Wayne McCoy

June 1987

MILITARY SUPPLEMENT

TO THE

ISO TRANSPORT PROTOCOL

Status of this Memo

This RFC is being distributed to members of the Internet community in order to solicit comments on the Draft Military Supplement. While this document may not be directly relevant to the research problems of the Internet, it may be of some interest to a number of researchers and implementors. Distribution of this memor is unlimited.

1. SCOPE

1.1 Purpose.

This document supplements the Transport Service and Protocol of the International Standards Organization (ISO), IS 8072 and IS 8073, respectively, and their formal descriptions by providing conventions, option selections and parameter values to be used when the protocol is operated within the scope of the applicability statement in Paragraph 1.3 below. Paragraph 1.4, below, describes the ISO standards. Full implementation detail is not provided in this document, but reference is made to a separate document, entitled "Implementation Guide for the ISO Transport Protocol", in which guidance for implementation is given.

1.2 Organization.

Five sections comprise this supplement. In Section 1, the role and purpose of the Transport Protocol are stated and the international standards upon which the protocol is based are described. These documents, as well as others supporting the international standards and this supplement are listed in Section 2. Other definitions not already included in the international standards and supporting documents are given in Section 3. The international standards cover a very wide variety of network environments and situations. There is, thus, a collection of options and parameters provided by the standards which must be determined for specific uses. Section 4 states the options and parameters relevant to those implementations to which this supplement applies, and defines usage conventions.

Conventions for addressing and Transport connection reference number usage and recovery of the Transport connection from peer deactivation are covered in Section 5.

1.3 Application.

The use of the Transport Protocol Class 4 and the Protocol for Providing the Connectionless-Mode Network Service (IS 8473) is mandatory foruse in all DOD packet-switched data networks where there is a potential for host-to-host connectivity across network or subnetwork boundaries. The term "network" as used here shall include Local Area Networks but not integrated weapons systems. The use of the Transport Protocol Class 4 and IS 8473 is strongly encouraged, particularly where a need for equipment interchangeability or survivability is perceived. Use of the Transport Protocol Class 4 and IS 8473 in weapons systems, where such usage does not diminish required performance, is also encouraged.

1.4 International Standards Organization Transport Protocol.

The international standard upon which this supplement is based is described in four documents:

a. IS 8072, the Transport Service Definition, which defines the service that Transport provides to a user, described in English text;

b. WG4 N53, the Formal Description of the Transport Service, in which the Transport Service is described using a formal description language;

c. IS 8073, the Transport Protocol, in which the protocol is specified in English text; and

d. N123, the formal description of the Transport Protocol, in which the specification IS 8073 is written in a formal description language.

The ISO protocol has five classes of service, named Class 0 through Class 4. Only Classes 4 and 2 will apply to this supplement. The formal description language, Estelle, DP 9074, provides for protocol descriptions in terms of communicating finite state automata. It contains a subset language which corresponds to the international standard Pascal. The Class 4 protocol operation when supported by a connectionless network service is described in an addendum to IS 8073, N3339(rev).

2. REFERENCED DOCUMENTS

2.1 Issues of Documents.

The following documents of the issue in effect on date of invitation for bids or request for proposal form a part of this supplement to the extent specified herein.

FED-STD-1037 - Federal Standard - 1037,
Glossary of Telecommunication Terms.

Implementation Guide for the ISO Transport Protocol

2.2 Other Publications.

The following documents form part of this standard to the extent specified herin. Unless otherwise indicated, the issue in effect on the date of invitation for bids or request for proposal shall apply.

IS 8072 - Information Processing Systems -
Open Systems Interconnection - Transport Service Definition. Available from: ANSI ISO TC97/SC6 Secretariat 1430 Broadway New York, NY 10018 (212) 354-3343

IS 8073 - Information Processing Systems -
Open Systems Interconnection - Transport Protocol Specification. Available from ANSI (SC6 Secretariat).

N3339(rev) - Draft Proposed Addendum to IS 8073
to Enable Class 4 Operation Over Connectionless Mode Network Service as Defined in ISO/ISO 8348/AD1. Available from ANSI (SC6 Secretariat).

