)	323	
KOSOVO (KO)	324	
LATIN AMERICA (LM)	325	
MIDDLE EASTERN/NORTH AFRICAN COUNTRIES (ME)	326	
NAGORNO-KARABAKH (NK)	327	ARMENIAN-POPULATED ENCLAVE ASSIGNED TO SOVIET AZERBAIJAN IN THE 1920S BY MOSCOW. HELD BY ARMENIA SINCE MAY 1994.
NORDIC COUNTRIES (NN)	328	
NORTH OSSETIA (OS)	329	ONE OF TWO SEPARATIST REGIONS IN GEORGIA (ABKAHAZIA AND SOUTH OSSETIA).
SOUTH AMERICA (UT)	330	
SOUTH ASIA (AI)	331	
SOUTH MARIANA ISLAND (MS)	332	
SOUTH OSSETIA (OF)	333	ONE OF TWO SEPARATIST REGIONS IN GEORGIA (ABKAHAZIA AND SOUTH OSSETIA).
SOUTH PACIFIC ISLAND NATIONS OR TERRITORIES (PI)	334	
SOUTH EAST ASIA (EO)	335	
SUB-SAHARAN AFRICA (UB)	336	
TARTAR HOMELAND (TJ)	337	
TRANSKEI (TR)	338	AREA OR CITY IN SOUTH AFRICA.
UNIDENTIFIED (UI)	339	
WEST EUROPEAN COUNTRIES (EW)	340	
WEST HEMISPHERE (HW)	341	

DFI NAME
6002 USER DATA MESSAGE HANDLING DESIGNATOR

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
WORLDWIDE (GW)	342	
SERBIA AND MONTENEGRO (YI)	343	
UNDEFINED	344 THROUGH 511	
----- FOR DUI 006 -----		
ROUTINE	0	USED FOR ALL TYPES OF USER DATA MESSAGES THAT JUSTIFY TRANSMISSION BY RAPID MEANS UNLESS OF SUFFICIENT URGENCY TO REQUIRE A HIGHER PRECEDENCE.
PRIORITY	1	USED FOR USER DATA MESSAGES THAT REQUIRE EXPEDITIOUS ACTION BY THE ADDRESSEE(S) AND/OR FURNISHES ESSENTIAL INFORMATION FOR THE CONDUCT OF OPERATIONS IN PROGRESS WHEN ROUTINE PRECEDENCE WILL NOT SUFFICE.
IMMEDIATE	2	USED FOR USER DATA MESSAGES RELATING TO SITUATIONS THAT GRAVELY AFFECT THE SECURITY OF NATIONAL/ALLIED FORCES OR POPULACE AND THAT REQUIRE IMMEDIATE DELIVERY TO THE ADDRESSEE(S).
FLASH	3	USED FOR INITIAL ENEMY CONTACT USER DATA MESSAGES OR OPERATIONAL COMBAT MESSAGES OF EXTREME URGENCY.
FLASH OVERRIDE	4	USED FOR USER DATA MESSAGES OF HIGHER PRECEDENCE THAN FLASH.
UNDEFINED	5 THROUGH 7	

DFI	NAME	DEFINITION
6003	USER DATA MESSAGE PROCESSING DESIGNATOR	INDICATES USER DATA MESSAGE DISPOSITION.

DUI	NAME	EXPLANATION
001	USER DATA MESSAGE RECEIPT/COMPLIANCE [3 BIT]	INDICATES THE RECIPIENT'S ABILITY TO COMPLY WITH A RECEIVED USER DATA MESSAGE.
002	CANTCO REASON [3 BIT]	INDICATES THE REASON A RECIPIENT CANNOT COMPLY WITH A RECEIVED USER DATA MESSAGE.
005	CANTPRO REASON [6 BIT]	INDICATES THE REASON THE RECIPIENT CANNOT PROCESS A RECEIVED USER DATA MESSAGE.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
UNDEFINED	0	
MACHINE RECEIPT	1	MACHINE RECEIPT - AUTOMATICALLY GENERATED IN RESPONSE TO A MACHINE ACKNOWLEDGE REQUEST FROM THE ORIGINATOR TO INDICATE THAT THE ORIGINAL USER DATA MESSAGE CAN BE SUCCESSFULLY PROCESSED AT THE ULTIMATE DESTINATION.
CANTPRO	2	CANNOT PROCESS - AUTOMATICALLY GENERATED TO INDICATE THAT AN ORIGINAL USER DATA MESSAGE CANNOT BE SUCCESSFULLY PROCESSED AT THE ULTIMATE DESTINATION.
OPERATOR ACKNOWLEDGE	3	OPERATOR ACKNOWLEDGE - A POSITIVE OPERATOR-GENERATED AKNOWLEDGMENT TO INDICATE RECEIPT OF A USER DATA MESSAGE AT THE ULTIMATE DESTINATION.
WILCO	4	WILL COMPLY - AN OPERATOR REPLY GENERATED TO INDICATE THAT A RECEIVED USER DATA MESSAGE IS UNDERSTOOD AND THAT THE ULTIMATE DESTINATION WILL COMPLY.

