INTERNATIONAL STANDARD

ISO/IEC 8473-1

First edition
1994-07-15

Information technology — Protocol for providing the connectionless-mode network service: Protocol specification

Technologies de l'information — Protocole de fourniture de service de réseau en mode sans connexion: Spécification du protocole

Reference number
ISO/IEC 8473-1:1994(E)

CONTENTS

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 8473-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as CCITT Recommendation X.233.

ISO/IEC 8473 consists of the following parts, under the general title *Information technology — Protocol for providing the connectionless-mode network service*:

— Part 1: *Protocol specification*

Annex A forms an integral part of this part of ISO/IEC 8473. Annexes B and C are for information only.

Introduction

This is one of a set of Recommendations and International Standards produced to facilitate the interconnection of open systems. The set covers the services and protocols required to achieve such interconnection.

This Recommendation | International Standard is positioned with respect to other related Recommendations and International Standards by the layers defined in ITU-T Rec. X.200 | ISO/IEC 7498-1. In particular, it is a protocol of the Network layer. The protocol specified by this Recommendation | International Standard may be used between Network entities in end systems, between Network entities in intermediate systems, or between a Network entity in an end system and a Network entity in an intermediate system. In an end system, it provides the connectionless-mode Network service defined in CCITT Rec. X.213 | ISO/IEC 8348.

The interrelationship of the protocol specification and the related service definitions is illustrated in Figure Intro.1.

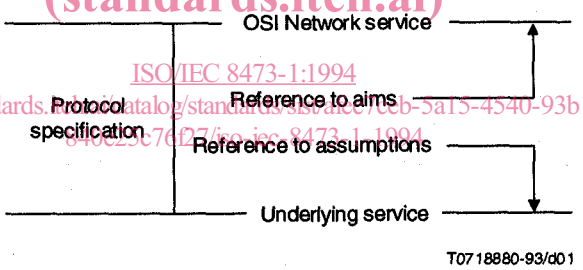

Figure Intro. 1 – Interrelationship of protocol and services

In order to evaluate the conformance of a particular implementation of this protocol, it is necessary to have a statement of which of the protocol's capabilities and options have been implemented. Such a statement is called a Protocol Implementation Conformance Statement (PICS), as defined in CCITT Rec. X.290 | ISO/IEC 9646-1. A PICS proforma, from which a PICS may be prepared for a specific implementation, is included in this Recommendation | International Standard as normative Annex A.

INTERNATIONAL STANDARD

CCITT RECOMMENDATION

INFORMATION TECHNOLOGY – PROTOCOL FOR PROVIDING THE CONNECTIONLESS-MODE NETWORK SERVICE: PROTOCOL SPECIFICATION

1 Scope

This Recommendation | International Standard specifies a protocol that is used to provide the connectionless-mode Network service described in CCITT Rec. X.213 | ISO/IEC 8348 and to perform certain Network layer management functions. The protocol relies upon the provision of an underlying connectionless-mode service by real subnetworks and/or data links. The underlying connectionless-mode service assumed by the protocol may be obtained either directly, from a connectionless-mode real subnetwork, or indirectly, through the operation of an appropriate Subnetwork Dependent Convergence Function (SNDCF) or Protocol (SNDCP) over a connection-mode real subnetwork, as described in ISO/IEC 8648. This Recommendation | International Standard specifies the operation of the protocol with respect to a uniform, abstract "underlying subnetwork service". Other Recommendations | International Standards specify the way in which this "underlying subnetwork service" is obtained from real subnetworks, such as those which conform to ISO/IEC 8802 or ISO/IEC 8208. The "underlying subnetwork service" may be obtained from real subnetworks other than those that are specifically covered by the other Recommendations | International Standards.

This Recommendation | International Standard specifies

a) procedures for the connectionless transmission of data and control information from one Network entity to a peer Network entity;

b) the encoding of the protocol data units (PDUs) used for the transmission of data and control information, comprising a variable-length protocol header format;

c) procedures for the correct interpretation of protocol control information; and

d) the functional requirements for implementations claiming conformance to this Recommendation | International Standard.

The procedures are defined in terms of

a) the interactions among peer Network entities through the exchange of protocol data units;

b) the interactions between a Network entity and a Network service user through the exchange of Network service primitives; and

c) the interactions between a Network entity and an abstract underlying service provider through the exchange of service primitives.