DP 9074 - Estelle - A Formal Description
Technique Based on an Extended State Transition Model. Available from ANSI (SC21 Secretariat), address as for SC6, above.

WG4 N53 - Information Processing Systems -
Open Systems Interconnection - Formal Description of IS 8072 in Estelle. (Working draft, ISO TC 97/SC 6/WG 4)

N123 - Information Processing Systems -
Open Systems Interconnection - Formal Description of IS 8073 in Estelle. (Working draft, ISO TC 97/SC 6)

IS 8473 - Information Processing Systems -
Data Communications - Protocol for Providing the Connectionless-mode Network Service. Available from ANSI (SC6 Secretariat).

3. DEFINITIONS

3.1 Definition of terms.

The definition of terms used in this standard shall comply with FED-STD-1037, ISO IS 8072, IS 8073 and IS 8473. Other terms and definitions unique to N3756, WG4 N53 and N3339(rev) appear in those documents.

3.2 Abbreviations and acronyms.

The following abbreviations and acronyms are used in this supplement:

a. ISO. The International Standards Organization;

b. OSI. Open Systems Interconnection;

c. TS. Transport service;

d. TSAP. Transport service access point;

e. NSAP. Network service access point;

f. TPDU. Transport protocol data unit;

g. CR. Connect request;

h. CC. Connect confirm;

i. DR. Disconnect request;

j. ER. Error;

k. AK. Acknowledgement;

l. IP. Internetwork protocol;

m. LAN. Local area network.

n. CONS. Connection oriented network service.

o. CLNS. Connectionless network service.

(Other provisions of this Section are under consideration.)

4. GENERAL REQUIREMENTS

4.1 Conformance.

Implementations to which this supplement applies shall satisfy the conformance requirements (Clause 14, of IS 8073 and N3339(rev), as adapted for this supplement) in the following statements.

a. A system claiming to implement the procedures specified in this standard shall comply with the requirements in b. - d., below.

b. The system shall implement:

b.1 Class 2 or Class 0 or both, if operated over a connection oriented network service; or

b.2 Class 4 if operated over a connectionless network service.

c. If the system implements Class 4, it shall also implement Class 2, if it is operated over a connection oriented network service. Class 2 shall not be implemented if operation is exclusively over a connectionless network service.

d. For each class which the system claims to implement, the system shall be capable of:

d.1 initiating CR TPDUs or responding to CR TPDUs with TPDUs or both;

d.2 responding to any other TPDU and operating network service in accordance with procedures for the class;

d.3 operating all the procedures for the class listed as mandatory in the Provisions of Options table below;

d.4 operating those procedures for the class, listed as as optional in the Provisions of Options table, for which conformance is claimed; and

d.5 handling all TPDUs of lengths up to the lesser value of:

d.5.1 the maximum length for the class;

d.5.2 the maximum for which conformance is claimed.

e. Claims of conformance shall state:

e.1 whether or not operation over connectionless service is implemented;

e.2 which class or classes of protocol are implemented, if

operation over a connection oriented network is implemented;

e.3 whether the system is capable of initiating or responding to CR TPDUs or both;

e.4 which of the procedures listed in the Provisions of Options table are implemented;

e.5 the maximum size of TPDU implemented; the value shall be chosen from the following list and all values in the list which are less than this maximum shall be implemented:

128, 256, 512, 1024, 2048, 4096, or 8192 octets.

Provision of options (adapted from IS 8073, Table 9)

PROCEDURE	CLASS 2	CLASS 4
TPDU with checksum	not applicable	mandatory
TPDU without checksum	mandatory	optional
Expedited data transfer	mandatory	mandatory
No expedited data transfer	mandatory	mandatory
Flow control in Class 2	mandatory	not applicable
No flow control in Class 2	optional	not applicable
Normal formats	mandatory	mandatory
Extended formats	optional	optional

The explicit manner in which implementations, to which this supplement applies, shall satisfy these conformance statements is given in Paragraph 4.4. The options are described in more detail in Paragraph 4.3.