DFI	NAME	DEFINITION
6003	USER DATA MESSAGE PROCESSING DESIGNATOR	INDICATES USER DATA MESSAGE DISPOSITION.

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
HAVCO	5	HAVE COMPLIED - AN OPERATOR REPLY GENERATED TO INDICATE THAT A RECEIVED USER DATA MESSAGE IS UNDERSTOOD AND THAT THE ULTIMATE DESTINATION HAS COMPLIED.
CANTCO	6	CANNOT COMPLY - AN OPERATOR REPLY GENERATED TO INDICATE THAT A RECEIVED USER DATA MESSAGE CANNOT OR WILL NOT BE CARRIED OUT.
UNDEFINED	7	
----- FOR DUI 002 -----		
COMMUNICATIONS PROBLEM	0	
AMMUNITION PROBLEM	1	
PERSONNEL PROBLEM	2	
FUEL PROBLEM	3	
TERRAIN/ENVIRONMENT PROBLEM	4	
EQUIPMENT PROBLEM	5	
TACTICAL SITUATION PROBLEM	6	
OTHER	7	
----- FOR DUI 005 -----		
UNDEFINED	0	
FIELD CONTENT INVALID	1	
USER DATA MESSAGE INCORRECTLY ROUTED	2	
ADDRESS INACTIVE	3	
REFERENCE POINT UNKNOWN TO RECEIVING AGENCY	4	
FIRE UNITS ARE CONTROLLED BY RECEIVING AGENCY	5	
MISSION IS CONTROLLED BY RECEIVING AGENCY	6	
MISSION NUMBER UNKNOWN BY RECEIVING AGENCY	7	

DFI	NAME	DEFINITION
6003	USER DATA MESSAGE PROCESSING DESIGNATOR	INDICATES USER DATA MESSAGE DISPOSITION.

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
TARGET NUMBER UNKNOWN BY RECEIVING AGENCY	8	
SCHEDULE NUMBER UNKNOWN BY RECEIVING AGENCY	9	
INCORRECT CONTROLLING ADDRESS FOR A GIVEN TRACK NUMBER	10	
TRACK NUMBER NOT IN OWN TRACK FILE	11	
INVALID ACCORDING TO GIVEN FIELD	12	
USER DATA MESSAGE CANNOT BE CONVERTED	13	
AGENCY FILE FULL	14	
AGENCY DOES NOT RECOGNIZE THIS MESSAGE NUMBER	15	
AGENCY CANNOT CORRELATE USER DATA MESSAGE TO CURRENT FILE CONTENT	16	
AGENCY LIMIT EXCEEDED ON REPEATED FIELDS OR GROUPS	17	
AGENCY COMPUTER SYSTEM INACTIVE	18	
ADDRESSEE UNKNOWN	19	
CAN'T FORWARD (AGENCY FAILURE)	20	
CAN'T FORWARD (LINK FAILURE)	21	
ILLOGICAL JUXTAPOSITION OF APPLICATION HEADER FIELDS	22	
CANNOT UNCOMPRESS UNIX (LZW) COMPRESSED DATA	23	
CANNOT UNCOMPRESS LZ-77 COMPRESSED DATA	24	
USER DATA MESSAGE TOO OLD, BASED ON PERISHABILITY	25	
SECURITY LEVEL RESTRICTION	26	
AUTHENTICATION FAILURE	27	
CERTIFICATE NOT FOUND	28	
CERTIFICATE INVALID	29	

DFI	NAME	DEFINITION
6003	USER DATA MESSAGE PROCESSING DESIGNATOR	INDICATES USER DATA MESSAGE DISPOSITION.

