PUBLICLY
AVAILABLE
SPECIFICATION

IEC
PAS 62412

First edition
2005-08

Real-time Ethernet P-NET on IP specification

Reference number
IEC/PAS 62412:2005(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

PUBLICLY AVAILABLE SPECIFICATION

IEC PAS 62412

First edition
2005-08

Real-time Ethernet P-NET on IP specification

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE U

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

Real-time Ethernet P-NET on IP specification

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

A PAS is a technical specification not fulfilling the requirements for a standard but made available to the public.

IEC-PAS 62412 has been processed by subcommittee 65C: Digital communications, of IEC technical committee 65: Industrial-process measurement and control.

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
65C/360/NP	65C/376/RVN

Following publication of this PAS, the technical committee or subcommittee concerned will transform it into an International Standard.

It is intended that the content of this PAS will be incorporated in the future new edition of the various parts of IEC 61158 series according to the structure of this series.

This PAS shall remain valid for an initial maximum period of three years starting from 2005-08. The validity may be extended for a single three-year period, following which it shall be revised to become another type of normative document or shall be withdrawn.

INTRODUCTION

The P-NET on IP specification is designed for use in an IP-environment. P-NET on IP enables use of P-NET (IEC 61158, type 4) real-time communication wrapped into UDP/IP packages.

P-NET packages can be routed through IP-networks in exactly the same way as they can be routed through non-IP-networks. Routing can be through any type of P-NET network and in any order.

Nodes on an IP-network are addressed with two P-NET Route elements, but this is entirely handled by the IP-nodes. This means that any P-NET client (master) can access servers on an IP-network without knowing anything about IP-addresses.

Real-time Ethernet P-NET on IP specification

1 Scope and object

This PAS consists of paragraphs that are meant to be additional to the definitions and specifications, which are already found in the IEC 61158 series. Following each heading, there will be a reference to which paragraph must be inserted or replaced within the relevant IEC 61158 series.

After the modifications to IEC 61158 series a few descriptions explain how to perform address conversions and handle dynamic clients.

NOTE These descriptions are more implementation specific and will not be included in the normative parts of the new standard.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61158-2:2003, *Digital data communications for measurement and control – Fieldbus for use in industrial control systems – Part 2: Physical layer specification and service definition*

IEC 61158-4:2003, *Digital data communications for measurement and control – Fieldbus for use in industrial control systems – Part 4: Data link protocol specification*

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

RFC 768 (UDP, User Datagram Protocol)

RFC 791 (IP, Internet Protocol)

3 Conventions

This PAS specifies paragraphs that shall either be replaced or added to the IEC 61158 series.

Paragraphs that shall be replaced are indicated with the paragraph number(s) in question as reference and begin and end with the lines as shown:

---------------------------------- Replace begin --------------------------------

modified text

---------------------------------- Replace end --------------------------------

Paragraphs that shall be added are indicated with first paragraph number(s) to add and begin and end with the lines as shown:

---------------------------------- Addition begin --------------------------------

new text

---------------------------------- Addition end --------------------------------

4 61158-2 Physical Layer specification

----------------------------------- Addition begin --------------------------------

ISO/IEC 8802-3 shall be used.

4.1 OSI Data Link Layer

4.1.1 MAC sublayer

ISO/IEC 8802-3 shall be used.

4.1.2 LLC sublayer

ISO/IEC 8802-3 shall be used.

4.2 OSI Network layer

Internet standard RFC 791 (IP, Internet protocol) and its amendments and successors shall be used.

4.3 OSI Transport layer

Internet standard RFC 768 (UDP, User Datagram Protocol) and its amendments and successors and the Data Link Layer protocol specification within this document shall be used.

----------------------------------- Addition end --------------------------------

5 61158-4 Data Link Layer protocol specification

5.1 Terms and definitions

5.1.1 P-NET-route

The following term is to be replaced in 3.7.8, Type 4: Additional terms and definitions:

---------------------------------- Replace begin --------------------------------

A P-NET route holds a sequence of P-NET-route-elements.

NOTE A P-NET-route is defined as an encoded DL-route, with one of the formats used when transmitting the DLPDU on the Link. The P-NET-route format can be Simple, Extended, Complex, Immediate or IP.

---------------------------------- Replace end --------------------------------

5.2 Additions to terms and definitions

The following terms are to be added in paragraph 3.7, Type 4: Additional terms and definitions:

---------------------------------- Addition begin --------------------------------

5.2.1 IPNetTable

An IpNetTable defines the relation between IPNetID, IP address, UPD port number and Router NodeAddress, where IPNetID is used as index in the table.