4.2 Transport Service access parameters.

Each of the services of transport has parameters that identify communicating peers, express options for operation of the transport connection, or transmit data from one peer user to the other. The conventions for these parameters for usage in implementations to which this supplement applies are given below.

4.2.1 Connect Service.

The Connect Service is summarized below (refer to IS 8072 for detailed discussion):

Primitives		Parameters
T-CONNECT	request indication	Called Address, Calling Address, Expedited Data Option, Quality of Service, TS User-Data
T-CONNECT	response confirm	Responding Address, Quality of Service, Expedited Data Option, TS User-Data

Conventions for Called Address, Calling Address and Responding Address will appear in Paragraph 5.1.1. Use of the Expedited Data Option is dependent on the nature of the transport user; this supplement does not define how transport users will decide on such usage. The parameters that define Quality of Service are discussed in IS 8072. However, the manner in which these parameters are to be applied in an implementation issue , and the mechanisms to be used to maintain the requested quality of sevice are not defined. It is thus recommended that these parameters not be used in implementations until such time that usage definition exists. The amount of data passed in TS User-Data is constrained to 32 octets or less. (This TS User-Data parameter shall not be used for any data that requires any security protection whatever.) No implementation is required to be able to send such data received from its user, but each implementation shall be capable of passing data received from the remote peer user during connection establishment to its user.

4.2.2 Disconnect Service.

Primitives		Parameters
T-DISCONNECT	request	TS User-Data
T-DISCONNECT	indication	TS User-Data, Disconnect reason

The Disconnect Service is abrupt in the sense that data may be lost

whenever the service is invoked. Transport user processes should therefore ensure that all data intended to be received has in fact been received before issuing a T-DISCONNECT-request. The data used in the TS User-Data parameter is constrained to be 64 octets or less in length. (The TS User-Data parameter shall not be used for data that requires any security protection whatever.) Disconnect reasons are discussed in IS 8073, and reasons other than those listed in IS 8073 are permitted.

4.2.3 Data Transfer Service.

Primitives		Parameters
T-DATA	request	TS User-Data
	indication	

The length of the data that is carried by the TS User-Data parameter is not constrained by the ISO Standard, but interface considerations may impose practical limits. This is discussed further in the Implementors guide, Part 3.1. For the purposes of this supplement, the TS User-Data parameter in this service is considered to be protected and should be used for any data requiring security protection.

4.2.4 Expedited Data Service.

Primitives		Parameters
T-EXPEDITED-DATA	request	TS User-Data
	indication	

The TS User-Data parameter is constrained to be no longer than 16 octets and shall not be used for data requiring any security protection whatever. The T-EXPEDITED-DATA-request cannot be used whenever non-use of expedited data was called for in either the T-CONNECT-request or T-CONNECT-response primitive.

4.3 Options.

The protocol described in IS 8073 and N3756 permits certain options which qualify or enhance the service to be provided. Negotiated options are those which both communicating peer transport entities agree upon during connection establishment. Local options are those which apply to a particular implementation of transport that may be used to enhance performance, optimize resource utilization or improve resilience to network failures. The election of a local option is invisible to the remote peer entity.

4.3.1 Negotiated options.

The options in IS 8073 that shall be negotiated between peer transport entities are given in the following list. The elections of these options to be taken in an implementation to which this supplement applies are defined in Paragraph 4.4.

a. a. Class of service--agreement as to one of five classes of transport service, depending on which classes are supported by the entities, the quality of the network service available and the degree of resilience to network errors and failure required by the peer transport users.

b. b. Use of extended formats--agreement to use or not use extended formats for sequence numbering and flow control credit; normal formats provide sequence numbers in the range 0 - (2**7 - 1) and flow control credit in the range 0 - (2**15 - 1); extended formats provided sequence numbers in the range 0 - (2**31 - 1) and credit in the range 0 - (2**16 - 1).

c. Use of expedited data transfer--agreement to use or not to use expedited data transfer during normal data transfer procedures.

d. Maximum size of protocol data units to be exchanged--agreement to limit size of exchanged protocol data units, depending on buffer resources that the entities have and network quality of service; values negotiated are in the range 2**7 - 2**13 octets (total length).

