INTERNATIONAL STANDARD

ISO/IEC 10030

Second edition
1995-04-15

Information technology — Telecommunications and information exchange between systems — End System Routeing Information Exchange Protocol for use in conjunction with ISO/IEC 8878

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Protocole d'échange d'information pour le routage d'un système d'extrémité à utiliser conjointement avec l'ISO/CEI 8878

Reference number
ISO/IEC 10030:1995(E)

Contents

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

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 10030 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.*

This second edition cancels and replaces the first edition (ISO 10030:1990), which has been technically revised. It is a consolidation of Amendments 2 and 3 as well as Technical Corrigenda 1 and 2.

Annexes A and B form an integral part of this International Standard. Annex C is for information only.

Introduction

This International Standard is one of a number of standards concerned with Network Layer Routeing Protocols. An overall framework for routeing is described in ISO/IEC TR 9575. This International Standard specifically relates to that part of the framework which deals with Single Subnetwork Routeing.

This International Standard is related to ISO/IEC 8878 which specifies the use of X.25 to provide the ISO connection-mode Network Service. This Protocol provides solutions for the following practical problems:

a) How do End Systems discover the reachability of Intermediate Systems that can route NPDUs to destinations on subnetworks other than the one(s) to which the End System is directly connected?

b) How do End Systems discover the reachability of other End Systems on the same subnetwork (when direct examination of the destination NSAP address does not provide information about the destination subnetwork address)?

c) How does a Subnetwork Address Resolution Entity discover the reachability of End Systems on the subnetwork to which it is directly connected?

d) How does an end System, which has not been pre-configured with its own Network Address, request the temporary assignment of a Network Entity Title (NET) and thus, derive the necessary Network Address(es), from a SNARE located on a common subnetwork?

e) How do Intermediate systems discover the reachability of End Systems on the same subnetwork (when direct examination of the NSAP destination address does not provide information about the destination subnetwork address)?

The Protocol assumes that:

a) Routeing to a specified subnetwork point of attachment (SNPA) address on the same subnetwork is carried out satisfactorily by the subnetwork itself.

b) The subnetwork is not, however, capable of routeing on a global basis using the NSAP address alone to achieve communication with a requested destination.

c) End Systems and Intermediate Systems using this protocol require to know at least one SNPA address that can be used to access a SNARE.

The protocol is designed to:

a) minimize the amount of a priori state information needed by End Systems before they can begin to communicate with other End Systems;

b) minimize the amount of memory needed to store routeing information in End Systems; and

c) minimize the computational complexity of End Systems routeing algorithms.

This Protocol performs similar functions to the ones specified in ISO 9542. However, the characteristics of environments operating ISO/IEC 8208 (X.25/PLP) and the actual functionality of ISO/IEC 8208 (X.25/PLP) in itself invalidate the operation of ISO 9542 as follows:

a) In general non-broadcast environments, the Configuration subset of ISO 9542 is inadequate.

b) In broadcast environments operating ISO/IEC 8208 (X.25/PLP), the Redirection subset of ISO 9542 is invalidated.

Therefore, this Protocol is developed to perform all the aforementioned functions in harmony with the operation of ISO/IEC 8208 (X.25/PLP).

This page intentionally left blank

Information technology — Telecommunications and information exchange between systems — End System Routeing Information Exchange Protocol for use in conjunction with ISO/IEC 8878

1 Scope

This International Standard defines a protocol for the exchange of routeing information between an End System and a Subnetwork Address Resolution Entity, and between an Intermediate System and a Subnetwork Address Resolution Entity.

This International Standard is applicable to:

a) End Systems which operate according to the main body of ISO/IEC 8878 to provide and support the OSI Connection-mode Network Service using ISO/IEC 8208.

b) Subnetwork Address Resolution Entities which operate ISO/IEC 8208.

NOTE — The Subnetwork Address Resolution Entity defined in this International Standard may be associated with relay functions as defined in ISO/IEC 10028 and ISO/IEC 10177.

c) Intermediate systems which operate ISO/IEC 8208.

End Systems which provide and support the OSI CONS using the fast select 1980 procedures or the alternative 1980 procedures in annex A of ISO/IEC 8878 are outside the scope of this International Standard.

This International Standard does not specify any protocol elements nor algorithms for facilitating routeing and relaying among SNAREs. Such functions are intentionally outside the scope of this International Standard.

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented. Such a statement is called Protocol Implementation Conformance Statement (PICS), as defined in ISO/IEC 9646-1. This International Standard provides the PICS proforma in compliance with the relevant requirements, and in accordance with the relevant guidance, given in ISO 9646-7.

2 Normative references

The following standards contain provisions which, through reference in the text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 7498-1 : 1994, *Information technology — Open Systems Interconnection — Basic Reference Model — Part 1: The Basic Model.*

ISO/IEC 8208 : 1990, *Information technology — Data communications — X.25 Packet Layer Protocol for Data Terminal Equipment.*

ISO/IEC 8208 : 1990/Amd. 3 : 1991 *Information technology — Data communications — X.25 Packet Layer Protocol for Data Terminal Equipment — Amendment 3: Conformance requirements.*

ISO/IEC 8348 : 1993, *Information technology — Open Systems Interconnection — Network Service Definition.*

ISO 8648 : 1988, *Information processing systems — Open Systems Interconnection — Internal organization of the Network Layer.*

ISO 8802-2 : 1989, *Information processing systems — Local area networks — Part 2: Logical link control.*

ISO/IEC 8878 : 1992, *Information technology — Telecommunications and information exchange between systems — Use of X.25 to provide the OSI Connection-mode Network Service.*

ISO/IEC 8880-1 : 1990, *Information technology — Telecommunications and information exchange between systems — Protocol combinations to provide and support the OSI Network Service — Part 1: General principles.*

ISO/IEC 8880-2 : 1992, *Information technology — Telecommunications and information exchange between systems — Protocol combinations to provide and support the OSI Network Service — Part 2: Provision and support of the connection-mode Network Service.*

ISO/IEC 8881 : 1989, *Information processing systems — Data communications — Use of the X.25 packet level protocol in local area networks.*

ISO/IEC 8886 : 1992, *Information technology — Telecommunications and information exchange between systems — Data link service definition for Open Systems Interconnection.*

ISO 9542 : 1988, *Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473).*

ISO/IEC TR 9575 : 1990, *Information technology — Telecommunications and information exchange between systems — OSI Routeing Framework.*

ISO/IEC TR 9577 : 1993, *Information technology — Telecommunications and information exchange between systems — Protocol identification in the network layer.*

ISO/IEC 9646-1 : 1994, *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 1: General concepts.*

ISO/IEC 9646-7 : ________[1], *Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation conformance statements.*

ISO/IEC 10028 : 1993, *Information technology — Telecommunications and information exchange between systems — Definition of the relaying functions of a Network layer intermediate system.*

ISO/IEC 10039 : 1991, *Information technology — Open Systems Interconnection — Local area networks — Medium Access Control (MAC) service definition.*

ISO/IEC 10177 : 1993, *Information technology — Telecommunications and information exchange between systems — Provision of the connection-mode Network internal layer service by intermediate systems using ISO/IEC 8208, the X.25 Packet Layer Protocol.*

ISO/IEC TR 10178 : 1992, *Information technology — Telecommunications and information exchange between systems — The structure and coding of Logical Link Control addresses in Local Area Networks.*

3 Definitions

3.1 Reference Model Definitions

This International Standard makes use of the following terms defined in ISO/IEC 7498-1:

a) Network Layer
b) Network Service Access Point
c) Network Service Access Point address
d) Network Entity
e) Routeing
f) Network Protocol
g) Network Relay
h) Network Protocol Data Unit

3.2 Network Layer Architecture Definitions

This International Standard makes use of the following terms defined in ISO 8648:

a) Subnetwork
b) End System
c) Intermediate System
d) Subnetwork Service
e) Subnetwork Access Protocol

3.3 Network Layer Addressing Definitions

This International Standard makes use of the following terms defined in ISO/IEC 8348:

a) Network Entity Titles
b) Subnetwork address
c) Subnetwork Point of Attachment

3.4 Local Area Network Definitions

This international Standard makes use of the following terms defined in ISO 8802-2:

a) Multicast address
b) Broadcast address

3.5 Additional Definitions

For the purposes of the International Standard, the following definitions apply:

3.5.1 configuration information: Information about the collection of End Systems and Intermediate Systems attached to a subnetwork defined in

[1] To be published.

terms of the system types, Network Addresses present, Network Entity Titles present, and the correspondence between systems, SNPA addresses, and potential routes.

3.5.2 redirection information: Information supplied when a Call Request fails to achieve establishment of a Network Connection, indicating an SNPA which could be used to establish such a connection.

3.5.3 subnetwork address resolution entity: Supplier of information concerning routeing within a single subnetwork.