This Recommendation | International Standard also provides the PICS proforma for this protocol, in compliance with the relevant requirements, and in accordance with the relevant guidance, given in CCITT Rec. X.290 | ISO/IEC 9646-1.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of the currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Reference Model: Basic Reference Model.*
- ITU-T Recommendation X.210 (1993) | ISO/IEC 10731:1993, *Information technology – Open Systems Interconnection – Conventions for the definition of OSI services.*
- CCITT Recommendation X.213 (1992) | ISO/IEC 8348:1992, *Information technology – Network service definition for Open Systems Interconnection.*

2.2 Paired Recommendations | International Standards identical in technical content

- ITU-T Recommendation X.224 (1993), *Protocol for providing the OSI connection-mode Transport service.*

  ISO/IEC 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service.*
- CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – General concepts.*

  ISO/IEC 9646-1:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework: General concepts.*

2.3 Additional references

- ITU-T Recommendation X.25 (1993), *Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit.*
- ISO/IEC 8208:1990, *Information technology – Data communications – X.25 Packet Layer Protocol for Data Terminal Equipment.*
- ISO/IEC 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organization of the network layer.*
- ISO/IEC 8802:1990, *Information processing systems – Data communications – Local area networks.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Reference model definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

a) end system;
b) Network entity;
c) Network layer;
d) Network protocol;
e) Network protocol data unit;
f) Network relay;
g) Network service;
h) Network service access point;
i) Network service access point address;
j) routeing;
k) service;
l) service data unit;
m) service primitive.

3.2 Service conventions definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.210 | ISO/IEC 10731:

a) service provider;
b) service user.

3.3 Network layer architecture definitions

This Recommendation | International Standard makes use of the following terms defined in ISO/IEC 8648:

a) intermediate system;
b) relay system;
c) subnetwork;
d) subnetwork dependent convergence protocol;
e) subnetwork dependent convergence function;
f) subnetwork independent convergence protocol;
g) subnetwork independent convergence function;
h) subnetwork access protocol.

3.4 Network layer addressing definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.213 | ISO/IEC 8348:

a) Network addressing domain;
b) Network protocol address information;
c) subnetwork point of attachment.

3.5 Local area network definitions

This Recommendation | International Standard makes use of the following term defined in ISO/IEC 8802:

local area network

3.6 PICS definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.290 | ISO/IEC 9646-1:

a) PICS proforma;
b) protocol implementation conformance statement.

3.7 Additional definitions

3.7.1 derived PDU: A protocol data unit the fields of which are identical to those of an initial PDU, except that it carries only a segment of the user data from an N-UNITDATA request.

3.7.2 initial PDU: A protocol data unit carrying the whole of the user data from an N-UNITDATA request.

3.7.3 local matter: A decision made by a system concerning its behaviour in the Network layer that is not prescribed or constrained by this Recommendation | International Standard.

3.7.4 Network entity title: An identifier for a Network entity which has the same abstract syntax as an NSAP address, and which can be used to unambiguously identify a Network entity in an end or intermediate system.

3.7.5 reassembly: The act of regenerating an initial PDU from two or more derived PDUs.

3.7.6 segment: A distinct unit of data consisting of part of the user data provided in the N-UNITDATA request and delivered in the N-UNITDATA indication.

3.7.7 segmentation: The act of generating two or more derived PDUs from an initial or derived PDU. The derived PDUs together carry the entire user data of the initial or derived PDU from which they were generated.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

4.1 Data units

NSDU	Network service data unit
PDU	protocol data unit
SDU	service data unit
SNSDU	subnetwork service data unit

4.2 Protocol data units

DT PDU	data protocol data unit
ER PDU	error report protocol data unit
ERP PDU	echo reply protocol data unit
ERQ PDU	echo request protocol data unit

4.3 Protocol data unit fields

DA	destination address
DAL	destination address length
DUID	data unit identifier
E/R	error report flag
LI	length indicator
LT	lifetime
MS	more segments flag
NLPID	Network layer protocol identifier
SA	source address
SAL	source address length
SL	segment length
SO	segment offset
SP	segmentation permitted flag