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
DO NOT SUPPORT THIS SECURITY PARAMETERS INFORMATION (SPI) VALUE	30	
CANNOT GENERATE A SIGNED ACKNOWLEDGMENT	31	
RESPONSE NOT AVAILABLE FOR RETRANSMISSION	32	
APPLICATION HEADER SIZE FIELD VALUE DOES NOT EQUAL RECEIVED HEADER SIZE	33	
USER DATA MESSAGE SIZE FIELD VALUE DOES NOT EQUAL RECEIVED USER DATA MESSAGE SIZE	34	
APPLICATION HEADER ZERO PADDING FIELD VALUE OTHER THAN "0"	35	
USER DATA MESSAGE STANDARD VERSION NOT SUPPORTED	36	
USER DATA MESSAGE VERSION NOT SUPPORTED	37	
USER DATA MESSAGE CASE NOT SUPPORTED	38	
CANNOT UNCOMPRESS EXI COMPRESSED	39	EFFICIENT XML INTERCHANGE (EXI).
UNDEFINED	40 THROUGH 63	

DFI	NAME	DEFINITION
6004	USER DATA MESSAGE HANDLING COMMENTS	TEXT RELATED TO HANDLING AND PROCESSING A USER DATA MESSAGE

DUI	NAME	EXPLANATION
001	REPLY AMPLIFICATION	PROVIDES TEXTUAL DATA AMPLIFYING THE RECIPIENT'S REPLY TO A USER DATA MESSAGE.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
----- THE 350 CHARACTERS OF THIS REPLY AMPLIFICATION ARE DIVIDED INTO 50 GROUPS OF 7 BITS EACH REPRESENTING ASCII CHARACTER CODING. REGEX: [-A-Za-z0-9!"#$%&'*+;<=>@\[\\\]^_`{|}~(),./:?{1,64}		
ILLEGAL	0 THROUGH 31	
BLANK CHARACTER	32	ASCII SPACE
EXTENDED SPECIAL CHARACTERS	33 THROUGH 39	ASCII ! " # $ % &
EXTENDED SPECIAL CHARACTERS	40 THROUGH 41	ASCII ( )
EXTENDED SPECIAL CHARACTERS	42 THROUGH 43	ASCII * +
SPECIAL CHARACTERS	44 THROUGH 47	ASCII , - .
NUMERIC CHARACTERS	48 THROUGH 57	ASCII 0 TO 9
SPECIAL CHARACTER	58	ASCII :
EXTENDED SPECIAL CHARACTERS	59 THROUGH 62	ASCII ; < = >
SPECIAL CHARACTER	63	ASCII ?
EXTENDED SPECIAL CHARACTER	64	ASCII @
UPPERCASE ALPHABETIC CHARACTERS	65 THROUGH 90	ASCII A TO Z
EXTENDED SPECIAL CHARACTERS	91 THROUGH 96	ASCII [/] ^ _ `
LOWERCASE ALPHABETIC CHARACTERS	97 THROUGH 122	ASCII a to z
EXTENDED SPECIAL CHARACTERS	123 THROUGH 126	ASCII { | } ~
END OF LITERAL FIELD MARKER	127	ASCII DELETE USED TO SIGNIFY TRUNCATION OF THE FIELD.

DFI	NAME	DEFINITION
6005	USER DATA MESSAGE HEADER NUMBER	AN IDENTIFIER OF AN ENTITY, COMMONLY CONSIDERED TO BE, OR REFERRED TO AS A "NUMBER" AND USED IN THE MIL-STD-2045-47001 APPLICATION HEADER.