3.6 PICS Definitions

This International Standard makes use of the following terms defined in ISO/IEC 9646-7.

a) Protocol Implementation Conformance Statement (PICS)

b) PICS proforma

4 Abbreviations

4.1 Systems

DTE	Data Terminal Equipment
ES	End System
IS	Intermediate System
SNARE	Subnetwork Address Resolution Entity

4.2 Protocol Data Units

ECQ PDU	End/Intermediate System Configuration Query Protocol Data Unit
ENC PDU	End/Intermediate System Notification Complete Protocol Data Unit
ERA PDU	End System Request Address Protocol Data Unit
ESC PDU	End/Intermediate System Connect Protocol Data Unit
ESH PDU	End/Intermediate System Hello Protocol Data Unit
RD PDU	Redirect Protocol Data Unit
SAA PDU	SNARE Assign Address Protocol Data Unit
SCC PDU	SNARE Configuration Complete Protocol Data Unit
SCR PDU	SNARE Configuration Response Protocol Data Unit
SHL PDU	SNARE Hello Protocol Data Unit
SNC PDU	SNARE Notification Complete Protocol Data Unit
SRH PDU	SNARE Request Hello Protocol Data Unit
SRN PDU	SNARE Received Notification Protocol Data Unit

NOTE — The name of the PDU should not be construed as implying a definition of the PDU's function. For example an ECQ PDU can be transmitted by an IS.

4.3 Miscellaneous

BCD	Binary Coded Decimal
LLC	Logical Link Control
MAC	Medium Access Control
NA	Network Address
NPDU	Network Protocol Data Unit
QOS	Quality of Service
SNPA	Subnetwork Point of Attachment

5 Overview of the Protocol

The protocol specified in this International Standard comprises two subsets:

a) The Configuration Information subset

b) The Redirection Information subset

The functions of the Configuration Information subset are:

a) To enable ESs to notify a SNARE of the existence and reachability of their Network Addresses (NAs).

b) To enable ESs to discover, for certain remote NAs, the SNPA addresses of systems on the subnetwork via which communications may potentially be routed.

c) To enable ESs to obtain their own Network Addresses without manual intervention.

d) To enable ISs to obtain, for NAs identifying NSAPs located within End Systems directly attached to the same subnetwork, the SNPA address of these systems.

The function of the Redirection Information subset is to enable ESs which are attempting to establish a connection to be directed to a specific appropriate SNPA address via which the connection should be routed and to permit ISs which are attempting to establish a connection to an ES on the subnetwork to be directed to the appropriate SNPA address via which the connection can be established.

The two subsets are complementary in that the information obtained from the Redirection Information subset implicitly carries associated Configuration Information, and in that the information obtained from the Configuration Information subset may be used to derive a suitable SNPA address and so avoid the need for use of the Redirection Information subset. The choice of which subset to use to obtain Routeing Information for any individual instance of communication is a local ES or IS decision, which may be different for different instances of communication and may be varied freely during ES or IS operation without impacting the ability to interwork.

5.1 The SNARE Function

A SNARE is an entity which collects configuration information from ESs, and which distributes configuration and redirection information to them.

The SNARE also distributes configuration and redirection information to the ISs.

NOTE — A SNARE may also interact with Intermediate Systems for the purpose of collecting configuration information but the details of such interactions are outside the scope of this International Standard.

The function of a SNARE may be carried out by one or more ESs or ISs attached to the subnetwork. Where the subnetwork is one which itself acts on the X.25 protocol, it is also possible that some or all of the SNARE operations may be performed by functions integrated with the subnetwork itself.

In order for an ES (or IS) to use this protocol, it requires knowledge of at least one SNPA address which can be used to access a SNARE. In general, this address is pre-configured in the ESs (or ISs). Annex A describes techniques which may be used in certain circumstances to avoid the need for such pre-configuration.

5.2 Overview of Configuration Information

The protocol exchanges which constitute the Configuration Information subset begin with the ES establishing an X.25 connection to a SNARE by issuing an X.25 Call Request. The first octet of the call user data contains a protocol identifier indicating the protocol defined in this International Standard. When the SNARE accepts the call, the ES may then transmit to the SNARE details of its Network Addresses. Once the information concerning all of its Network Addresses is transmitted the ES explicitly notifies the SNARE that the notification is complete so that the SNARE can ensure that all the information received is secure to the extent required for its use. Optionally, following acceptance of the call by the SNARE, a non-configured End System may request a NET for itself. Once it obtains this information it may derive additional Network addresses for subsequent interactions with other End Systems. However, it is not necessary or even permitted for an End System to use a NET obtained in this manner indefinitely. The ES may also request information about remote Network Addresses. For each requested Network Address the SNARE supplies details of the SNPA or SNPAs on the subnetwork via which the Network Address can be reached, and the associated potential Quality of Service. Having received information about one Network Address, the ES can request information about another. When it has all the information it requires, the ES clears the call.

An IS also may request information about Network Addresses. In the present context this request will strictly take place within the realm of Single Network Routeing, as defined in ISO/TR 9575, and is thus hierarchically placed under any IS-IS routeing activity. Therefore this request can only occur for Network Addresses corresponding to End Systems directly attached to the subnetwork. However, this protocol contains no provisions to ensure that this is so, and relies instead on the processes effected above it in the routeing hierarchy.

The protocol exchanges begin with the IS establishing an X.25 connection to a SNARE by issuing an X.25 Call Request. When the SNARE accepts the call, the IS may request information about one or several Network Addresses. For each requested Network Address the SNARE supplies details of the SNPA (or SNPAs) of the system at which the Network Address resides. Having received information about one Network Address, the IS can request information about another. When it has all the information it requires, the IS clears the call."

5.3 Overview of Redirection Information

The redirection information functions can be considered as two parts.

The first part takes place when an ES (or IS) is about to establish a Network Connection according to ISO/IEC 8878, but does not have the information necessary to determine the appropriate subnetwork address to which the Call Request should be transmitted. The action of the ES (or IS) in this case is simply to use the address of a SNARE. The Call Request packet is constructed exactly in accordance with ISO/IEC 8878 and is transmitted to the SNARE.

The ES (or IS) subsequently continues to operate the connection in accordance with ISO/IEC 8878. In the event that the SNARE is an ES or IS attached to the subnetwork, rather than having functionality integrated with the subnetwork itself, it may:

— use the X.25 Call Deflection facility to deflect the call to an appropriate ES or IS;

— clear the call, supplying information about the appropriate SNPA which should be used for future attempts; or

— if it contains relay functions, accept the call itself and take part in the connection as a relay.

If the SNARE function is integrated with the subnetwork itself, then in addition to the above it may be able to deliver the call to an appropriate SNPA by other means which are outside the scope of this International Standard (for example, by invoking the X.25 Call Redirection facility).

Since, therefore, the connection establishment may now be going to proceed satisfactorily without the originating ES (or IS) doing any further routeing operations, the ES (or IS) continues to process the Network Connection in accordance with ISO/IEC 8878 unless a Clear Indication is received.

Receipt of a Clear Indication in response to a Call Request causes the second part of the redirection information procedure to take place. At this point, provided the cause and diagnostic codes in the clear indication packet show that the disconnection was not initiated by the Network Service user, the ES (or IS) checks whether there is user data in the packet containing information encoded according to this International Standard indicating an appropriate subnetwork address via which a Network Connection equivalent to that being rejected could be established. An equivalent Network Connection is one between the same NSAPs with the same Quality of Service parameters. The ES (or IS) may use this information either to retry the connection establishment, according to the provisions of ISO/IEC 8878, or in establishing future equivalent network connections.

6 Conformance

6.1 Static Conformance Requirements

An ES for which conformance to this International Standard is claimed shall implement one or more of the following:

a) The procedures of the system Configuration Information Subset, specified in clause 8, that apply to an ES.

b) The procedures of the system Redirection Information Subset, specified in clause 9, that apply to an ES.

An IS for which conformance to this International Standard is claimed shall implement one or more of the following:

a) The procedures of the system Configuration Information Subset, specified in clause 8, that apply to an IS, in particular 8.2.3.3.

b) The procedures of the system Redirection Information Subset, specified in clause 9, that apply to an IS.

A SNARE for which conformance to this International Standard is claimed shall implement those procedures which clause 11 prescribes as requirements.

NOTE — Therefore a SNARE is required to process both Configuration and Redirection Information.

6.2 Dynamic Conformance Requirements

A system for which conformance to this International Standard is claimed shall exhibit external behavior consistent with having implemented:

a) for each supported function, the corresponding procedures and the encoding of any transmitted Protocol Data Units, as specified in the relevant subclauses of clauses 8, 9, 10, 11 and 12;

b) the X.25 Packet Layer Protocol in conformance with the requirements of ISO/IEC 8208 Amd. 3, and in conformance with the procedures invoked by ISO 8880 for the relevant environment.

7 SNARE Subnetwork Address

The use of this protocol requires an ES (or an IS) to be aware of at least one subnetwork address at which a SNARE can be reached. Local methods may be provided for determining such an address; alternate methods described in Annex A may be used where they are available.

In the event that an ES is aware of more than one SNPA at which a SNARE can be reached, the choice between them is a local matter.

8 Configuration Information Subset

8.1 Protocol Parameters

This clause defines parameters used in this protocol and, where applicable, specifies which values of these parameters are required to be supported by all conforming end systems. The ability to support values other than those specifically required, and the means of identifying that such a value is to be used in any particular instance, are local matters.

8.1.1 Response Time

This is the time limit used by an ES (or IS) during operation of the protocol.

Any implementation of the Configuration Information subset shall be capable of supporting a response time value of 180 s, accurate to within ± 30 s.

8.1.2 Notification Retry Time

This is the time interval at which an ES shall retry a failed attempt to convey its configuration to a SNARE.