5.2.2 IPNetID

IPNetID identifies a unique IP network. The value of IPNetID shall be in the range of 0-127. The values 0, 126 and 127 are reserved for special purposes.

NOTE An IPNetID is translated into an IP-address and a UPD port number.

5.2.3 UDP port number

A Server can receive requests on two different UPD port numbers: Normal UDP port and Secure UDP port. UDP port number shall be 34378 for Normal UDP port. UDP port number shall be 34379 for Secure UDP port.

NOTE These UDP port numbers are registered with the IANA (Internet Assigned Numbers Authority)

5.2.4 Nettype

An IP network is of a certain type, a Nettype that can be “Unused”, “IP Range net” or “UDP Range net”.

5.2.5 IP Range net

An IP Range net is used for local access, where nodes can be accessed directly on the same subnet as the client, or through a local Router where the subnets are configured in the local Router.

5.2.6 UDP Range net

A UDP Range net is used for remote access, where a node cannot be accessed directly on the same subnet as the client. The IPNetTable holds a NAT Router IP address and access to the node is obtained through this NAT Router.

NOTE The NAT Router shall hold a table that translates the UDP port number to the actual server node IP address and UDP port number.

---------------------------------- Addition end --------------------------------

5.3 Type 4: Additional symbols and abbreviations

5.3.1 Constants, variables, counters and queues

The following paragraph shall be added to paragraph 4.5.1, Type 4: Additional symbols and abbreviations:

---------------------------------- Addition begin --------------------------------

5.3.1.1 **IPNetTable** **Table to convert IPNetID to IP-addresses**

---------------------------------- Addition end --------------------------------

5.4 Type 4: Data Link Protocol Definition

5.4.1.1 Half-duplex and full duplex

The following paragraphs are to be replaced in paragraph 24.1.2.2, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

Unless otherwise stated, the PhL is assumed to support half-duplex transfer. However, a PhL supporting full duplex is allowed.

Full duplex systems allow up to 125 DLEs on a Link, all of Normal class. Each DLE is allowed to transmit immediately, that is, there is no Link Access system. DLEs supporting full duplex PhEs have separate state machines for receive and transmit, as illustrated in Figure 91 to Figure 92.

In full duplex systems, as well Confirmed as Unconfirmed DLPDUs are unacknowledged.

PhLs supporting full duplex shall not provide Link-Idle indications.

---------------------------------- Replace end --------------------------------

5.4.1.2 Responder role, receiving a DLPDU from the PhE

The following paragraphs are to be replaced in 24.1.2.5, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

This action includes a sequence of steps, as described in the following.

a) Receive a single PhIDU specifying START-OF-ACTIVITY. This PhIDU holds a Node address. This address is examined to determine, whether its value is equal to the Node-address of this DLE, or equal to the Broadcast-Node-address (BNA) or the Service-Node-Address (SNA). If not, ignore this sequence and wait for the next PhIDU specifying START-OF-ACTIVITY.

b) Receive a sequence of PhIDUs from the PhE, specifying DATA, concatenate them to a received DLPDU, compute a frame check sequence over the entire sequence of received data as specified by the value of V(FCM) - FrameCheckMethod, and, if necessary, check for the proper value. If the value is not correct, ignore the DLPDU and wait for the next PhIDU specifying START-OF-ACTIVITY.

c) Convert the received DLPDU into its DL-protocol control information and data components.

d) Generate a DLS-user indication primitive.

e) If the DLPDU received from the remote DLE is of type Confirmed, and the receipt of the DLPDU must be acknowledged, according to the rules described in 24.1.2.1, wait for a request or response primitive from the local DLS-user.

If no request or response primitive is issued from the local DLS-user in time (before a PhIDU specifying "LINK-IDLE for 30 bit periods" is received from the PhE), generate and immediately send an Acknowledge DLPDU. This DLPDU must specify "Wait" if this DLE is of Simple class, and "Response Comes Later / Acknowledge" ("RCL/ACK") if this DLE is of Normal class.

If a response primitive is issued from the local DLS-user in time, generate and immediately send an Acknowledge DLPDU, specifying "Wait" if this DLE is of Simple class, and "RCL/ACK" if this DLE is of Normal class.