DUI	NAME	EXPLANATION
001	USER DATA MESSAGE SIZE [20 BIT]	A BINARY NUMBER INDICATING THE SIZE OF THE USER DATA MESSAGE IN OCTETS.
002	DTG EXTENSION [12 BIT]	A NUMBER THAT DISAMBIGUATES BETWEEN TWO OR MORE USER DATA MESSAGES WITH THE SAME DATE TIME GROUP.
003	HEADER SIZE [16 BIT]	INDICATES THE SIZE OF THE APPLICATION HEADER IN OCTETS.
004	GROUP SIZE [12 BIT]	A BINARY NUMBER INDICATING THE SIZE, IN BITS, OF THE FUTURE USE GROUP IN WHICH THE FIELD IS CONTAINED. IN A PRIMARY FUTURE USE GROUP, THE GROUP SIZE FIELD INDICATES THE SIZE IN BITS OF THE PRIMARY FUTURE USE GROUP IN WHICH THE FIELD IS CONTAINED, INCLUDING ALL NESTED SUB-GROUPS AND GROUP SIZE FIELDS, AND EXCLUDING THE 12 BITS OF THE PRIMARY FUTURE USE GROUP GROUP SIZE FIELD. IN A SUB-GROUP NESTED WITHIN A PRIMARY FUTURE USE GROUP, THE GROUP SIZE FIELD INDICATES THE SIZE IN BITS OF THE SUB-GROUP IN WHICH THE FIELD IS CONTAINED, AND EXCLUDING THE 12 BITS OF THE SUB-GROUP GROUP SIZE FIELD.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
ILLEGAL	0	
NUMERIC	1 THROUGH 1048575	IN 1 OCTET INCREMENTS.

DFI NAME
6005 USER DATA MESSAGE HEADER NUMBER

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
----- FOR DUI 002 -----		
NUMERIC	0 THROUGH 4095	
----- FOR DUI 003 -----		
ILLEGAL	0	
NUMERIC	1 THROUGH 65535	IN 1 OCTET INCREMENTS.
----- FOR DUI 004 -----		
ILLEGAL	0	
NUMERIC	1 THROUGH 4095	IN 1 OCTET INCREMENTS.

DFI	NAME	DEFINITION
6006	FILE NAME	THE NAME OF A COMPUTER FILE OR DATA BLOCK.

DUI	NAME	EXPLANATION
001	FILE NAME [448 BIT]	THE NAME OF THE BINARY FILE CONTAINED IN THE USER DATA PORTION OF THE APPLICATION LAYER PROTOCOL DATA UNIT.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
----- THE 448 BITS OF THIS DUI ARE DIVIDED INTO 64 GROUPS OF 7 BITS ----- EACH REPRESENTING ASCII CHARACTER CODING. THE LAST FOUR ----- CHARACTERS OF THE FIELD MAY CONSIST OF A PERIOD FOLLOWED BY A THREE ----- CHARACTER ENDING, INDICATIVE OF THE FILE TYPE (E.G., .TXT, .DOC, ----- .EXE, .BIN). THE ASCII DELETE CHARACTER IS LEGAL. -----		
REGEX: [-A-Za-z0-9!"#$%&'*+;<=>@\[\\\]^_`{|}~(),./:?{1,64}		
ILLEGAL	0 THROUGH 31	
BLANK CHARACTER	32	ASCII SPACE
EXTENDED SPECIAL CHARACTERS	33 THROUGH 39	ASCII ! " # $ % &
EXTENDED SPECIAL CHARACTERS	40 THROUGH 41	ASCII ( )
EXTENDED SPECIAL CHARACTERS	42 THROUGH 43	ASCII * +
SPECIAL CHARACTERS	44 THROUGH 47	ASCII , - .
NUMERIC CHARACTERS	48 THROUGH 57	ASCII 0 TO 9
SPECIAL CHARACTER	58	ASCII :
EXTENDED SPECIAL CHARACTERS	59 THROUGH 62	ASCII ; < = >
SPECIAL CHARACTER	63	ASCII ?
EXTENDED SPECIAL CHARACTER	64	ASCII @
UPPERCASE ALPHABETIC CHARACTERS	65 THROUGH 90	ASCII A TO Z
EXTENDED SPECIAL CHARACTERS	91 THROUGH 96	ASCII [/] ^ _ `
LOWERCASE ALPHABETIC CHARACTERS	97 THROUGH 122	ASCII a to z
EXTENDED SPECIAL CHARACTERS	123 THROUGH 126	ASCII { | } ~
END OF LITERAL FIELD MARKER	127	ASCII DELETE USED TO SIGNIFY TRUNCATION OF THE FIELD.