Any implementation of the Configuration Information subset shall be capable of supporting a Notification Retry Time value of 900 s, accurate to within ± 120 s, if it supports any values of the Notification Required parameter other than that which indicates that notification is never required and that which indicates that no specific value is being suggested.

NOTE — There are no requirements on the support of Notification Retry Time by an implementation which does not support such values of the Notification Required parameter.

8.1.3 Notification Required

This parameter indicates the circumstances in which an ES shall attempt to notify its configuration to a SNARE.

Any implementation of the Configuration Information subset shall be capable of supporting a value of this parameter which indicates that notification is never required.

NOTE — Examples of other Notification Required parameter values which might optionally be supported include:

- A value indicating that notification is required each time the ES is initialized and subsequently at the expiry of the time specified by the SNARE at the end of each preceding notification.
- A value indicating that notification is required each time the ES is attached to a different subnetwork.

It is emphasized that these are only examples — other values are permitted.

8.1.4 Address Holding Time

This is the time for which the End System may continue to use an NET that has been assigned to it by the SNARE.

8.2 Protocol Operation

This clause specifies the protocol making use of the X.25 Packet Layer Procedures specified in ISO/IEC 8208. Subject to the provisions of ISO/IEC 8208, the choice of values for X.25 fields which are not specified in this clause is a local matter.

8.2.1 Connection Establishment

An ES (or an IS) shall attempt to establish a connection whenever it needs to obtain configuration information from a SNARE. In addition, an ES shall attempt to establish connection to a SNARE when conditions specified in 8.1.3 make it necessary to notify configuration information to a SNARE. The ES shall attempt to establish a connection to a SNARE when it needs to obtain a NET when initially connecting to the subnetwork or upon expiration of the Address Holding Time value. However, neither an ES nor an IS shall attempt to establish a connection that have already a connection established or being established for the use for configuration information, and neither an ES nor an IS shall attempt to establish more than one connection to SNAREs from any one one system SNPA at any one time.

An ES (or an IS) shall attempt to establish a connection to the SNARE by originating a virtual call in accordance with the procedures for virtual call setup specified in ISO/IEC 8208. The SNPA address to which the Call Request shall be transmitted shall be one applicable to the SNARE, as described in clause 7. The Fast Select facility shall be specified, indicating no restriction on response. The User Data to be transmitted with the Call Request packet shall contain an ESC PDU.

If the virtual call setup procedure succeeds, the ES (or IS) shall examine the User Data received with the Call Connected packet.

If this contains a valid SNC PDU, then the ES (or IS) shall proceed to perform data transfer as specified in 8.2.3. Otherwise the ES (or IS) shall clear the call according to the procedures for virtual call clearing specified in ISO/IEC 8208 using a cause code of 0 and a diagnostic code of 242, and shall then act according to the procedure for failed connection establishment in 8.2.2.

If the virtual call setup procedure fails, the ES (or IS) may retry it provided that the failure was due to a cause which, if it occurred in an attempt to establish a Network Service connection, would have been interpreted according to ISO/IEC 8878 as "connection rejection — transient condition". However, attempts to retry shall not continue for longer than the value of the Response Time parameter. When it has finished retrying, the ES (or IS) shall proceed as specified in 8.2.2.

8.2.2 Connection Establishment Failure Procedure

When an attempt to establish a connection fails, if the ES (or IS) has knowledge of any alternative SNARE subnetwork address, it shall attempt to establish a connection to one which it has not previously tried in this establishment attempt.

When all known SNARE addresses have been tried unsuccessfully:

a) If the ES (or IS) needed to obtain Configuration Information from the SNARE, the time at which a further attempt is made (if any) or the invocation of other forms of action (e.g., fallback to default configuration, or use of Redirection subset as a basis for routeing) is a local matter.

b) If according to the provisions of 8.1.3 the ES was due to notify its configuration to a SNARE, the attempt at notification shall be considered to have failed. Another attempt shall be made after the expiry of the Notification Retry Time.

c) If the ES needed to obtain a NET, the time at which a further attempt is made (if any) is a local matter.

8.2.3 Data Transfer Procedure

This clause specifies the transfer of data once an acceptable connection to a SNARE has been achieved.

This clause requires transmission of a number of PDUs. Each PDU shall be transmitted as a single M-bit sequence without the Q-bit set, according to the procedures for data transfer specified in ISO/IEC 8208.

This clause also requires, in some circumstances, that the connection be abandonded before completion. This shall be done by clearing the call according to the procedures for virtual call clearing specified in ISO/IEC 8208, using a cause code of 0 and a diagnostic code of 242.

In the event that the virtual call is cleared (whether by the ES (or IS) itself abandoning the connection according to the provisions of this International Standard, or as a consequence of the operation of ISO/IEC 8208 procedures) before the normal completion of the data transfer procedure specified in this clause, the ES shall follow the procedure for failed connection specified in 8.2.4.

In the event that a Reset Indication, an Interrupt packet, or Q-bit data is received at any time during the operation of the data transfer procedure, the ES (or IS) shall abandon the connection.

The data transfer procedure consists of 3 parts -- address assignment, configuration notification and configuration collection. When the address assignment procedure is applicable, it shall be carried out immediately following connection establishment. When the configuration notification procedure is applicable, it shall be carried out after completion of the address assignment procedure (or immediately if the address assignment procedure is not applicable). When the configuration collection procedure is applicable, it shall be carried out after completion of the address assignment and/or configuration notification procedures (or immediately if the address assignment and configuration notification procedures are not applicable). After completion of all applicable parts, the ES shall follow the procedure for normal completion as specified in 8.3.

8.2.3.1 Configuration Notification

The configuration notification procedure is an optional procedure and, when implemented, its operation is controlled by the setting of the Notification Required parameter.

This procedure is applicable when (and only when) the following conditions are satisfied:

a) The Notification Required parameter is set to a value which indicates that the ES should notify its configuration to a SNARE at this time.

b) An attempt to notify configuration has not failed within the duration specified by the Notification Retry Time parameter.

The ES shall start the procedure by transmitting one ESH PDU for each Network Address reachable through its SNPA. Following the ESH PDUs it shall transmit an ENC PDU. It shall then wait to receive an SRN PDU. If the received SRN PDU contains the Notification Required parameter then the ES shall extract and use this value as the next time interval prior to notification to the SNARE. On receipt of the SRN PDU, the configuration notification procedure is successfully completed.

NOTE 1 — After such successful completion, the value of the Notification Required parameter determines if and when this procedure will subsequently again be applicable.

After the transmission of the first ESH PDU, if the SRN PDU has not been received within a time equal to the Response Time parameter, the connection shall be abandoned.

NOTE 2 — The expiry of this time may be a result either of delays in transmitting the PDUs (e.g., because of flow control), or delay in response by the SNARE.

If any data is received by the ES before transmission of the ENC PDU, or if any data is received which does not contain a valid SRN PDU, the connection shall be abandoned.

8.2.3.2 Configuration Collection by End Systems

The configuration collection procedure is an optional procedure and, when implemented, its operation is applicable whenever the ES requires to obtain information from a SNARE about the SNPAs of systems which may be used to reach remote Network Addresses. This International Standard does not impose any constraints on how often an ES attempts to collect configuration information.

The ES shall transmit an ECQ PDU specifying a Network Address for which it requires information. In response it may receive a number of SCR PDUs, containing information about SNPAs through which the specific Network Address may be reached. The SCR PDU may include an Address Mask parameter and a SNPA Mask parameter. These parameters may be used as described in 8.1.4 and 8.1.5, respectively.

The receipt of an SCC PDU indicates that the information is complete; if no SCR PDUs are received before the SCC PDU this indicates that no information is available for the specified Network Address. If the ES requires information about further Network Addresses, it may then repeat the process provided that the Query Limit field in the SCC PDU specifies that another query is allowed. If the Query Limit field specifies that no more queries are allowed, the ES shall not transmit any more ECQ PDUs. When the ES has information for all the Network Addresses it requires, or the Query Limit disallows further queries, the configuration collection function is successfully complete.

If a time greater than the Response Time parameter elapses after transmission of an ECQ PDU and before receipt of the corresponding SCR or SCC PDU, the connection shall be abandoned.

The following shall also cause the connection to be abandoned:

a) Receipt of any data which does not contain a valid SCR or SCC PDU.

b) Receipt of any PDU before transmission of the first ECQ PDU, or between receipt of an SCC PDU and transmission of the next ECQ PDU.

c) Receipt of a PDU relating to a Network Address other than that for which the ES has transmitted an ECQ PDU on the connection and not received an SCC PDU.

8.2.3.3 Configuration Collection by Intermediate Systems

The configuration collection procedure is an optional procedure and, when implemented, its operation is applicable whenever the IS requires to obtain information from a SNARE about the SNPAs of End Systems directly attached to the same subnetwork at which are located certain Network Addresses. This International Standard does not impose any constraints on how often an IS attempts to collect configuration information.

The IS shall transmit an ECQ PDU specifying a Network Address for which it requires information. Because of the hierarchical fashion after which routeing is organized within OSI, this request takes place under the umbrella of an IS-ES exchange. Therefore the SCR PDUs that the IS may receive in response from the SNARE can only contain information on SNPAs of End Systems directly attached to the subnetwork. The SNPA correspond to system at which the NSAPs are located. The SCR PDU may include an Address Mask parameter, and a SNPA Mask parameter which may be used as described in 10.1 and 10.2 respectively.