If a request primitive is issued from the local DLS-user in time, convert it into an Immediate-reply DLPDU and send it immediately. After sending, wait for the next PhIDU specifying START-OF-ACTIVITY.

f) If the DLPDU received from the remote DLE is of type Confirmed, and the receipt of the DLPDU shall not be acknowledged, wait for the next PhIDU specifying START-OF-ACTIVITY.

g) If the DLPDU received from the remote DLE is of type Unconfirmed, and the receipt of the DLPDU must be acknowledged, according to the rules described in 24.1.2.1, generate and immediately send an Acknowledge DLPDU, specifying RCL/ACK. After sending, wait for the next PhIDU specifying START-OF-ACTIVITY.

h) If the DLPDU received from the remote DLE is of type Unconfirmed, and the receipt of the DLPDU shall not be acknowledged, wait for the next PhIDU specifying START-OF-ACTIVITY.

---------------------------------- Replace end --------------------------------

5.4.2 PhIDU structure and encoding

The following paragraphs are to be replaced in 24.2.1, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

Each PhIDU consists of Ph-interface-control-information and in some cases one octet of Ph-interface-data (see 24.1.3). When the DLE transmits a DLPDU, it computes a frame check sequence for the DLPDU as specified in 24.2.2, concatenates the DLPDU and the frame check sequence, and transmits the concatenated pair as a sequence of PhIDUs as follows:

a) The DLE issues a single Ph-DATA request primitive with PhICI specifying START-OF-ACTIVITY-2 if sending from the queue, and specifying START-OF-ACTIVITY-11 if sending an Acknowledge or Immediate-reply DLPDU, or if re-transmitting because of missing acknowledge. The request primitive is accompanied by one octet holding the first octet from the DLPDU as Ph-interface-data. After that, the DLE awaits the consequent Ph-DATA confirm primitive.

b) The DLE issues a sequence of Ph-DATA request primitives with PhICI specifying DATA, each accompanied by one octet of the DLPDU as Ph-interface-data, from second to last octet of the DLPDU, and after each Ph-DATA request primitive awaits the consequent Ph-DATA confirm primitive.

c) If the value of V(FCM) - FrameCheckMethod - specifies reduced frame check, the DLE issues a single Ph-DATA request primitive with PhICI specifying DATA, accompanied by one octet holding the computed FCS as Ph-interface-data, and after the Ph-DATA request primitive awaits the consequent Ph-DATA confirm primitive. If the value of V(FCM) - FrameCheckMethod - specifies normal frame check, the DLE issues a sequence of Ph-DATA request primitives with PhICI specifying DATA, each accompanied by one octet of the FCS as Ph-interface-data, from first to last octet of the FCS, and after each Ph-DATA request primitive awaits the consequent Ph-DATA confirm primitive. If the value of V(FCM) - FrameCheckMethod - specifies None frame check, the transmission is finished.

d) The DLE issues a single Ph-DATA request primitive with PhICI specifying END-OF-ACTIVITY, and awaits the consequent Ph-DATA confirm primitive.

It is a task of the implementation to ensure that there are no idle periods between the octets of a transmitted DLPDU.

The DLE forms a received DLPDU by concatenating the sequence of octets received as Ph-interface-data of consecutive Ph-DATA indications, computing a frame check sequence for those received octets as specified in 24.2.2, and compares the received FCS value with the computed, as follows:

1) The DLE received a single Ph-DATA indication primitive with PhICI specifying START-OF-ACTIVITY, accompanied by one octet of the received DLPDU as Ph-interface-data, and initializes its computation of an FCS for the received DLPDU.

2) The DLE receives a sequence of Ph-DATA indication primitives with PhICI specifying DATA, each accompanied by one octet of the received DLPDU as Ph-interface-data, incrementally computes an FCS on the received octet, and concatenates all, or all except the last one or two as specified by V(FCM), of those received octets to form the received DLPDU. During reception, the DLE encodes the DLPDU being received to compute the number of octets forming the DLPDU.

3) When the DLE has received the last Ph-DATA indication, it compares the value(s) (if any – depending on frame check method) of the computed FCS to zero:

i) If the value(s) is (are) zero, then the DLE reports the reconstructed DLPDU as a correctly received DLPDU suitable for further analysis.

ii) If the value(s) is (are) not zero, the DLE ignores the received DLPDU, and performs no further actions related to the received DLPDU.

----------------------------------- Replace end --------------------------------

5.4.3 Frame check sequence

The following paragraphs are to be replaced in 24.2.2, Type 4: Data Link Protocol Definition:

----------------------------------- Replace begin --------------------------------

The value of the DLE local variable V(FCM) determines which frame check method to use.

The following frame check methods are defined: "Normal", "Reduced" and “None”.