DFI	NAME	DEFINITION
6007	USER DATA MESSAGE HEADER 1-BIT INDICATION	INDICATES AN EITHER/OR CONDITION USED IN THE MIL-STD-2045-47001 APPLICATION HEADER.

DUI	NAME	EXPLANATION
001	MACHINE ACKNOWLEDGE REQUEST INDICATOR [1 BIT]	INDICATES WHETHER THE ORIGINATOR REQUIRES A MACHINE ACKNOWLEDGE FOR THE USER DATA MESSAGE.
002	OPERATOR ACKNOWLEDGE REQUEST INDICATOR [1 BIT]	INDICATES WHETHER THE ORIGINATOR REQUIRES AN OPERATOR ACKNOWLEDGE FOR THE USER DATA MESSAGE.
003	OPERATOR REPLY REQUEST INDICATOR [1 BIT]	INDICATES WHETHER THE ORIGINATOR REQUIRES AN OPERATOR REPLY FOR THE USER DATA MESSAGE.
004	RETRANSMIT INDICATOR [1 BIT]	INDICATES WHETHER THIS USER DATA MESSAGE IS A RETRANSMISSION.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001-003 -----		
NOT REQUIRED	0	
REQUIRED	1	
----- FOR DUI 004 -----		
ORIGINAL	0	
RETRANSMISSION	1	

DFI	NAME	DEFINITION
6008	SECURITY PARAMETERS	PARAMETERS AND ALGORITHMS USED IN SECURITY PROCESSING.

DUI	NAME	EXPLANATION
001	SECURITY PARAMETERS INFORMATION [4 BIT]	IDENTIFIES THE PARAMETERS AND ALGORITHMS THAT ENABLE UNAMBIGUOUS SECURITY PROCESSING.
002	KEYING MATERIAL ID [64 BIT]	IDENTIFIES THE KEY, A UNIQUE VALUE, WHICH WAS USED FOR ENCRYPTION.
003	CRYPTOGRAPHIC INITIALIZATION [1024 BIT]	IDENTIFIES A SEQUENCE OF BITS USED BY THE ORIGINATOR AND RECIPIENT TO INITIALIZE THE ENCRYPTION AND DECRYPTION PROCESS.
004	KEY TOKEN [16384 BIT]	CONTAINS INFORMATION WHICH ENABLES RECIPIENTS TO DECRYPT THE USER DATA ASSOCIATED WITH THIS APPLICATION LAYER PROTOCOL DATA UNIT
005	AUTHENTICATION DATA (A) [8192 BIT]	AN AUTHENTICATION TOKEN CREATED BY THE ORIGINATOR IN ACCORDANCE WITH THE RULES OF THE SECURITY PARAMETERS INFORMATION (SPI) IN FORCE. UP TO 128 64-BIT BLOCKS AS SPECIFIED BY THE AUTHENTICATION DATA (A) LENGTH FIELD. THE AUTHENTICATION DATA (A) FIELD PROVIDES FOR DATA ORIGIN AUTHENTICATION, CONNECTIONLESS INTEGRITY AND NON-REPUDIATION WITH PROOF OF ORIGIN. IT IS GENERATED BY DIGITALLY SIGNING THE HASH OF BOTH THE APPLICATION HEADER AND USER DATA IN ACCORDANCE WITH FIPS 180-4.
006	AUTHENTICATION DATA (B) [8192 BIT]	A DIGITAL SIGNATURE (PROOF OF RECEIPT) OF THE USER DATA MESSAGE WHICH IS BEING ACKNOWLEDGED. WITH THE RULES OF THE SECURITY PARAMETERS INFORMATION (SPI) IN FORCE. UP TO 128 64-BIT BLOCKS AS SPECIFIED BY THE AUTHENTICATION DATA (B) LENGTH FIELD. THE AUTHENTICATION DATA (B) FIELD PROVIDES FOR DATA ORIGIN AUTHENTICATION, CONNECTIONLESS INTEGRITY AND NON-REPUDIATION WITH PROOF OF ORIGIN. IT IS GENERATED BY DIGITALLY SIGNING THE HASH OF BOTH THE APPLICATION HEADER AND USER DATA IN ACCORDANCE WITH FIPS 180-4.
007	SIGNED ACKNOWLEDGE REQUEST INDICATOR [1 BIT]	INDICATES WHETHER THE ORIGINATOR OF A USER DATA MESSAGE REQUIRES A SIGNED RESPONSE FROM THE RECIPIENT.