The receipt of an SCC PDU indicates that the information is complete; if no SCR PDUs are received before the SCC PDU this indicates that no information is available for the specified Network Address. If the ES requires information about further Network Addresses, it may then repeat the process provided that the Query Limit field in the SCC PDU specifies that another query is allowed. If the Query Limit field specifies that no more queries are allowed, the ES shall not transmit any more ECQ PDUs. When the ES has information for all the Network Addresses it requires, or the Query Limit disallows further queries, the configuration collection function is successfully complete.

If a time greater than the Response Time parameter elapses after transmission of an ECQ PDU and before receipt of the corresponding SCR or SCC PDU, the connection shall be abandoned.

The following shall also cause the connection to be abandoned:

a) Receipt of any data which does not contain a valid SCR or SCC PDU.

b) Receipt of any PDU before transmission of the first ECQ PDU, or between receipt of an SCC PDU and transmission of the next ECQ PDU.

c) Receipt of a PDU relating to a Network Address other than that for which the ES has transmitted an ECQ PDU on the connection and not received an SCC PDU.

NOTE — A procedure identical to the Configuration Collection procedure could conceivably be used by an IS-IS protocol. It is not within the scope of this document to discuss this matter.

8.2.4 Failed Connection Procedure

When a connection fails:

a) If the configuration notification procedure is applicable, then it shall be considered that the notification attempt has failed. (Consequently it will again be applicable when the time indicated by the Notification Retry Time parameter has expired.)

b) Any Configuration Information received in SCR PDUs for which no corresponding SCC PDU has been received is incomplete.

NOTE — It is a local matter whether the system (ES or IS) will make use of incomplete data or whether it will discard it. Whether and when to make another attempt to obtain the remainder of incomplete data, or information still required for other Network Addresses, is also a local matter.

8.3 Normal Completion Procedure

When the applicable data transfer procedures have been successfully completed, if the Query Limit field contained in the SCC PDU indicated that no more query requests are allowed, then the ES (or IS) shall clear the call according to the virtual call clearing procedure specified in ISO/IEC 8208, using cause code 0 and diagnostic code 241. If the Query Limit field does permit another request, then the ES (or IS) shall do either (a) or (b) below:

a) It may clear the call immediately, using cause code 0 and diagnostic code 241.

b) It may retain the call for a time and subsequently use it for further data transfer functions as specified in 8.2.3 when these functions again become applicable. The maximum time for which a call may be retained without such further data transfer taking place is half the value of the Request Time parameter received in the SNC PDU. Once this time has elapsed the system (ES or IS) shall clear the call with a cause code 0 and a diagnostic code 241. The ES is not required to retain calls for this maximum time period; instead it may, as a local choice, clear the call at any convenient earlier time, still using cause code 0 and diagnostic code 241. During the time that the call is retained, the system (ES or IS) shall continue to operate it according to the procedures specified in ISO/IEC 8208. If a Data, Reset, or Interrupt packet is received, it shall clear the call with cause code 0 and diagnostic code 242. In the event that this occurs, or in the event that a Clear Indication is received or the operation of ISO/IEC 8208 procedures results in the call being cleared, it is a local matter whether and when to attempt to establish another call according to the procedures specified in 8.2.1.

The choice between (a) and (b), and the length of time for which calls are retained if action (b) is chosen, are purely local matters and the ES may freely vary them according to internal conditions without impact on interworking.

8.4 Use of Configuration Information

This clause applies applies identically to End Systems and Intermediate Systems. This international Standard does not impose any constraints on how much of the information collected by a system is retained or used. A system may discard collected information at any time, and make a new request to collect the information again if it is subsequently required.

A system may at any time use local knowledge or any other method of determining the SNPA to be used in establishing any Network Connection to any Network Address, regardless of whether it has collected Configuration Information which would be applicable.

The configuration information obtained by this protocol is valid only subject to the following restrictions:

a) Configuration Information indicating which SNPA address to use for establishing a connection is not valid unless it was supplied in information for the relevant Network Address and applies to a QOS range which includes the minimum acceptable QOS for the required network connection.

b) Configuration Information is not valid if the time since it was received is greater than that specified in the Holding Time field of the SCR PDU which conveyed it.

c) Configuration Information which has already been collected is no longer valid once the system has again successfully collected complete configuration information for the same Network Address, regardless of whether the Holding Time specified when the first information was collected has yet elapsed.

8.5 Address Assignment for End Systems

8.5.1 Request Address Function

The Request Address procedure is an optional procedure and, when implemented, its operation is controlled by the setting of the Address Holding Time parameter.

This procedure is applicable when (and only when) the following conditions are satisfied:

a) The End System is being initially attached to the subnetwork and is not pre-configured with knowledge of its Network Address, or

b) The Addressing Holding Timer for this End System has expired, indicating that the ES should request a new NET.

Such a system initiates a request for a NET, following connection establishment as outlined in 8.2.1, by forwarding a single ERA PDU.

Following the ERA PDU it shall transmit an ENC PDU. It shall then wait to receive an SAA PDU followed by an SRN PDU.

After the transmission of the ERA PDU requesting the NET, and subsequent ENC PDU, if the SAA PDU has not been received within a time equal to the Response Time Parameter, the connection shall be disconnected.

8.5.2 Record Address Function

The record address function receives the SAA PDU and extracts the assigned NET from it. It starts an Address Holding Timer (see 8.1.4) based on the address holding time parameter contained in SAA PDU. The value "zero" is excluded as an allowable value for the AHT parameter. The assigned NET may be used as a Network address. If the End System employs more than one Network address for its operation, it may derive additional addresses from the assigned NET by using the code points provided by the "zeros" in the last octet (binary DSP format) or last two digits (decimal DSP syntax). Using this function the NET sent to the ES in the SAA PDU shall have its last octet (binary DSP syntax) or last two digits (decimal DSP format) set to "zero" value and the ES may derive Network address(es) by changing only that last octet or two digits. (Also see 11.3.)

Note — The method of derivation is not specified in this standard.

8.5.3 Flush Address Function

If an End System acquires a NET through the operation of the "request address" function, it must implement an Address Holding Timer associated with this NET based on the address holding time parameter contained in the SAA PDU. If the timer expires, the End System discards the NET and all derived Network addresses, and performs the "request address" function to obtain a new NET.

Note — This ensures that NETs that have been erroneously or improperly assigned (as, for example, by a malfunctioning SNARE) will eventually be purged. To provide continuous service, the "request address" function may be performed before expiration of the AHT. When this function is used to obtain a "new" NET, it is entirely possible for the "new" one to be the same as the "old", depending on how the SNAREs have implemented their NET administrative algorithms.

There is an additional cause to discard the NET (and derived Network addresses). This is if the ES changes its SNPA for any reason.

9 System Redirection Information Subset

Except where noted, the Redirection Information Subset applies indifferently to End Systems or Intermediate Systems.

9.1 Invoking Redirection

This clause defines the procedure which shall be followed by a system in order to use the Redirection Information subset to select the SNPA to which a connection request is to be sent. It is a local decision whether to use this procedure for any particular instance of communication, or whether to use previously obtained Redirection or Configuration Information or some other method.

In order to invoke Redirection, the ES shall proceed with the Network Connection establishment procedure as specified in ISO/IEC 8878, but shall use as the SNPA address to which the call is sent an address of a SNARE as defined in clause 7.

In order to invoke Redirection, the IS acts similarly, except that it is the ISO/IEC 10028 Network Internal Connection establishment that is procedded according to ISO/IEC 10177.

NOTES

1 For example, in the case of a packet-switching subnetwork, the DTE address of the SNARE would be placed in the Called Address Field of the packet. In the case of an ISO 8802 LAN, the ES would be operating according to ISO 8881, and the LLC address of the SNARE would be used as the destination address for the transmission of the frame containing the Call Request packet.

2 Where this results in the address in the Called Address Field of the Call Request packet being that of the SNARE, it follows from the provisions of ISO/IEC 8878 that the called NSAP address is encoded in the Address Extension Facility, since the remote ES may not be able to deduce it from the Address Field.

The system shall continue to process the connection in accordance with ISO/IEC 8878 and the IS in accordance with ISO/IEC 10177.

9.2 Receiving Redirection Information

This clause describes the procedure to be followed in order to receive Redirection Information.

9.2.1 Redirect Information Procedure for Clear Indications

A system (ES or IS) which implements the Redirection Information subset shall follow this procedure whenever an attempt to establish a Network Connection fails because a Clear Indication packet is received.

NOTE — This procedure is not restricted to calls which were originally transmitted to SNARE in accordance with 9.1. This is because even if the SNPA address for a call was selected by other means, it may in fact be the SNPA of a system with SNARE functionality, or the call may have been redirected to a SNARE.

The cause and diagnostic codes shall be examined to determine the corresponding values of Network Service disconnect indication Originator and Reason parameters according to the criteria specified in ISO/IEC 8878.

If the Originator value is not NS-Provider, then the procedure is complete — no redirection information is available. The system shall continue to follow the procedures specified in ISO/IEC 8878 for dealing with clear indications in ISO/IEC 8878 if the system is an ES, in ISO/IEC 10177 if the system in an IS.