----------------------------------- Replace end --------------------------------

5.5 Additions to Frame check sequence

The following paragraph is to be added after 24.2.2.2, Type 4: Data Link Protocol Definition:

---------------------------------- Addition begin --------------------------------

5.5.1.1 None frame check method

The "None" frame check method uses no frame check. This method is only used for IP networks. In this case the DLPDU is data within a frame on the IP network and the IP network specifies the frame check.

---------------------------------- Addition end --------------------------------

5.5.2 Common DLPDU structure, encoding and elements of procedure

The following paragraph is to be replaced in 24.2.3, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

Each DLPDU consists of a P-NET-route field, a Control-status field, a Data-field-format field, and for most DLPDUs a Data field. An FCS field (see 24.2.2), which is used to check the integrity of the received DLPDU can be appended before transmission, and removed after reception.

---------------------------------- Replace end --------------------------------

5.5.2.1 P-NET-route field

The following paragraphs are to be replaced in 24.2.3.1, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

The first field in each DLPDU is a P-NET-route field. The P-NET-route field holds a P-NET-route and consists of 2-30 octets, called P-NET-route-elements. Each P-NET-route-element is an octet, holding a 7-bit DL-route-element or Remaining-route-length, and a 1-bit Source/Destination designator. Five different P-NET-route field formats are defined: "Simple", "Extended", "Complex", "Immediate" and “IP”. The P-NET-route field format is indicated by the sequence of Source/Destination designators.

The Source/Destination designator is physically located as bit 8 in the octet. A value of "0" designates "Destination", and a value of "1" designates "Source".

---------------------------------- Replace end --------------------------------

5.6 Additions to P-NET-route field

The following paragraphs are to be added after 24.2.3.1.4, Type 4: Data Link Protocol Definition:

---------------------------------- Addition begin --------------------------------

5.6.1.1.1 IP P-NET-route format

P-NET-route fields of IP format consist of more than 2 destination P-NET-route-elements followed by 2 or more source P-NET-route-elements, as illustrated in Figure 1.

0	**Destination address**
0	**Destination address**
0	**Remaining-route-length**
1	**Source address**
1	**Source address**

Figure 1 – IP P-NET-route format

The first Destination address is the IPNetID, which identifies the IP net to receive the DLPDU. The second Destination address identifies the DLE to receive the DLPDU. The remaining Destination addresses are used by the DLS-user. The third P-NET-route-element holds the number of P-NET-route-elements following the third P-NET-route-element. The first Source address identifies the transmitting IP net. The second Source address identifies the transmitting DLE. The remaining source addresses (maybe except the last) are used by the DLS-user.

Complex routes are used when sending Confirmed or Unconfirmed DLPDUs holding requests or Unconfirmed DLPDUs holding responses to DLEs of normal class. The DLPDU is Unconfirmed if the value of the last Source address equals 0, or the value of one of the Destination addresses equals BNA.

---------------------------------- Addition end --------------------------------

5.7 DLPDU-specific structure, encoding and elements of procedure

The following paragraphs are to be replaced in 24.3, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

Table 1 – Summary structure of DLPDUs

DLPDU type	P-NET-route format	Destination Node-addresses	Last Source address	Control-status	Data size	Data
Confirmed	Simple	≠ BNA	≠ 0	Any	> 2	user data
Confirmed	Extended	≠ BNA	≠ 0	Any	> 2	user data
Confirmed	Complex	≠ BNA	≠ 0	Any	> 2	user data
Confirmed	IP	≠ BNA	≠ 0	Any	> 2	user data
Unconfirmed	Simple	= BNA	≠ 0	Any	> 2	user data
Unconfirmed	Extended	= BNA	≠ 0	Any	> 2	user data
Unconfirmed	Complex	= BNA	≠ 0	Any	> 2	user data
Unconfirmed	Complex	≠ BNA	= 0	Any	≥ 0	user data
Unconfirmed	IP	= BNA	≠ 0	Any	> 2	user data
Unconfirmed	IP	≠ BNA	= 0	Any	≥ 0	user data
Immediate-reply	Immediate	Any	Any	Any	≥ 0	user data
Acknowledge	Immediate	Any	Any	= Wait / RCL/ACK	= 0	-

The DLPDU type is indicated by the P-NET-route format, the contents of the Destination Node-addresses in the P-NET-route, the contents of the last Source address in the P-NET-route, the contents of Control-status, and the contents of the data size subfield of Data-field-format, as shown in Table 1.