e. Use of checksum--agreement to use or not to use a 16-bit checksum on each protocol data unit exchange between the entities, depending on expected residual error rate in the network service used.

f. Protection parameters--agreement as to how protection will be defined and maintained on the transport connection; these parameters are defined by the communicants which elect to use them.

g. Use of flow control in Class 2--agreement to use or not to use flow control in Class 2 when Class 2 operation has been negotiated. Conformance to the ISO Standard requires that if Class 4 is supported over CONS, then Class 2 shall also be supported.

h. Service quality parameters--agreement as to the quality of service to be expected on the transport connection; the ISO Standard does not state how these parameters are to be used by the transport entities or their users.

4.3.2 Local options, Class 2.

The options that an implementor may decide in a particular Class 2 implementation are given in the following list. Recommendations and requirements for these options for the purposes of this this supplement are given in Paragraph 4.5.1.

a. Multiplexing on network connection--for better usage of of network resources, an implementation may elect to share a network connection among two or more transport connections.

b. Acknowledgement strategy--an implementation is not required by IS 8073 to use any particular strategy for sending acknowledgements for received data: each data transfer protocol data unit may be explicitly acknowledged (one-for-one) or may be implicitly acknowledged by a group acknowledgement (one-for-N).

c. Concatenation of protocol data units--when network service data units are large compared to the protocol data units to be sent, an implementation may elect to concatenate these protocol data units into a single network service data unit.

d. Lockup prevention timer--when the wait-before-closing state is entered, there is a possibility of deadlock if the peer transport entity never responds to the CR TPDU. The standard provides for an optional timer to alleviate this situation.

4.3.3 Local options, Class 4.

The options that an implementor may decide in a particular Class 4 implementation are given in the list below. Recommendations and requirements for use of these options in implementations to which this supplement applies are given in Paragraph 4.5.2.

a. Withdrawal of flow control credit--when supporting several connections of differing precedence or priority, resource management must be practiced so as to maintain the precedence or priority relationships.

b. Flow control confirmation--when flow control credit is reduced, extra delay may be encountered because acknowledgements carrying new flow control information are lost; this procedure aids in speeding up resynchronization of the flow control.

c. Subsequenced acknowledgements--when the flow control window has been closed this procedure alleviates ambiguity due to lost or out-of-order acknowledgements.

d. Splitting over network connection--when operating over a connection-oriented network service, a Class 4 implementation is permitted to use more than one network connection, for better performance and better resilience to network connection failure.

e. Acknowledgement strategy--an implementation is not required by the standard to use any particular strategy for sending acknowledgements for received data: each data transfer protocol data unit may be explicitly acknowledged (one-for-one) or may be implicitly acknowledged by a group acknowledgement (one-for-N).

f. Wait-before-closing state--when a connect request has been sent to the peer and the user has requested a disconnection before the connect confirmation has been received, an implementation may elect to wait until the confirmation has arrived before sending the disconnection request to the peer, to ensure positive identification of the connection to be released.

g. Multiplexing on network connection--for better usage of network resources, an implementation may elect to share a network connection among two or more transport connections.

h. Concatenation of protocol data units--when network service data units are large compared to the protocol data units to be sent, an implementation may elect to concatenate these protocol data units into a single network service data unit.

i. Checksum algorithm--the Fletcher checksum algorithm provided in an annex to the standard is not part of the standard and is provided for information only. The checksum algorithm used nature of network errors expected and need only satisfy the summation criterion given in the standard.

j. Send network RESET when bad checksum received--it may not be possible to know with certainty which of several transport connections multiplexed on a network connection is to receive a protocol data unit which carries a bad checksum. A N-RESET or N-DISCONNECT may be sent on the network connection to all transport entities on the connection to indicate the error.

k. Protocol data unit retransmission policy--protocol data units for which no acknowledgement has been received may be retransmitted in case the originals were never received. Whether to retransmit only the oldest unacknowledged protocol data unit or all those that are outstanding has implications for buffer management in the sending entity and for utilization of the bandwidth in the network transmission

medium.