If the Originator value is NS-Provider, the User Data field of the Clear Indication packet shall be examined.

If it contains a RD PDU, and if the Network Connection Establishment Delay has not been exceeded, then the call shall be retried using the SNPA in the RD PDU, unless that is the same as the SNPA which was used for the failed call.

If the Clear Indication packet contains an RD PDU but the Network Connection Establishment Delay has been exceeded, then the information from the RD PDU may be saved for use in establishing future connections with the same Network Address and QOS, unless the SNPA is the same as that which was used for the failed call in which case the information shall be discarded.

If the Clear Indication packet does not contain an RD PDU, then it is recommended that if the call was originally transmitted to a SNARE according to 9.1, the clearing cause code should be analyzed in terms of the categories defined in CCITT recommendation X.96. If it is a category D code, then preference should be given to using a different SNPA address for subsequent access to a SNARE, if other SNARE SNPA addresses are available.

It is recommended that when a call which was transmitted to a SNARE SNPA fails to be established without Redirection Information being received, the existence of any information about other possible SNARE SNPA addresses which may be able to supply Redirection Information should be taken into account in determining whether to retry the call in accordance with ISO/IEC 8878 or ISO/IEC 10177 as applicable.

The RD PDU may include an Address Mask parameter and an SNPA Mask parameter. These parameters may be used as described in 10.1 and 10.2, respectively.

9.2.2 Recommended Processing of Call Connected Packets

The recommendation below applies to both ESs and ISs using the protocols defined by this International Standard. It is recommended that when a system which implements the Redirection Information subset receives a Call Connected packet which completes a virtual call setup initiated by transmission of a Call Request packet to a SNARE SNPA, it should check whether the Call Connected packet indicates that the call was deflected (where applicable) or redirected. If so, it may then record the SNPA to which the call was eventually established, and may use this information in establishing subsequent connections with the same Network Addresses and QOS, to save having to refer to the SNARE.

However, a system which implements this recommendation shall cease to use information obtained in this way when an attempt to use it results in failure to establish a connection, other than because of connection rejected by the remote user.

NOTES

1 A system which implements this procedure and uses the recorded SNPA for a subsequent connection is not required to use it for all such connections, but may use it for some instances of communication and not others, on the basis of local decisions.

2 Since there is no timer associated with information derived in this way, it is possible that a system can be continuing to use a route when it is no longer optimal, provided it is still sufficiently good to supply the required QOS. The system may trade-off this possibility of less than optimal routeing against the saving of not having to access the SNARE for more up-to-

date information (and the consequent reduction in connection establishment time).

9.3 Use of Redirection Information

This International Standard does not impose any constraints on how much of the Redirection Information obtained by ESs and ISs is retained or used. An ES may discard received information at any time, and invoke redirection again for subsequent connections.

An ES may at any time use local knowledge or any other method of determining the SNPA to be used in establishing any Network Connection to any Network Address, regardless of whether it has received redirection information which would be applicable.

The redirection information obtained by this protocol is valid only subject to the following restrictions:

a) Redirection Information indicating which SNPA address to use for establishing a connection is not valid unless it was supplied in information for the relevant Network Address and applies to a QOS range which includes the minimum acceptable QOS for the required network connection.

b) Redirection Information is not valid if the time since it was received is greater than that specified in the Holding Time field of the RD PDU which conveyed it.

c) An item of Redirection Information is no longer valid if an attempt to establish a connection using it fails other than through rejection by the remote user.

10 Address and SNPA Masks

This clause describes a method of conveying additional information in SCR and RD PDUs. The information is conveyed by means of the PDU fields "Address Mask" and "SNPA Mask" whose significance is described below.

A SNARE may optionally include in any SCR or RD PDU either an Address Mask field alone, or else both an Address Mask and a SNPA Mask field. An ES receiving one of these PDUs containing either of these fields shall either ignore both fields, or shall process them according to the following subclauses.

10.1 Address Mask

The Address Mask parameter indicates that the Forwarding Information applies to a larger population of NAs than the original destination NA associated with the received SCR or RD PDU. A System may choose to ignore this parameter.

The Address Mask establishes the equivalence class of NAs to which the same Forwarding Information applies. In order to determine whether or not a potential destination NA falls within the equivalence class, an originating system aligns the potential destination NA with the Address Mask, padding the latter with trailing zero octets (binary 0000 0000) if necessary. If in all the bit positions where the Address Mask is "1" the trial destination NA matches the NA associated with the SCR or RD PDU, then that trial destination NA belongs to the equivalence class described by the SCR or RD PDU. In making routeing decisions, an exact NA match takes precedence over the use of equivalence classes. An exact match occurs when the trial NA is identical to the one associated with the SCR or RD PDU, without considering any mask. If a destination NA is within more than one equivalence class, the choice of which to use, if any, is a local matter.

An all zero Address Mask may be used to indicate an omniscient IS for outgoing calls for which no route is otherwise known.

NOTE — By choosing an Address Mask according to the boundaries in the hierarchically administered Network Address, the Address Mask permits routeing by subnetwork, by routeing domains, or by other administratively controlled criteria.

The Address Mask parameter has additional semantics when considered in conjunction with the SNPA Mask parameter; see 8.1.5.

10.2 SNPA Mask

When the SNPA Mask is present, the equivalence class defined by the Address Mask also has a common structure below the Address Mask, i.e., in the portion of the Network Address where the Address Mask is logically "0." The SNPA Mask supplies additional information about that structure, by indicating certain bit positions within the space "below" the Address Mask. Specifically, the SNPA Mask indicates the location of the SNPA in the Network Address.

A system which receives such a SCR or RD PDU containing Address Masks and/or SNPA Masks may choose to ignore both masks. However, since the presence of both masks dictates different behavior from the presence of the Address Mask alone, a system (ES or IS) shall not ignore one of the masks while heeding the other. If the system (ES or IS) receives one of these PDUs containing an SNPA Mask but no Address Mask, the system (ES or IS) shall either ignore the SNPA Mask, or else treat the PDU as invalid.

11 SNARE Procedures

The procedures to be followed in a SNARE function which is integrated with an X.25 subnetwork are outside the scope of this International Standard. This clause describes the procedures to be followed by a system attached to a subnetwork in order to perform a SNARE function.

On receiving an Incoming Call packet, provided that it currently has resources available to accept the call, the SNARE shall examine the first octet of the User Data field, and proceed as follows;

a) If there is no user data, or if the first octet has a value in the range 00000010 to 00111111, the SNARE shall proceed as specified in 11.2.

b) If the first octet of user data has the value defined in 12.1.1, the SNARE shall proceed as specified in 11.1.

c) For any other case, the action taken by the SNARE is outside the scope of this International Standard.

11.1 Processing of Configuration Subset

11.1.1 Protocol Parameters

This clause defines parameters used in the protocol, and where applicable specifies which values of these parameters are required to be supported by all conforming systems. The ability to support values other than those specifically required, and the means of identifying that such a value is to be used in any particular instance, are local matters.

11.1.1.1 Request Time

This parameter indicates the time which the SNARE will wait for requests from a system (ES or IS) with which it has a connection established, or may indicate that it will wait an unlimited time.

Any SNARE implementation shall be capable of supporting a request time value of 60 s, accurate to within ± 10 s.

11.1.2 Configuration Information Procedure

If the User Data field of the Incoming Call does not contain a valid ESC PDU, the SNARE shall clear the call according to the procedures for virtual call clearing defined in ISO/IEC 8208, with a cause code of 0 and a diagnostic code 248.

If the call does not contain an unrestricted Fast Select facility, the SNARE shall clear the call with a cause code of 0 and a diagnostic code 76.

If the SNARE is temporarily unable to service configuration information, it shall clear the call with a cause code of 0 and a diagnostic code 244.

If the SNARE is not willing to provide services to the calling system, it shall clear the call with a cause code of 0 and a diagnostic 245.

Otherwise the SNARE shall accept the call according to the procedure for call setup specified in ISO/IEC 8208, transmitting a SNC PDU in the User Data of the Call Connected packet. The Request Time field in the SNC PDU shall be set to indicate the largest value which is permitted by the field encoding defined in 12.1.11 and which is not greater than the minimum time limit, if any, which the SNARE will wait for requests from a system with which it has a connection established.

NOTE 1 — The minimum time limit for which the SNARE will wait for requests is determined by the value of the Request Time parameter making allowances for the degree of accuracy within which this parameter is implemented.

The SNARE shall operate the virtual circuit according to the procedures for data transfer specified in ISO/IEC 8208. If it receives a Reset Indication, a Data packet with the Q-bit set, an Interrupt packet, or data which does not conform to the PDU formats specified in clause 12. It shall clear the call with a cause code of 0 and a diagnostic code 242.

If a time greater than the Request Time parameter elapses without receipt of an ESH or ECQ PDU, the SNARE shall clear the call with a cause code of 0 and diagnostic code 242.

On receiving ESH PDUs, the SNARE shall record the information from them.

NOTES

2 The use made by the SNARE of this information is outside the scope of this International Standard.

3 Determination of routes on the basis of information obtained through the configuration notification function may, in some environments, introduce a security risk. It may be possible to mitigate such risk, as an administrative or local matter, by making use of features of the ISO/IEC 8208 protocol which provide a degree of authentication, such as closed user groups.