4.4 Parameters

DA	destination address
QOS	quality of service
SA	source address

4.5 Miscellaneous

CLNP	connectionless-mode network protocol (i.e. the protocol defined in this Recommendation | International Standard)
NPAI	Network protocol address information
NS	Network service
NSAP	Network service access point
PICS	protocol implementation conformance statement
SN	subnetwork
SNAcP	subnetwork access protocol
SNDCF	subnetwork dependent convergence function
SNDCP	subnetwork dependent convergence protocol
SNICP	subnetwork independent convergence protocol
SNPA	subnetwork point of attachment

5 Overview of the protocol

5.1 Internal organization of the Network layer

The architectural organization of the Network layer is described in ISO/IEC 8648. ISO/IEC 8648 identifies and categorizes the way in which functions can be performed within the Network layer by Network layer protocols, thus providing a uniform framework for describing how protocols operating either individually or cooperatively in the Network layer can be used to provide the OSI Network service. This protocol is designed to be used in the context of the internetworking protocol approach to the provision of the connectionless-mode Network service defined in ISO/IEC 8648.

This protocol is intended for use in the Subnetwork Independent Convergence Protocol (SNICP) role. A protocol which fulfills the SNICP role operates to construct the OSI Network service over a defined set of underlying services, performing functions which are necessary to support the uniform appearance of the OSI connectionless-mode Network service over a homogeneous or heterogeneous set of interconnected subnetworks. This protocol is defined to accommodate variability where subnetwork dependent convergence protocols and/or subnetwork access protocols do not provide all of the functions necessary to support the connectionless-mode Network service over all or part of the path from one Network Service Access Point (NSAP) to another.

As described in ISO/IEC 8648, a protocol at the Network layer may fulfill different roles in different configurations. Although this protocol is designed particularly to be suitable for a SNICP role in the context of the internetworking protocol approach to the provision of the connectionless-mode Network service, it may also be used to fulfill other roles, and may therefore be used in the context of other approaches to subnetwork interconnection.

The operation of this protocol is specified with respect to an "underlying subnetwork service" which is made available through the operation of other Network layer protocols or through provision of the Data Link service. The "underlying subnetwork service" assumed by this protocol is described in 5.5.

5.2 Subsets of the protocol

Two subsets of the full protocol are defined, which exploit the known subnetwork characteristics of particular configurations and are therefore not subnetwork independent.

The Inactive Network Layer Protocol Subset is a null-function subset which can be used when it is known that the source and destination end systems are connected by a single subnetwork, and when none of the functions performed by the full protocol is required to provide the connectionless-mode Network service between any pair of end systems.

The Non-segmenting Protocol Subset permits simplification of the header when it is known that the source and destination end systems are connected by subnetworks whose individual service data unit sizes are greater than or equal to a known bound which is large enough so that segmentation is not required. This subset is selected by setting the segmentation permitted flag to zero (see 6.7).

5.3 Addresses and titles

The following clauses describe the addresses and titles used by this protocol.

5.3.1 Addresses

The source address and destination address parameters referred to in 7.3 are NSAP addresses. The syntax and semantics of an NSAP address are described in CCITT Rec. X.213 | ISO/IEC 8348.

The encoding used by this protocol to convey NSAP addresses is the "preferred encoding" specified in CCITT Rec. X.213 | ISO/IEC 8348. The NSAP address, encoded as a string of binary octets according to CCITT Rec. X.213 | ISO/IEC 8348, is conveyed in its entirety in the address fields described in 7.3.

5.3.2 Network entity titles

A Network Entity Title (NET) is an identifier for a Network entity in an end system or intermediate system. Network entity titles are allocated from the same name space as NSAP addresses, and the determination of whether a name is an NSAP address or a Network entity title depends on the context in which the name is interpreted. The values of the source route and record route parameters defined in 7.5.4 and 7.5.5 respectively are Network entity titles. The values of the source address and destination address parameters in the Error Report PDU defined in 7.9, in the Echo Request PDU defined in 7.10, and in the Echo Response PDU defined in 7.11 are also Network entity titles.

The encoding used by this protocol to convey Network entity titles is the "preferred encoding" specified in CCITT Rec. X.213 | ISO/IEC 8348. The Network entity title, encoded as a string of binary octets according to CCITT Rec. X.213 | ISO/IEC 8348, is conveyed in its entirety in the appropriate fields.