4.4 Negotiations.

Paragraph 4.2.1 lists those options that shall be negotiatied by communicating transport entities. Below, conventions are given for these options, in usage to which this supplement applies. These requirements reflect the conformance statement of IS 8073 and the needs of the DOD.

4.4.1 Options.

4.4.1.1 Class of service.

a. An implementation operating on CONS shall be capable of offering Class 2 and may optionally support Class 0.

b. An implementation shall not respond by a proposal of Class 0 and shall not respond by a proposal of Class 2 if the connect request was received on a CLNS.

c. An implementation may offer Class 2 as an alternative class of operation in a connect request when operating over CONS. No alternative class may be offered if operation over a CLNS.

d. An implementation shall respond to a connect request that proposes Class 1 or 3 as primary choice with a disconnect request, reason code 128+2 (see p. 87 of IS 8073).

e. An implementation shall not propose Class 1 or Class 3 in response to a connect request carrying Class 1 or Class 3 as an alternative class of service.

f. An implementation which proposes Class 4 in a connect request need not accept a proposal for Class 2 from its peer if Class 2 was not offered as an alternative in the connect request, or if operation is over a CLNS. Class 2 shall be accepted when proposed by the responding peer if it was offered as an alternative in the connect request.

4.4.1.2 Extended formats.

a. An implementation shall always propose use of extended formats when either Class 4 or Class 2 is proposed in a connect request.

b. An implementation shall always accept the use of extended formats when so proposed in a received connect request.

4.4.1.3 Expedited data.

a. Use of expedited data is subject to negotiation by users of Transport Service.

b. Expedited data shall be supported in Class 2.

4.4.1.4 Maximum protocol data unit size.

(The provisions of this paragraph are under consideration.)

4.4.1.5 Use of checksum.

An implementation shall propose use of checksums consistent with the expected quality of service and security requirements.

a. Checksums should be used when operating with the IP on catenated networks.

b. Checksums should not be used if high performance is required, except when required by high error rates in the network service.

c. Checksums should always be used when any encryption is being used.

4.4.1.6 Protection parameters.

Use of the security parameters is not defined in this supplement.

4.4.1.7 Use of flow control in Class 2.

a. An implementation shall always propose the use of flow control in Class 2 whenever Class 2 is proposed as either primary or alternative choice of service.

b. An implementation shall accept use of flow control in Class 2 whenever negotiation to Class 2 occurs.

4.4.1.8 Service quality parameters.

a. Use of the service quality parameters in the CR and CC protocol data units is not defined except for the residual error rate parameter and the priority parameter.

b. Residual error rate (the use of this parameter is under consideration).

c. Priority (the use of this parameter is under consideration).

4.4.2 Parameters.

This paragraph defines the values to be used in the CR and CC TPDUs.

4.4.2.1 Class 2 parameters.

4.4.2.1.1 Connect request (CR) protocol data unit.

4.4.2.1.1.1 Fixed part of header.

a. Connect request code: as in IS 8073.

b. Initial credit allocation: this field defines the number of TPDUs offered as initial credit by the connection initiator. Since the field is of length 4, the maximum credit that can be initially offered is limited to 15. These TPDUs are constrained in length to the maximum size defined in the TPDU size field, listed below in Paragraph 4.4.2.1.1.2.

c. Destination reference: as in IS 8073.

d. Source reference: this reference shall be selected pursuant to the provisions of Paragraph 5.2.1.

e. Class and option: the class field shall take binary value 0010; the option field shall take binary value 0010. (These values select Class 2, and the options of extended formats and flow control in Class 2.)

4.4.2.1.1.2 Variable part of header.

a. TSAP identifiers: the parameter values shall follow the conventions given in Paragraphs 5.1.1 and 5.1.2.

b. TPDU size: (The values to be used are under consideration.)

c. Version number: as in IS 8073.

d. Protection parameters: should not be used.

e. Checksum: shall not be used.

f. Additional options: this field shall take binary value 0001 if the initiating user has proposed the use of expedited data, and shall take value 0000 otherwise.

g. Alternative protocol classes: this field shall not be used unless Class 0 is to be proposed as an alternate class of operation.

h. Throughput: should not be used.

i. Residual error rate: should not be used.

j. Priority: (Use of this parameter is under consideration.)

k. Transit delay: should not be used.