After receipt of an ESH PDU, if the SNARE receives an ECQ PDU before receiving an ENC PDU, it shall clear the call with a cause code of 0 and a diagnostic code 243. It may but need not also do so if it receives more than one ESH PDU specifying the same Network Address.

If a time greater than the Request Time parameter elapses after receipt of an ESH PDU without receipt of an ENC PDU or another ESH PDU, the SNARE shall clear the call with a cause code of 0 and a diagnostic code 242.

On receiving an ENC PDU, the SNARE shall ensure that all the information received from ESH PDUs is secure to the extent required for its use, and shall then transmit an SRN PDU in a single M-bit sequence according to the procedures specified in ISO/IEC 8208. The Notification Required parameter of the SRN PDU shall be set to indicate the time for which it is suggested the ES should wait, in the absence of a change in configuration or availability, before carrying out a further notification. If the SNARE subsequently receives another ESH PDU, it shall clear the call using a cause code of 0 and a diagnostic code 243.

If a time greater than Request Time elapses after transmission of an SRN PDU without receipt of an ECQ PDU, the SNARE shall clear the call with a cause code of 0 and a diagnostic code 242.

On receiving an ECQ PDU, if the SNARE has information about SNPAs on the subnetwork which may be used by the system (ES or IS) to reach the specified Network Address, it shall transmit for each such SNPA an SCR PDU. When it has transmitted an SCR PDU for each relevant SNPA (or immediately if it has no information about any suitable SNPAs), the SNARE shall transmit an SCC PDU. The Query Limit field of the SCC PDU will be set by the SNARE to indicate whether another query request is allowed.

After transmission of an SCC PDU, if a time greater than Request Time elapses before receipt of another ECQ PDU, the SNARE shall clear the call with a cause code 0 and a diagnostic code 242.

If the SNARE receives another ESC PDU, or if it receives another ECQ PDU before having transmitted the SCC arising from the previous one, or if it receives PDU other than those specified above, it shall clear the call using a cause code of 0 and a diagnostic code 243.

If the SNARE receives another ECQ PDU after having sent an SCC PDU with the Query Limit field indicating no more query requests, it shall clear the call with a cause code of 0 and diagnostic code 242.

11.2 Processing of Redirection Subset

The SNARE shall determine the called Network Address identified by the Call Request packet, in accordance with ISO/IEC 8878. If this is a Network Address allocated to the SNARE itself, the SNARE shall deal with the Network Connection in accordance with the procedures specified in ISO/IEC 8878.

If the Network Address is located in another system to which the SNARE is prepared to act as a Relay, it may do so.

If the Network Address is located in another system, which can be reached by the originating ES via another SNPA on the same subnetwork with an acceptable Quality of Service, the SNARE shall do one of the following:

a) If the Call Deflection facility is available for use on this call, the SNARE may use it in accordance with the procedures defined in ISO/IEC 8208 to deflect the call to an appropriate SNPA.

b) If the Call Deflection facility is not available, or if the SNARE chooses not to use it, then it shall clear the call according to the procedures for virtual call clearing specified in ISO/IEC 8208, using cause code 0 and diagnostic code 230, and transmit an RD PDU in the user data field of the Clear Request packet.

   However, if the Call Request packet did not have the Fast Select facility present, it shall clear the call without User Data, with cause 0 and diagnostic code 76.

If the SNARE does not have information indicating an SNPA via which the required Network Connection could be established, then it shall clear the call without User Data, with cause 0 and diagnostic code 232.

11.3 Assign Address by SNARE

A SNARE maintaining the appropriate subnetwork configuration information acts on the receipt of an ERA PDU followed by an ENC PDU, by determining a NET for assignment to the End System that originated the ERA PDU. SNAREs that do not support the address administration option discard ERA PDUs.

NOTE — The way in which a SNARE determines NETs according to this function is not specified. The SNARE may use any algorithm that ensures unambiguous NET assignment. That is, no NET may be assigned to more than one SNPA. The SNARE may assign the same NET if requested from the same subnetwork on separate occasions. For example, the SNARE may construct a NET based on the ERA originator's source SNPA address and local information, or maintain a manually administered database from which NET are selected according to some locally specified criterion. If more than one SNARE on a given subnetwork supports the address administration option, they must coordinate their NET assignment algorithms to ensure that all NETs are unambiguous. Such procedures would be out of the scope of this standard. For illustrative purposes, however, a static algorithm for address distribution could be one in which each SNARE participating in address administration would be assigned a range of NETs to distribute.

The SNARE constructs a SAA PDU, placing the newly determined NET in the appropriate field, and including an address holding time (AHT) parameter, which represents the amount of time that the End System may continue to use it. The SAA PDU, followed by an SRN PDU is forwarded to the ES. The NET has the structure and semantics of an NSAP address in which the last octet (binary DSP syntax) or two digits (decimal DSP syntax) is "zero" (See 8.5.2). The AHT should be much larger than the value indicated in the Notification Required parameter. (See 8.1.3.)

The SNARE shall not record the configuration for this End System as part of the "Assign Address" function, since the End System is not *required* to use the assigned NET as a Network address. The End System configuration is recorded only via the "record configuration" function described in 11.1.

12 Structure and Encoding of PDUs

12.1 Parameters

PDUs shall contain at least the following parameters as ordered:

- the Network Layer Protocol Identifier parameter;
- the Version Number parameter; and
- the PDU Type parameter.

All the other parameters listed appear in some PDUs only, as shown in 12.2.

12.1.1 Network Layer Protocol Identifier

The value of this parameter shall be 1000 1010.

This parameter identifies this Network Layer protocol as ISO/IEC 10030.

12.1.2 Version Number

The value of this parameter is 0000 0001. This identifies a standard version of ISO/IEC 10030.

12.1.3 PDU Type

The PDU Type parameter identifies the type of the protocol data unit. Allowed values are given in Table 1.

Table 1 — Valid PDU Types

PDU Types	Bits							
	8	7	6	5	4	3	2	1
ECQ PDU	0	0	0	0	0	0	0	1
ENC PDU	0	0	0	0	0	0	1	0
ERA PDU	0	0	0	0	0	1	0	1
ESC PDU	0	0	0	0	0	0	1	1
ESH PDU	0	0	0	0	0	1	0	0
RD PDU	0	0	0	0	1	0	0	0
SAA PDU	0	0	0	1	0	0	1	0
SCC PDU	0	0	0	0	1	0	0	1
SCR PDU	0	0	0	0	1	0	1	0
SHL PDU	0	0	0	1	0	0	0	0
SNC PDU	0	0	0	0	1	0	1	1
SRN PDU	0	0	0	0	1	1	0	0
SRH PDU	0	0	0	1	0	0	0	1

All other PDU Type values are reserved.

12.1.4 Network Address

In an ESH PDU this specifies a Network Address which is being notified as present and accessible in the ES. In an ECQ PDU it specifies the Network Address for which information is to be collected. In SCR and SCC PDUs it specifies the Network Address for which information is being supplied.

In the SAA PDU it specifies the Net being assigned to the ES that originated the request for a NET.

The Network Address parameter is encoded as shown in Figure 1.

	Octet
Network Address Length Indicator (e.g., *k*)	*j*
Network Address Parameter Value	*j*+1 *j*+*k*

Figure 1 — Network Address Parameter

The contents of this field shall be encoded according to the preferred binary encoding defined in ISO/IEC 8348.

12.1.5 SNPA Address

In SCR and RD PDUs, this specifies an SNPA address which may be used to reach the required Network Address.

The SNPA Address parameter is encoded as shown in Figure 2.

		Octet
Type	SNPA Address Length Indicator (e.g., *k*)	*j*
SNPA Address Parameter Value		*j*+1 *j*+*k*

Figure 2 — SNPA Address Parameter

The Type field consists of 2 bits indicating the encoding format of the SNPA. It takes on the following values:

00 Encoding per this International Standard
01 Reserved
10 Reserved
11 Local — For transitional use only

When the Type field is 00, the next 6 bits are the length of the SNPA Address Parameter Value. The following standard encodings are defined:

a) When the SNPA address is carried in the subnetwork access protocol as a sequence of whole octets, that sequence of octets is the value of the SNPA Address Parameter Value.

NOTE 1 — This includes, for example, ISO 8802 MAC addresses which will be encoded as a sequence of six octets according to the hexadecimal representation of MAC addresses specified in ISO/IEC 10039. Also included are cases where IA5 encoding is used.

b) When the SNPA address is carried in the subnetwork access protocol as a sequence of semi-octets using BCD encoding, that sequence of semi-octets is encoded in the SNPA Address Parameter Value field, and if it is an odd number of semi-octets, a final semi-octet containing the value 1111 is added at the end.

NOTE 2 — The values in items (a) and (b) are chosen to match those believed to be commonly used in SNPA fields of ISO 9542, with a view to the same specification being adopted by that standard.

12.1.6 QOS

In an SCR PDU, this specifies the range of QOS over which the indicated SNPA is applicable. In an ESH PDU, this specifies the range of QOS that can be supported by the identified End System on the specified SNPA.

Each QOS parameter is encoded as shown in Figure 3.

	Octet
Parameter Code	j
Parameter Length	$j+1$
Parameter Value	$j+2$ $j+k+1$

Figure 3 — Encoding of QOS Parameters

The *parameter code field* is coded in binary and, without extensions, provides a maximum of 255 different parameters. A parameter code of 255 (binary 1111 1111) is reserved for possible future extensions.