5.4 Service provided by the protocol

This protocol provides the connectionless-mode Network service described in CCITT Rec. X.213 | ISO/IEC 8348. The relevant Network service primitive and its parameters are shown in Table 1.

NOTE – CCITT Rec. X.213 | ISO/IEC 8348 states that the maximum size of a connectionless-mode Network service data unit (NSDU) is 64 512 octets.

Table 1 – Connectionless-mode Network service primitive

Primitive		Parameters
N-UNITDATA	Request Indication	NS-Source-Address, NS-Destination-Address, NS-Quality-of-Service, NS-Userdata

5.5 Underlying service assumed by the protocol

It is intended that this protocol be capable of operating over connectionless-mode services derived from a wide variety of real subnetworks and data links. Therefore, in order to simplify the specification of the protocol, its operation is defined (in clause 6) with respect to an abstract "underlying subnetwork service" rather than any particular real subnetwork service. This underlying service consists of a single SN-UNITDATA primitive which conveys the source and destination subnetwork point of attachment addresses, a subnetwork quality of service parameter, and a certain number of octets of user data.

The SN-UNITDATA primitive is used to describe the abstract interface that exists between the CLNP protocol machine and an underlying real subnetwork or a subnetwork dependent convergence function that operates over a real subnetwork or real data link to provide the required underlying service.

The primitive provided and its parameters are shown in Table 2.

Provision of the "underlying subnetwork service" by real subnetworks and data links is described in clause 8 and in other Recommendations | International Standards.

Table 2 – Underlying service primitive

Primitive		Parameters
SN-UNITDATA	Request Indication	SN-Source-Address, SN-Destination-Address, SN-Quality-of-Service, SN-Userdata

6 Protocol functions

This clause describes the functions performed as part of the protocol.

Not all of the functions must be performed by every implementation. Subclause 6.21 specifies which functions may be omitted, and the correct behavior when requested functions are not implemented.

6.1 PDU composition function

This function is responsible for the construction of a protocol data unit according to the rules governing the encoding of PDUs given in clause 7. The Protocol Control Information (PCI) required is determined from current state and local information and from the parameters associated with the N-UNITDATA request.

Network Protocol Address Information (NPAI) for the source address and destination address fields of the PDU header is derived from the NS-Source-Address and NS-Destination-Address parameters. The NS-Destination-Address and NS-Quality-of-Service parameters, together with current state and local information, are used to determine which optional functions are to be selected. User data passed from the Network service user (NS-Userdata) form the data part of the protocol data unit.

During the composition of the protocol data unit, a Data Unit Identifier (DUID) is assigned to distinguish this request to transmit NS-Userdata to a particular destination Network service user from other such requests. The originator of the PDU shall choose the DUID so that it remains unique (for this source and destination address pair) for the maximum lifetime of the Initial PDU in the network; this rule applies for any PDUs derived from the Initial PDU as a result of the application of the segmentation function (see 6.7). Derived PDUs are considered to correspond to the same Initial PDU, and hence to the same N-UNITDATA request, if they have the same source address, destination address, and data unit identifier.

The DUID is also available for ancillary functions such as error reporting (see 6.10).

The total length of the PDU in octets is determined by the originator and placed in the total length field of the PDU header. This field is not changed for the lifetime of the protocol data unit, and has the same value in the Initial PDU and in each of any Derived PDUs that may be created from the Initial PDU.

When the non-segmenting protocol subset is employed, neither the total length field nor the data unit identifier field is present. The rules governing the PDU composition function are modified in this case as follows. During the composition of the protocol data unit, the total length of the PDU in octets is determined by the originator and placed in the segment length field of the PDU header. This field is not changed for the lifetime of the PDU. No data unit identification is provided.

6.2 PDU decomposition function

This function is responsible for removing the protocol control information from the protocol data unit. During this process, information pertinent to the generation of the N-UNITDATA indication is determined as follows. The NS-Source-Address and NS-Destination-Address parameters of the N-UNITDATA indication are recovered from the NPAI in the source address and destination address fields of the PDU header. The data part of the received PDU is retained until all segments of the original service data unit have been received; collectively, these form the NS-Userdata parameter of the N-UNITDATA indication. Information relating to the Quality of Service (QOS) provided during the transmission of the PDU is determined from the quality of service and other information contained in the options part of the PDU header. This information constitutes the NS-Quality-of-Service parameter of the N-UNITDATA indication.