4.4.2.1.1.3 User data.

The CR TPDU shall not carry user data which has any requirement whatever for security protection.

4.4.2.1.2 Connect Confirm (CC) TPDU.

4.4.2.1.2.1 Fixed part of header.

a. Connect confirm code: as in IS 8073.

b. Initial credit allocation: same as Paragraph 4.4.2.1.1.1.

c. Destination reference: this reference shall be the "Source reference" number from the received CR TPDU.

d. Source reference: this reference shall be selected pursuant to the provisions of Paragraph 5.2.1.

e. Class and option: the class field shall take binary value 0010 and the option field shall take binary value 0010 (selects Class 2 and options of extended formats and flow control in Class 2).

4.4.2.1.2.2 Variable part of header.

a. TSAP identifier(s): the parameter values shall follow the conventions given in Paragraphs 5.1.1 and 5.1.2.

b. b. TPDU size: (The values for this parameter are under consideration.)

c. Version number: as in IS 8073.

d. Protection parameters: should not be used.

e. Checksum : shall not be used.

f. Additional options: This field shall take binary value 0001 if the responding transport entity has proposed the use of expedited data, and shall take binary value 0000 otherwise.

g. Alternative protocol classes: shall not be used.

h. Throughput: should not be used.

i. Residual error rate: should not be used.

j. Priority: (The use of this parameter is under consideration.)

k. Transit delay: should not be used.

4.4.2.1.2.3 User data.

The CC TPDU shall not carry any data which has any requirement whatever for security protection.

4.4.2.2 Class 4 parameters.

4.4.2.2.1 Connect request (CR) TPDU.

4.4.2.2.1.1 Fixed part of header.

a. Connect request code: as in IS 8073.

b. Initial credit allocation: this field defines the number of TPDUs offered as initial credit by the connection initiator. Since the field is of length 4, the maximum credit that can be initially offered is limited to 15. These TPDUs are constrained in length to the maximum size defined in the TPDU size field, listed below in Paragraph 4.4.2.2.1.2.

c. Destination reference: as in IS 8073.

d. Source reference: this reference shall be selected pursuant to the provisions of Paragaph 5.2.1.

e. Class and option: the class field shall take binary value 0100; the option field shall take binary value 0010. (These values select Class 4, and the options of extended formats and flow control in Class 2. This latter option is ignored if the class negotiated is Class 2.)

4.4.2.2.1.2 Variable part of header.

a. TSAP identifiers: the parameter values shall follow the conventions given in Paragraphs 5.1.1 and 5.1.2.

b. PDU size: (The values for this parameter are under consideration.)

c. Version number: as in IS 8073.

d. Protection parameters: should not be used.

e. Checksum: if Class 4 has been selected, this parameter may be used. If Class 2 (or Class) has been selected, this parameter shall not be used.

f. Additional options: this field shall take binary value 0001 if the initiating user has proposed the use of expedited data, and shall take binary value 0000 otherwise.

g. Alternative protocol classes: this field shall be used only if Class 2 (or Class 0) is to be proposed as an alternate class of operation, conformant to the conditions of Paragraph 4.4.1.1. If Class 2 is proposed, the field shall take binary value 00000010 (1 octet).

h. Acknowledge time: should not be used.

i. Throughput: should not be used.

j. Residual error rate: (The use of this parameter is under consideration.)

k. Priority: (The use of this parameter is under consideration.)

l. Transit delay: should not be used.

4.4.2.2.1.3 User data.

The CR TPDU shall not carry user data which has any requirement whatever for security protection.

4.4.2.2.2 Connect confirm (CC) TPDU.

4.4.2.2.2.1 Fixed part of header.

a. Connect confirm code: as in IS 8073.

b. Initial credit allocation: same as Paragraph 4.4.2.2.1.1.b.

c. Destination reference: this reference shall be the number in "Source reference" from the received CR TPDU.

d. Source reference: this reference shall be selected pursuant to the provisions of Paragraph 5.2.1.

e. Class and option: if Class 2 has been selected, then the class field shall take binary value 0010 and the option field shall take binary value 0010. If Class 4 has been selected, then the class field shall take binary value 0100 and the option field shall take binary value 0010.