DFI	NAME	DEFINITION
6008	SECURITY PARAMETERS	PARAMETERS AND ALGORITHMS USED IN SECURITY PROCESSING.

DUI NAME	EXPLANATION
008 USER DATA MESSAGE SECURITY PADDING [2040 BIT]	THE USER DATA MESSAGE SECURITY PADDING LENGTH FIELD IS AN 8-BIT BINARY FIELD WHOSE VALUE DEFINES THE SIZE, IN OCTETS, OF THE USER DATA MESSAGE SECURITY PADDING FIELD. THE USER DATA MESSAGE SECURITY PADDING LENGTH FIELD VALUE REPRESENTS THE NUMBER OF OCTETS IN THE RANGE OF 0 TO 255.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
AUTHENTICATION (USING SHA-1 AND DSA)/NO ENCRYPTION	0	DIGITAL SIGNATURE ALGORITHM (DSA), SECURE HASH ALGORITHM (SHA).
UNDEFINED	1 THROUGH 15	
----- FOR DUIS 002-006-----		
AS REQUIRED		SIZE DEFINED BY THE ASSOCIATED LENGTH FIELD.
----- FOR DUI 007 -----		
SIGNED ACKNOWLEDGMENT RESPONSE NOT REQUIRED	0	
SIGNED ACKNOWLEDGMENT RESPONSE REQUIRED	1	
----- FOR DUI 008 -----		
----- THE 2040 BITS OF THIS DUI ARE DIVIDED INTO 255 8-BIT OCTETS. -----		

DFI	NAME	DEFINITION
6009	SECURITY PARAMETER LENGTH INDICATORS	INDICATES THE LENGTH OF THE CURRENT INSTANCE OF THE CORRESPONDING BINARY FIELD.

DUI	NAME	EXPLANATION
001	KEYING MATERIAL ID LENGTH [3 BIT]	DEFINES THE SIZE IN OCTETS OF THE KEYING MATERIAL ID FIELD.
002	CRYPTOGRAPHIC INITIALIZATION LENGTH [4 BIT]	DEFINES THE SIZE IN 64-BIT BLOCKS OF THE KEYING MATERIAL ID FIELD.
003	KEY TOKEN LENGTH [8 BIT]	DEFINES THE SIZE IN 64-BIT BLOCKS OF THE KEY TOKEN FIELD.
004	AUTHENTICATION DATA (A) LENGTH [7 BIT]	DEFINES THE SIZE IN 64-BIT BLOCKS OF THE AUTHENTICATION DATA (A) FIELD.
005	AUTHENTICATION DATA (B) LENGTH [7 BIT]	DEFINES THE SIZE IN 64-BIT BLOCKS OF THE AUTHENTICATION DATA (B) FIELD.
006	USER DATA MESSAGE SECURITY PADDING LENGTH [8 BIT]	DEFINES THE SIZE IN OCTETS OF THE USER DATA MESSAGE SECURITY PADDING FIELD.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
1 THROUGH 8 OCTETS	0 THROUGH 7	IN 1 OCTET INCREMENTS.
----- FOR DUI 002 -----		
1 THROUGH 16 64-BIT BLOCKS	0 THROUGH 15	IN 1 64-BIT BLOCK INCREMENTS.
----- FOR DUI 003 -----		
1 THROUGH 256 64-BIT BLOCKS	0 THROUGH 255	IN 1 64-BIT BLOCK INCREMENTS.

DFI	NAME	DEFINITION
6009	SECURITY PARAMETER LENGTH INDICATORS	INDICATES THE LENGTH OF THE CURRENT INSTANCE OF THE CORRESPONDING BINARY FIELD.

DATA ITEM (CONTINUED)	BIT CODE	EXPLANATION
----- FOR DUI 004 AND 005 -----		
1 THROUGH 128 64-BIT BLOCKS	0 THROUGH 127	IN 1 64-BIT BLOCK INCREMENTS.
----- FOR DUI 006 -----		
NUMERIC	0 THROUGH 255	IN 1 OCTET INCREMENTS.