6.3 Header format analysis function

This function determines whether the full protocol or the inactive Network layer protocol is in use, and whether or not a received PDU has reached its final destination. If the Network layer protocol identifier (NLPID) field in a received PDU contains a value that identifies the protocol defined by this Recommendation | International Standard, then either the full protocol or the non-segmenting subset is in use; the header format analysis function determines whether or not the received PDU has reached its destination, using the destination address in the PDU header. If the destination address provided in the PDU identifies either a Network entity title of this Network entity or an NSAP served by this Network entity, then the PDU has reached its destination; if not, it shall be forwarded.

If the NLPID field contains a value that identifies the inactive Network layer protocol, then no further analysis of the PDU header is required. The Network entity in this case determines that either the Subnetwork Point of Attachment (SNPA) address encoded as NPAI in the supporting subnetwork protocol (see 8.1) corresponds directly to an NSAP address serviced by this Network entity, or that an error has occurred.

6.4 PDU lifetime control function

This function is used to enforce the maximum PDU lifetime. It determines whether a received PDU may be forwarded or whether its assigned lifetime has expired, in which case it shall be discarded.

The operation of the PDU lifetime control function depends upon the lifetime field in the PDU header. This field contains, at any time, the remaining lifetime of the PDU (represented in units of 500 ms). The lifetime of the Initial PDU is determined by the originating Network entity and placed in the lifetime field of the PDU. If and when the segmentation function is applied to a PDU, the value of the lifetime field of the Initial PDU is copied into all of the corresponding Derived PDUs.

The value of the lifetime field of a PDU is decremented by every Network entity that processes the PDU. When a Network entity processes a PDU, it decrements the PDU lifetime by at least one. The value of the PDU lifetime field shall be decremented by more than one if the sum of

a) the transit delay in the underlying service from which the PDU was received, and

b) the delay within the system processing the PDU

exceeds or is estimated to exceed 500 ms. In this case, the lifetime field shall be decremented by one for each additional 500 ms of actual or estimated delay. The determination of delay need not be precise, but where a precise value cannot be ascertained, the value used shall be an overestimate, not an underestimate.

If the lifetime field reaches a value of zero before the PDU is delivered to its destination, the PDU shall be discarded. The error reporting function shall be invoked as described in 6.10. This may result in the generation of an Error Report PDU.

It is a local matter whether or not the destination Network entity performs the lifetime control function.

6.5 Route PDU function

This function determines the Network entity to which a PDU should be forwarded and the underlying service that must be used to reach that Network entity, using the destination address field and either the segment length field (if present) or the total length field (if the segment length field is not present). Where segmentation is required, the route PDU function further determines over which underlying service Derived PDUs shall be sent in order to reach that Network entity. The results of the route PDU function are passed to the forward PDU function (along with the PDU itself) for further processing.

Selection of the underlying service that shall be used to reach the "next" system in the route to the destination is initially influenced by the NS-Quality-of-Service parameter of the N-UNITDATA request, which specifies the QOS requested by the sending NS user. Whether this QOS is to be provided directly by the protocol, through the selection of the quality of service maintenance parameter and other optional parameters, or through the QOS facilities offered by each of the underlying services, or both, is determined prior to invocation of the forward PDU function. Route selection by intermediate systems may subsequently be influenced by the values of the quality of service maintenance parameter (if present), and other optional parameters (if present).

6.6 Forward PDU function

This function issues an SN-UNITDATA request primitive (see 5.5), supplying the subnetwork or SNDCF identified by the route PDU function with the protocol data unit as user data to be transmitted, the address information required by that subnetwork or SNDCF to identify the "next" system within the subnetwork-specific addressing domain (this may be an intermediate system or the destination end system), and quality of service constraints (if any) to be considered in the processing of the user data.

When the PDU to be forwarded is longer than the maximum service data unit size provided by the underlying service, the segmentation function is applied (see 6.7).