4.4.2.2.1.2 Variable part of header.

a. TSAP identifier(s): the parameters values shall follow the conventions given in Paragraphs 5.1.1 and 5.1.2.

b. TPDU size: (The values for this parameter are under consideration.)

c. Version number: as in IS 8073.

d. Protection parameters: should not be used.

e. Checksum: if Class 4 has been selected, this parameter may be used. If Class 2 (or Class 0) has been selected, this parameter shall not be used.

f. Additional options: if Class 4 or Class 2 has been selected, this field shall take binary value 0001 if the responding user has proposed use of expedited data and shall take binary value 0000 otherwise.

g. Alternate protocol classes: shall not be used.

h. Acknowledgement time: should not be used.

i. Throughput: should not be used.

j. Residual error rate: (The use of this parameter is under consideration.)

k. Priority: (The use of this parameter is under consideration.)

l. Transit delay: should not be used.

4.4.2.2.1.3 User data.

The CC TPDU shall not carry user data which has any requirement whatever for security protection.

4.5 Use of local options.

The paragraphs that follow give policy and guidance in the election of local options.

4.5.1 Local options, Class 2.

4.5.1.1 Multiplexing.

Any Class 2 connections may be multiplexed on the same network connection to the limits provided by the network service. Multiplexing Class 2 and Class 4 connections together on the same network connection is not recommended.

4.5.1.2 Acknowledgement strategy.

(The provisions of this paragraph are under consideration.)

4.5.1.3 Concatenation.

This permits placing certain TPDUs into a single network service data unit with a data-bearing TPDU. It is useful for reducing the overhead of separate transmission of the individual TPDUs.

4.5.1.4 Lockup prevention timer.

It is strongly recommended that this timer be used for all Class 2 connections. A description of the timer has been included in the transport formal description. (This timer corresponds to the optional TS1 timer that IS 8073 recommends.)

4.5.1.5 Treatment of protocol errors.

Protocol errors detected by a Class 2 transport connection shall result in that connection being terminated, without sending an ER TPDU.

4.5.1.6 Action on receipt of Error transport protocol data unit.

The receipt of an ER TPDU for a Class 2 transport connection shall cause immediate termination of that transport connection.

4.5.2 Local options, Class 4.

4.5.2.1 Withdrawal of flow control credit.

Because of the need to serve transport connections of various levels of operating priority, an implementation shall support the withdrawal of flow control credit from any Class 4 transport connection as a means of managing resource allocation among Class 4 connections.

4.5.2.2 Flow control confirmation.

The requirement to support withdrawal of flow control credit strongly indicates the need to use flow control confirmation. An implementation should support and use the flow control confirmation procedures of IS 8073, consistent with quality of service and other requirements.

4.5.2.3 Subsequenced acknowledgements.

The possibility of credit withdrawal strongly indicates the requirement for subsequence numbers on acknowledgements. An implementation shall support and use subsequence numbers as defined in IS 8073.

4.5.2.4 Splitting over network connection.

Implementations may use splitting as necessary or useful in the operating environment. (Splitting is defined only for operation over a CONS.

4.5.2.5 Acknowledgement strategy.

(The provisions of this paragraph are under consideration.)

4.5.2.6 Wait-before-closing state.

It is recommended that this state be used. A lockup prevention timer, such as used in Class 2, is not necessary, since the CR TPDU retransmission timer serves this purpose.

4.5.2.7 Multiplexing on network connection.

Multiplexing of Class 4 connections on a single network connection may be used as necessary or useful, within the limits permitted by the network service. Class 4 connections should not be multiplexed onto network connections serving Class 2 transport connections.

4.5.2.8 Concatenation of protocol data units.

Concatenation may be useful when operating over a CLNS that has large capacity service data units. Concatenation on networks that areconnection-oriented may be useful if transport connections are being multiplexed. A careful analysis of the treatment of the network service data unit in internetwork environments should be done to determine whether concatenation of TPDUs provides sufficient benefit to justify its usage in those circumstances.