DFI	NAME	DEFINITION
6010	ACTIVITY IDENTIFICATION	A SHORT SERIES OF ALPHABETIC OR NUMERIC CHARACTERS ASSIGNED TO UNIQUELY IDENTIFY THE ACTIVITY WHICH WILL FUNCTION AS A LINKAGE TO THE OFFICIAL NOMENCLATURE THAT ACTUALLY IDENTIFIES THE REFERENCED ACTIVITY.

DUI	NAME	EXPLANATION
013	UNIT NAME [448 BIT]	A LITERAL NAME FOR THE UNIT.

REGEX: [-A-Za-z0-9!"#$%&'*+;<=>@\[\\\]^_`{|}~(),./:?{1,64}

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 013 -----		
THE 448 BITS OF THIS DUI ARE DIVIDED INTO 64 GROUPS OF 7 BITS EACH REPRESENTING ASCII CHARACTER CODING.		
ILLEGAL	0 THROUGH 31	
BLANK CHARACTER	32	ASCII SPACE
EXTENDED SPECIAL CHARACTERS	33 THROUGH 39	ASCII ! " # $ % &
EXTENDED SPECIAL CHARACTERS	40 THROUGH 41	ASCII ( )
EXTENDED SPECIAL CHARACTERS	42 THROUGH 43	ASCII * +
SPECIAL CHARACTER	44 THROUGH 47	ASCII , - .
NUMERIC CHARACTERS	48 THROUGH 57	ASCII 0 TO 9
SPECIAL CHARACTER	58	ASCII :
EXTENDED SPECIAL CHARACTER	59 THROUGH 62	ASCII ; < = >
SPECIAL CHARACTER	63	ASCII ?
EXTENDED SPECIAL CHARACTER	64	ASCII @
UPPERCASE ALPHABETIC CHARACTER	65 THROUGH 90	ASCII A TO Z
EXTENDED SPECIAL CHARACTER	91 THROUGH 96	ASCII [/] ^ _ `
LOWERCASE ALPHABETIC CHARACTER	97 THROUGH 122	ASCII a to z
EXTENDED SPECIAL CHARACTER	123 THROUGH 126	ASCII { | } ~
END OF LITERAL FIELD MARKER	127	ASCII DELETE USED TO SIGNIFY TRUNCATION OF THE FIELD.

DFI	NAME	DEFINITION
6011	VARIABLE LENGTH NUMERIC	A NUMERIC FIELD OF VARYING LENGTH.

DUI	NAME	EXPLANATION
001	HEADER ZERO PADDING [7 BIT]	THIS FIELD IS USED WHEN AN APPLICATION HEADER IS LESS THAN A MULTIPLE OF 8 BITS WHEN CREATED, THE FIELD IS ZERO-FILLED BY THE HOST SYSTEM UNTIL THE HEADER BECOMES A MULTIPLE OF 8 BITS. THIS PADDING ALLOWS THE USER DATA PORTION OF THE ALPDU TO START ON AN OCTET BOUNDARY.

DATA ITEM	BIT CODE	EXPLANATION
----- FOR DUI 001 -----		
----- THIS IS A VARIABLE LENGTH FIELD OF 1 TO 7 BITS WHERE THE ONLY ----- ALLOWABLE VALUE IN ANY OF ITS BINARY REGISTRIES IS "0"(ZERO). THE ----- HOST SYSTEM TRUNCATES THE FIELD TO ENSURE THE HEADER ENDS ON AN ----- OCTET BOUNDARY. -----		

CONCLUDING MATERIAL

Custodians:
Army: CR2
Navy: OM
Air Force: 93
DISA: DC1

Preparing Activity:
Army: CR2

Project Number:
DCPS-2019-001

Review Activities:
OT: SE, MP, DI, NS
Army: AC, AV, CR, MI, PT
Navy: CG, CH, EC, MC, ND
Air Force: 11, 13, 33, 99

NOTE:
The activities listed above were interested in this document as of the date of this document. Since organizations and responsibilities can change, you should verify the currency of the information above using the ASSIST Online database at https://assist.dla.mil.