6.7 Segmentation function

Segmentation is performed when the length of a protocol data unit is greater than the maximum service data unit size supported by the underlying service to be used to transmit the PDU.

Segmentation consists of composing two or more new PDUs (Derived PDUs) from the too-long Initial or Derived PDU that is to be segmented. All of the header information from the PDU to be segmented, with the exception of the segment length and checksum fields of the fixed part, and the segment offset field of the segmentation part, is duplicated in each Derived PDU, including all of the address part, the data unit identifier and total length of the segmentation part, and the options part (if present).

NOTE – The rules for forwarding and segmentation guarantee that the header length is the same for all segments (Derived PDUs) of an Initial PDU, and is the same as the header length of the Initial PDU. The size of a PDU header therefore will not change due to the operation of any protocol function.

The user data field of the PDU to be segmented is divided and apportioned among the user data fields of the Derived PDUs in such a way that the Derived PDUs satisfy the maximum-length requirements of the SN-Userdata parameter of the SN-UNITDATA request primitive used to access the selected underlying service. The user data field of each derived PDU, except for the last, shall contain a number of octets that is a non-zero multiple of 8. Thus, the value of the segment offset field in any PDU is either zero or a non-zero multiple of 8. Segmentation shall not result in the generation of a Derived PDU containing fewer than eight octets of user data.

Derived PDUs are identified as being from the same Initial PDU by means of

a) the source address field;

b) the destination address field; and

c) the data unit identifier field.

The following fields of the PDU header are used in conjunction with the segmentation function:

a) *Segment offset* – Identifies the octet at which the segment begins with respect to the start of the data part of the Initial PDU;

b) *Segment length* – Specifies the number of octets in the Derived PDU, including both header and data;

c) *More segments flag* – Set to one if this Derived PDU does not contain the final octet of the user data from the Initial PDU as its final octet of user data; and

d) *Total length* – Specifies the number of octets in the Initial PDU, including both header and data.

Derived PDUs may be further segmented without constraining the routeing of the individual Derived PDUs.

The segmentation permitted flag is set to one to indicate that segmentation is permitted. If the Initial PDU is not to be segmented at any point during its lifetime, the flag is set to zero by the source Network entity. The setting of the segmentation permitted flag may not be changed by any other Network entity for the lifetime of the Initial PDU and any Derived PDUs.

6.8 Reassembly function

The reassembly function reconstructs the Initial PDU from the Derived PDUs generated by the operation of the segmentation function on the Initial PDU (and, recursively, on subsequent Derived PDUs).

A bound on the time during which segments (Derived PDUs) of an Initial PDU may be held at a reassembly point before being discarded is provided, so that reassembly resources may be released when it is no longer expected that missing segments of the Initial PDU will arrive at the reassembly point. Upon reception of a Derived PDU, a reassembly timer shall be initiated with a value that indicates the amount of time that shall elapse before any unreceived (missing) segments of the Initial PDU are assumed to be lost. When this timer expires, all segments (Derived PDUs) of the Initial PDU held at the reassembly point shall be discarded, the resources allocated for those segments may be freed, and, if selected, an error report shall be generated (see 6.10).

While the exact relationship between reassembly lifetime and PDU lifetime is a local matter, the reassembly function shall preserve the intent of the PDU lifetime. Consequently, the reassembly function shall discard PDUs whose lifetime would otherwise have expired had they not been under the control of the reassembly function; that is, the reassembly lifetime for a given PDU shall be less than the PDU lifetime in all derived PDUs being held at the reassembly point.

NOTES

1 Methods of bounding reassembly lifetime are discussed in Annex B.

2 The segmentation and reassembly functions are intended to be used in such a way that the fewest possible segments are generated at each segmentation point and reassembly takes place at the final destination of a PDU. However, other schemes which

a) interact with the routeing algorithm to favor paths on which fewer segments are generated, or

b) generate more segments than absolutely required in order to avoid additional segmentation at some subsequent point

are not precluded. The information necessary to enable the use of one of these alternative strategies may be made available through the operation of a Network layer management function or by other means.

3 The originator of the Initial PDU determines the value of the segmentation permitted flag in the Initial PDU and all Derived PDUs (if any). An intermediate system may not change this value in the Initial PDU or any PDU derived from it, and may not therefore add or remove the segmentation part of the header.