The *parameter length field* indicates the length, in octets, of the parameter value field. The length is indicated by a positive binary number, *k*, with a theoretical maximum value of 254. The practical maximum value of *k* is lower, and for each succeeding parameter the maximum value of *k* decreases.

The *parameter value field* contains the value of the parameter identified in the parameter code field.

12.1.6.1 Throughput

When present, the Throughput QOS parameter indicates the range of throughput values applicable via the specified path.

Parameter Code: 0000 0001

Parameter Length: One (1) octet.

Parameter Value: The four (4) most significant bits specify the maximum throughput according to the encoding specified in Table 18 of ISO/IEC 8208, and the four (4) least significant bits specify the minimum throughput according to the encoding specified in Table 18 cf ISO/IEC 8208.

12.1.6.2 Transit Delay

When present, the Transit Delay QOS parameter indicates the maximum and minimum transit delay values to be expected via the specified path.

Parameter Code 0000 0010

Parameter Length: Four (4) octets.

Parameter Value: The first two (2) octets specify an integral number of seconds indicating the maximum transit delay to be expected, and the second two (2) octets specify an integral number of seconds indicating the minimum transit delay to be expected.

12.1.6.3 Priority

When present, the Priority QOS parameter indicates the maximum and minimum values for the priority of data on the connection, the priority to gain a connection, and the priority to keep a connection, respectively, to be expected via the specified path.

Parameter Code: 0000 0011

Parameter Length: Six (6) octets.

Parameter Value: The first three (3) specify the maximum value for the priority of data on the connection, the priority to gain a connection, and priority to keep a connection, respectively. The following three (3) octets specify the minimum value for the priority of data on the connection, the priority to gain a connection, and the priority to keep a connection, respectively.

12.1.6.4 Protection

When present, the Protection QOS parameter indicates the maximum and minimum protection levels to be expected via the specified path.

Parameter Code: 0000 0100

Parameter Length: Variable.

Parameter Value: Bits 8 and 7 of the first octet specify the protection format code where:

00	Reserved
01	Source-address specific
10	Destination-address specific
11	Globally unique

The remaining 6 bits are reserved and must be set to zero (0).

The second octet specifies the length *p*, in octets, of the maximum protection level to be expected. The actual value of the maximum protection level is placed in the following *p* octets.

The *p+2* octet specifies the length *q*, in octets, of the minimum protection level to be expected. The actual value of the minimum protection level is placed in the following *q* octets.

12.1.7 Holding Time

In SCR and RD PDUs, this is a two (2) octet parameter that specifies an integral number of seconds for which the conveyed information is valid. The binary value 0000 0000 0000 0000 indicates that there is no time limit imposed.

12.1.8 Address Mask

When present in SCR and RD PDUs, this field contains an Address Mask for use as specified in 10.1.

The Address Mask parameter is encoded as follows:

Parameter Code:	1110 0001
Parameter Length:	Variable, up to 20 octets.
Parameter Value:	A comparison mask of octets to be aligned with the Destination Address.

12.1.9 SNPA Mask

When present in SCR and RD PDUs, this field contains an SNPA Mask for use as specified in 10.2.

The SNPA Mask parameter is encoded as follows:

Parameter Code:	1110 0010
Parameter Length:	Variable.
Parameter Value:	A comparison mask of octets to be aligned with the Destination Address.

12.1.10 Query Limit

In SCC PDUs, this field specifies whether the system (ES or IS) is allowed to request Configuration Information about another Network Address, or whether no more requests are allowed for the existing connection.

The Query Limit parameter is encoded as a single octet where the binary value 0000 0000 indicates that no more queries are allowed, and the binary value 0000 0001 indicates that the system (ES or IS) is allowed another query, if it wishes.

12.1.11 Request Time

In SNC PDUs, this parameter indicates the time which the SNARE will allow between requests from the system (ES or IS). The binary value 0000 0000 indicates that no time limit is imposed.

The Request Time parameter is encoded as a single octet that specifies an integral number of seconds.

12.1.12 Notification Required

In SRN PDUs, this parameter indicates the time interval that it is suggested the ES should wait prior to notifying the SNARE again.

The Notification Required parameter is a two (2) octet parameter that specifies an integral number of seconds as the time interval. The binary value 0000 0000 0000 0000 indicates that notification is not required. The binary value 1111 1111 1111 1111 indicates that no specific value is recommended.

12.1.13 Address Holding Time

In SAA PDUs, this is a two-octet parameter that specifies an integral number of seconds for which the conveyed NET is valid.

12.2 PDU Structure

All Protocol Data Units shall contain an integral number of octets. The octets in a PDU are numbered in increasing order starting from one (1). The bits in an octet are numbered from one (1) to eight (8), where bit one (1) is the low-order bit.

When consecutive octets are used to represent a binary number, the lower octet number has the most significant value.

NOTE — When the encoding of a PDU is represented using a diagram in this section, the following representation is used:

- octets are shown with the lowest numbered octet to the top, higher number octets being further to the bottom;
- within an octet, bits are shown with bit eight (8) to the left and bit one (1) to the right.

12.2.1 ECQ PDU Structure

The ECQ PDU is formatted as shown in Figure 4.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Network Address Length Indicator	4
Network Address	5 *k–1*

Figure 4 — ECQ PDU Structure

12.2.2 ENC PDU Structure

The ENC PDU is formatted as shown in Figure 5.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3

Figure 5 — ENC PDU Structure

12.2.3 ESC PDU Structure

The ESC PDU is formatted as shown in Figure 6.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3

Figure 6 — ESC PDU Structure

12.2.4 ESH PDU Structure

The ESH PDU is formatted as shown in Figure 7.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Network Address Length Indicator	4
Network Address	5 *k*–*1*
QOS	*k* *k*+*m*

Figure 7 — ESH PDU Structure

12.2.5 RD PDU Structure

The RD PDU is formatted as shown in Figure 8.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Holding Time	4 5
Type | SNPA Address Length Indicator	6
SNPA Address Parameter Value	7 *k*–*1*
Address Mask Parameter	*k* *m*–*1*
SNPA Mask Parameter	*m* *n*–*1*

Figure 8 — RD PDU Structure

12.2.6 SCC PDU Structure

The SCC PDU is formatted as shown in Figure 9.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Network Address Length Indicator	4
Network Address	5 *k*–*1*
Query Limit	*k*

Figure 9 — SCC PDU Structure

12.2.7 SCR PDU Structure

The SCR PDU is formatted as shown in Figure 10.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Holding Time	4 5
Network Address Length Indicator	6
Network Address	7 *k*–*1*
Type | SNPA Address Length Indicator	*k*
SNPA Address Parameter Value	*k*+*1* *m*–*1*
Address Mask Parameter	*m* *n*–*1*
SNPA Mask Parameter	*n* *p*–*1*
QOS	*p* *p*+*q*

Figure 10 — SCR PDU Structure

12.2.8 SNC PDU Structure

The SNC PDU is formatted as shown in Figure 11.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Request Time	4

Figure 11 — SNC PDU Structure

12.2.9 SRN PDU Structure

The SRN PDU is formatted as shown in Figure 12.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Notification Required	4 5

Figure 12 — SRN PDU Structure

12.2.10 ERA PDU Structure

The ERA PDU is formatted as shown in Figure 13.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3

Figure 13 — ERA PDU Structure

12.2.11 SAA PDU Structure

The SAA PDU is formatted as shown in Figure 14.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Address Holding Time (AHT)	4, 5
NET Length Indicator	6
NET Parameter Value	7 *j-1*

Figure 14 — SAA PDU Structure

Annex A
(normative)

Obtaining SNARE SNPA Addresses using LLC Type 1 Procedures

A.1 Introduction

This Annex described procedures which may be used in certain specific environments to enable End Systems and Intermediate Systems to discover SNARE SNPA addresses.

A.2 Broadcast Subnetworks using LLC Type 1

A broadcast subnetwork is a subnetwork whose physical characteristics are such that a single transmission of a NPDU may be received by all or a predefined group of systems attached to the subnetwork. This clause applies to broadcast subnetworks on which the LLC Type 1 procedures specified in ISO 8802-2 are used.

When operating the procedures described in this clause, the LSAP value allocated in ISO/IEC TR 10178 for use with ISO/IEC TR 9577 shall be used. The PDUs of this protocol include an IPI field enabling the protocol to be identified by the means described in ISO/IEC TR 9577.

A.2.1 SNARE LLC Type 1 Broadcast Procedures

A.2.1.1 Protocol Parameters

A.2.1.1.1 Broadcast Time

The broadcast time is a parameter which determines the time interval at which a SNARE which chooses to implement this procedure shall broadcast information to enable its SNPA to be discovered.

A.2.1.1.2 Retention Time

The Retention Time is a parameter which is included in transmitted PDUs, to indicate how long the information contained in them is valid.

A.2.1.2 Protocol Operation

A SNARE which is attached to an ISO 8802-2 LAN and which chooses to operate the SNARE broadcast procedures shall transmit a SHL PDU, formatted as specified in A.2.3, at intervals equal to the value of the Broadcast Time parameter. It shall transmit these PDUs using a DL-UNITDATA request, specifying a destination address whose value shall be one defined to mean, on that subnetwork "All CONS End Systems".