When the value in the column Destination Node-addresses is "≠ BNA" it means, that none of the Node-addresses in the P-NET-route field are = BNA. When the value in the column Destination Node-addresses is "= BNA" it means, that at least one of the Node-addresses in the P-NET-route field is = BNA.

---------------------------------- Replace end --------------------------------

5.7.1.1 Structure of Confirmed DLPDUs

The following paragraphs are to be replaced in 24.3.1.1, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

The Structure of Confirmed DLPDUs is shown in Table 2.

Table 2 – Structure of Confirmed DLPDUs

P-NET-route format	Destination Node-addresses	Last Source address	Control-status	Data size	Data
Simple	≠ BNA	≠ 0	DLS-user info	> 2	user data
Extended	≠ BNA	≠ 0	DLS-user info	> 2	user data
Complex	≠ BNA	≠ 0	DLS-user info	> 2	user data
IP	≠ BNA	≠ 0	DLS-user info	> 2	user data

---------------------------------- Replace end --------------------------------

5.7.1.2 Sending the Confirmed DLPDU

The following paragraphs are to be replaced in 24.3.1.2, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

A Confirmed DLPDU is selected for transmission on the Link when the DLPDU is the first in the queue, and the DLE receives the Virtual Link-access token (except for Full duplex). Once selected, the DLPDU is removed from the queue, and transmission of the DLPDU commences. If the receipt of the DLPDU must be acknowledged, according to the rules described in 24.1.2.1, the DLPDU shall be transmitted until either

a) an Immediate-reply DLPDU is received, or

b) an Acknowledge DLPDU is received, or

c) the original transmission and the permitted maximum number or transmission retries, V(MRC), have all failed to elicit one of the permissible reply DLPDUs.

In addition to the above, the transmitting DLE shall act according to the rules described in 24.1.2.7.

---------------------------------- Replace end --------------------------------

5.7.1.3 Structure of Unconfirmed DLPDUs

The following paragraphs are to be replaced in 24.3.2.1, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

The Structure of Unconfirmed DLPDUs is shown in Table 3.

Table 3 – Structure of Unconfirmed DLPDUs

P-NET-route format	Destination Node-addresses	Last Source Node-address	Control-status	Data size	Data
Simple	= BNA	≠ 0	DLS-user info	> 2	user data
Extended	= BNA	≠ 0	DLS-user info	> 2	user data
Complex	= BNA	≠ 0	DLS-user info	> 2	user data
Complex	≠ BNA	= 0	DLS-user info	≥ 0	user data
IP	= BNA	≠ 0	DLS-user info	> 2	user data
IP	≠ BNA	= 0	DLS-user info	≥ 0	user data

---------------------------------- Replace end --------------------------------

5.7.1.4 Sending the Unconfirmed DLPDU

The following paragraphs are to be replaced in 24.3.2.2, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

An unconfirmed DLPDU is selected for transmission on the Link when the DLPDU is the first in the queue, and the DLE receives the Virtual Link-access token (except for Full duplex). Once selected, the DLPDU is removed from the queue, and transmission of the DLPDU commences. If the receipt of the DLPDU must be acknowledged, according to the rules described in 24.1.2.1, the DLPDU shall be transmitted until either

a) an Acknowledge DLPDU is received, or

b) the original transmission and the permitted maximum number or transmission retries, V(MRC), have all failed to elicit one of the permissible reply DLPDUs.

In addition to the above, the transmitting DLE shall act according to the rules described in 24.1.2.7.

---------------------------------- Replace end --------------------------------

5.7.1.5 Forming a Confirmed or Unconfirmed DLPDU

The following paragraphs are to be replaced in 24.4.1.2, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

The forming of a Confirmed or Unconfirmed DLPDU is described in the following.

The DLE's Node-address shall be inserted in front of all other addresses in the source DL-route.

Request P-NET-route generation encodes the resulting DL-route into a P-NET-route with Simple, Extended, Complex or IP format, and stores the result in the P-NET-route field of the DLPDU. Request P-NET-route generation is described in 24.5.1.

The user-specified Control-status parameter is stored in the Control-status (C-S) field of the DLPDU.

The user-specified Data-field-format parameter is stored in the Data-field-format (DFF) field of the DLPDU.

The user-specified Data unit (DLSDU) (the size of which is indicated in bit 1-6 of the Data-field-format field) is stored in the Data field of the DLPDU.

---------------------------------- Replace end --------------------------------

5.7.1.6 Parsing of a received Confirmed or Unconfirmed DLPDU

The following paragraphs are to be replaced in 24.4.4.1, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

The parsing of a received Confirmed or Unconfirmed DLPDU is described in the following.