4.5.2.9 Checksum algorithm.

It is strongly recommended that the algorithm described in the Implementors Guide Part 7, be used rather than the algorithm given in the Annex to IS 8073. The algorithm in Part 7 computes the same checksum as the one in IS 8073 but has been optimized. Guidance on the use and non-use of checksum is given in the Implementors Guide, Part 7.

4.5.2.10 Send network RESET when bad checksum received.

It is recommended that only an N-RESET be sent when encountering a TPDU with a bad checksum on a CONS. An implementation shall not send an N-DISCONNECT-request in such situations, since the TPDU with the bad checksum may have come from some entity intending to interfere with communications. When operating Class 4 over a CLNS, no action shall be taken on the receipt of a TPDU with a bad checksum, i.e., the TPDU shall be discarded.

4.5.2.11 Protocol data unit retransmission policy.

(The provisions of this paragraph are under consideration.)

4.5.2.12 Treatment of protocol errors.

In Class 4, a protocol error arising from a TPDU containing unrecognized parameters shall cause a DR TPDU to be sent to the sender, if the TPDU is otherwise valid. All other erroneous TPDUs shall be discarded.

4.5.2.13 Action on receipt of Error transport protocol data unit.

If an ER TPDU is received from a remote transport entity, an implementation to which this supplement applies shall release the transport connection with which the ER TPDU is associated, if such association can be made. When association cannot be made, the ER TPDU shall be discarded.

5. SPECIAL REQUIREMENTS

5.1 Addressing conventions.

(The provisions of Paragraph 5.1 and its subparagraphs are under consideration.)

5.1.1 Transport Service Access Point.

5.1.2 Connect-request/confirm protocol data units.

5.1.3 Network Service Access Point.

5.2 Convention for use of transport connection reference numbers.

The ISO Transport Protocol provides for freezing reference numbers by means of a timer, so that re-use of a reference number does not cause ambiguity in communications. However, certain requirements are imposed on DOD implementations, so that this means of reference number control is inadequate alone. The ISO standard defines only those actions to be followed if a timer is used. Other means of reference number control are not prohibited, providing that the minimum freeze time, as defined in IS 8073, is exceeded for each reference number used.

5.2.1 Specification of convention.

An implementation adhering to the applications definitions in this supplement, Paragraph 1.3, shall not re-use a transport connection reference number until the set of available reference numbers has recycled to that point. Expressed more formally, if all reference numbers are defined to be within the interval [1,N] and a reference number R in this interval is used, then R shall be prohibited from being selected again until all the numbers R+1,...,N,1,2,...,R-1 shall have been used. The choice of N should be sufficiently large that the expected recycle period exceeds the minimum freeze time as specified in IS 8073. This requirement is in addition to and does not supersede the freeze requirement of IS 8073. A simple means of implementing this convention is given in Part 9.3 of the Implementors Guide.

5.3 Operation over connectionless network service.

Implementations to which this supplement applies are required to operate over connectionless network services in addition to being able to operate over connection-oriented network services. The ISO standard specifies transport only for operation over a connection-oriented network. However, the specification for Class 4 has been written in such a way that use with connectionless network service is not precluded. The formal description offers even more flexibility in this regard. Consequently, operation over connectionless network services, whether a LAN or IP, is primarily an implementation issue for Class 4. Operation of Class 2 transportover a connectionless network service is not considered to be a reasonable option because of the lack of sufficent error recovery in Class 2. For the purposes of this supplement, operation of Class 2 on a connectionless network service is not recommended. Operation of Class 4 over a connectionless network service is discussed further in parts 1.2.2.2, 3.4, and 6 of the accompanying Implementors Guide.

5.4 Recovery from peer deactivation.

The ISO Standard does not provide for re-establishment of the transport connection when one of the communicating peers is deactivated ("crashes"). However, the state tables for Class 4 transport in Annex A to IS 8073 are flexible enough that simple adaptations in an implementation can yield some degree of crash recovery without change to the protocol. These adaptations are discussed in Part 9.2 of the Implementors Guide.