A.2.2 ES LLC Type 1 Broadcast Procedures

A system (ES or IS) which is attached to an ISO 8802-2 LAN and which chooses to operate the ES or IS LLC Type 1 broadcast procedures shall operate LLC Type 1 as specified in ISO 8802-2, and shall accept DL-UNITDATA indications whose destination address is a value defined to mean "All CONS End Systems" on the subnetwork.

If a DL-UNITDATA indication is received, the data contained in it shall be examined. If it does not contain a SHL PDU formatted as specified in A.2.3, it shall be ignored. If it does contain such a PDU, and if the system does not already have a record of a SNARE SNPA address, the system shall record the source address from which the DL-UNITDATA was received as a SNARE SNPA address, and shall associate with it the time contained in the Retention Time field.

If a valid SHL PDU is received when the system already has a record of the source address as a SNARE SNPA address, it shall update its record of the associated Retention Time to that contained in the received PDU.

If a valid SHL PDU is received when the system already has a record of a SNARE SNPA address but not of the one contained in the source address from the DL-UNITDATA indication, the system may record the SNPA and Retention Time as above, but need not to do so. If it does record it, it may discard any or all of the SNARE SNPA addresses it had already recorded.

The system shall discard any recorded SNARE SNPA address when the time elapsed since receipt of the last SHL PDU from that address reaches the associated retention time.

Furthermore, the system may examine the Notification Required field and determine whether or not notification is required.

A.2.3 SHL PDU Structure

The SHL PDU is formatted as shown in Figure A.1.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3
Notification Required	4 5
Retention Time	6 7

Figure A.1 — SHL PDU Structure

A.3 ES or IS LLC Type 1 Broadcast Procedure

These procedures are optional.

When operating the procedures described in this clause, the LSAP value allocated in ISO/IEC TR 10178 for use with ISO/IEC TR 9577 shall be used. The PDUs of this protocol include an IPI field enabling the protocol to be identified by the means described in ISO/IEC TR 9577.

A system (ES or IS) attached to an ISO 8202-2 LAN wishing to discover a SNARE SNPA address and which has not received a SHL PDU may transmit a SRH PDU formatted as specified in A.3.1. It shall transmit this PDU using a DL-UNITDATA request specifying a destination address whose value shall be defined to mean, on that subnetwork, "All CONS SNAREs."

A SNARE which is attached to an ISO 8802-2 LAN and which chooses to operate the SNARE broadcast procedures shall accept DL-UNITDATA indications whose destination address is defined to mean "All CONS SNAREs" on the subnetwork.

If a DL_UNITDATA indication is received, the data contained in it shall be examined. If it does not contain a SRH PDU formatted as specified in A.3.1 it shall be ignored. If it does contain such a PDU, the SNARE shall transmit a SHL PDU as specified in A.2.

NOTE — This transmission of the SHL PDU by the SNARE should be considered as an extra transmission and, therefore, should not cause the resetting of the normal timer for the SHL PDUs.

A.3.1 SRH PDU Structure

The SRH PDU is formatted as shown in Figure A.2.

	Octet
Network Layer Protocol Identifier	1
Version Number	2
PDU Type	3

Figure A.2 — SRH PDU Structure

Annex B
(normative)

Protocol Implementation Conformance Statement Proforma[2]

B.1 Introduction

The supplier of a protocol implementation which is claimed to conform to ISO/IEC 10030 : 1990 shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use:

- — by the protocol implementor, as a check-list to reduce the risk of failure to conform to the standard through oversight;
- — by the supplier and acquirer – or potential acquirer – of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- — by the user – or potential user – of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs);
- — by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

B.2 Notations

The following notations are used in this PICS proforma:

M	mandatory
O	optional
O.<n>	optional, but support of at least one of the group of options labelled by the same numeral <n> is required
X	prohibited
<pred>:	conditional-item symbol, including predicate identification (see B.3.4.2).
¬	Logical negation, applied to a conditional item's predicate (see B.3.4.2).

B.3 Instructions for completing the PICS proforma

B.3.1.General structure of the PICS proforma

The first part of the PICS proforma — Implementation Identification and Protocol Summary — is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PICS proforma is a fixed-format questionnaire. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No), or by entering a value or a set or range of values. (Note that there are some items where two or more choices from a set of possible answers can apply; all relevant choices are to be marked.)

Each item is identified by an item reference in the first column; the second column contains the question to be answered; the third column the reference or references to the material that specifies the item in ISO/IEC 10030. The remaining columns record the status of the item — whether support is mandatory, optional, prohibited or conditional — and provide the space for the answers; see also B.3.2 below. (Status is sometimes indicated by other means than a separate Status column: for example, where the same status applies to a whole group of items, as in B.3.4.2.)

A supplier may also provide — or be required to provide — further information, categorized as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled A<i> or X<i>, respectively, for cross-referencing purposes, where <i> is any unambiguous identification for the item (e.g., simply a numeral); there are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformance Statement for the implementation in question.

[2] **Copyright release for PICS proformas**

Users of this International Standard may freely reproduce the PICS proforma in this annex so that it can be used for the intended purpose and may further publish the completed PICS.

NOTE 1 — Where an implementation is capable of being configured in more than one way, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case this makes for easier and clearer presentation of the information.

B.3.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations or a brief rationale — based perhaps upon specific applications needs — for the exclusion of features which, although optional, are nonetheless commonly present in implementations of the ISO/IEC 10030.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

B.3.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this; instead, the supplier is required to write into the Support column an X<i> reference to an item of Exception Information and to provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to ISO/IEC 10030 : 1990.

NOTE 2 — A possible reason for the situation described above is that a defect in the standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

B.3.4 Conditional status

B.3.4.1 Conditional items

The PICS proforma contains a number of conditional items. These are items for which the status — mandatory, optional or prohibited — that applies is dependent upon whether or not certain other items are supported or upon the values supported for other items.

In many cases, whether or not the item applies at all is conditional in this way, as well as the status when the item does apply.

Where a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the "Not Applicable" answer is selected. Otherwise, individual conditional items are indicated by one or more conditional symbols (on separate lines) in the Status column.

A conditional symbol is of the form "<pred>: <s>" where "<pred>" is a predicate as described in B.3.4.2 below, and "<s>" is one of the status symbols **M**, **O**, **O**.<n> or **X**.

If the value of the predicate in any line of a conditional item is true (see B.3.4.2), the conditional item is applicable, and its status is that indicated by the status symbol following the predicate: the answer column is to be marked in the usual way. If the value of a predicate is false, the Not Applicable (N/A) answer is to be marked in the relevant line. (Each line in a multi-line conditional item is to be marked; at most one line will require an answer other than N/A.)

B.3.4.2 Predicates

A predicate is one of the following:

a) an item-reference for an item in the PICS proforma: the value of the predicate is true if the item is marked as supported, and is false otherwise; or

b) a predicate name, for a predicate defined elsewhere in the PICS proforma (usually in the Major Capabilities section or at the end of the section containing the conditional item): see below; or

c) the logical negation symbol "¬" prefixed to an item-reference or predicate name: the value of the predicate is true if the value of the predicate formed by omitting the "¬" symbol is false, and viceversa.

The definition for a predicate name is one of the following:

i) an item-reference, evaluated as at (a) above; or

ii) a relation containing a comparison operator (=, <, etc) with at least one of its operands being an item-reference for an item taking numerical values as its answer: the predicate is true if the relation holds when each item-reference is replaced by the value entered in the Support column as answer to the item referred to; or

iii) a Boolean expression constructed by combining simple predicates, as at (i) and (ii), using the Boolean operators AND, OR and NOT, and parentheses, in the usual way: the value of such a predicate is true if the Boolean expression evaluates to true when the simple predicates are interpreted as described above.

Each item whose reference is used in a predicate or predicate definition is indicated by an asterisk in the Item column.

B.4 Implementation Identification

Supplier	
Contact point for queries about this PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification (e.g., Name(s) and Version(s) for machines and/or operating systems, System Name(s))	

NOTES — 3 Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

4 The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (using, e.g., Type, Series, Model).

B.5 Protocol Summary: ISO/IEC 10030:1990

Identification of Protocol Specification	
Identification of Amendments and Corrigenda to this PICS proforma which have been completed as part of this PICS.	
Protocol Version(s) Supported	
Have any Exception items been required (see B.3.3) No □ Yes □ (The answer Yes means that the implementation does not conform to ISO/IEC 10030 : 1990)	

Date of Statement	

B.6 10030 System Implementation Identification

Item	Protocol Feature	References	Status	Support		
ES*	End System Implementation	Clauses 8, 9	O.1		Yes □	No □
SNARE*	SNARE Implementation	Clause 11	O.1		Yes □	No □
IS*	IS Implementation	Clauses 8, 0	O	N/A □	Yes □	No □

PDUs Implemented, End System (continued)

	Parameter Ranges			
RespT	If configuration information is supported, what range of values can be set for the Response Timer?	8.1.1	EsCl:M	From: seconds To: seconds by increment of†: (other - specify)†: with a tolerance of:
NtRtT	If configuration information is supported, what range of values can be set for the Notification Retry Timer?	8.1.2	EsCl:M	From: seconds To: seconds by increment of†: (other - specify)†: with a tolerance of:

† - delete if not applicable