DL-route generation generates Destination DL-route and Source DL-route from the received Simple, Extended, Complex or IP P-NET-route. DL-route generation is described in 24.5.2.

The value of Confirm is set to FALSE if the value of one of the addresses in the Destination DL-route is = BNA, or the value of the last address in the Source DL-route is = NCNA.

The first element of the Destination DL-route is removed.

The Control-status parameter shall be the Control-status (C-S) field of the DLPDU.

The Data-field-format parameter shall be the Data-field-format (DFF) field of the DLPDU.

The Data unit (DLSDU) parameter shall be the Data field of the DLPDU (the number of octets in DLSDU is indicated in bit 1-6 of the Data-field-format field).

---------------------------------- Replace end --------------------------------

5.7.2 Request P-NET-route generation

The following paragraphs are to be replaced in 24.5.1, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin --------------------------------

Request P-NET-route generation is performed by the DLE as a part of forming a DLPDU when it has received a DL-UNITDATA request primitive from the local DLS-user.

Request P-NET-route generation encodes the Destination DL-route and Source DL-route parameters into a P-NET-route of Simple, Extended, Complex or IP format.

Generally, a DL-route-element from the Destination DL-route is copied to a P-NET-route-element by copying the value of the DL-route-element to the address subfield of the P-NET-route-element, and setting the value of the Source/Destination designator to FALSE. A DL-route-element from the Source DL-route is copied to a P-NET-route-element by copying the value of the DL-route-element to the address subfield of the P-NET-route-element, and setting the value of the Source/Destination designator to TRUE.

Figure 2 illustrates the generation of the Source/Destination designator.

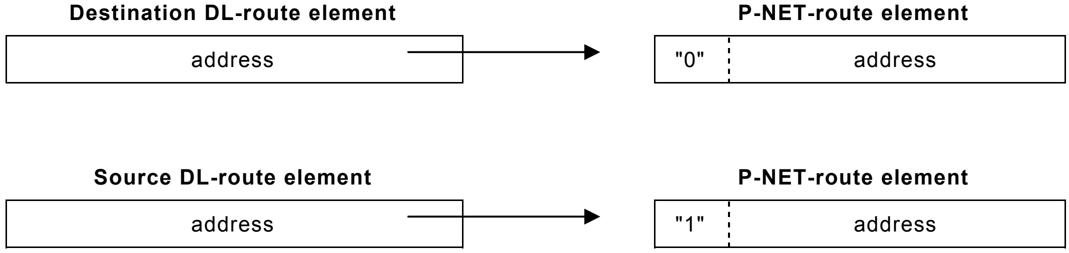

Figure 2 – Source / destination designator

The Destination DL-route is copied to the first elements of the P-NET-route, and the Source DL-route is copied to the succeeding elements.

One of three alternatives apply:

a) If the Destination DL-route holds only one element, the P-NET-route shall be of Simple format.

The first element of the P-NET-route shall be a copy of the first element of the Destination DL-route. The second octet of the P-NET-route shall be a copy of the first element of the Source DL-route. Figure 3 illustrates this.

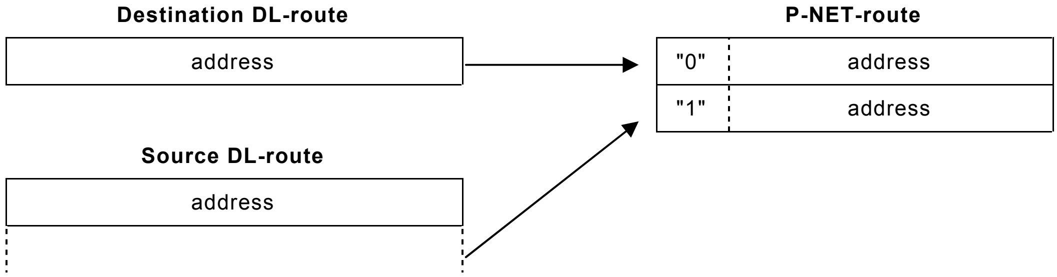

Figure 3 – Simple P-NET-route generation

b) If the Destination DL-route <u>and</u> the Source DL-route hold only two elements each, the P-NET-route shall be of Extended format.

The first two elements of the P-NET-route shall be a copy of the two elements in the Destination DL-route. The next two elements of the P-NET-route shall be a copy of the two elements in the Source DL-route. Figure 4 illustrates this.

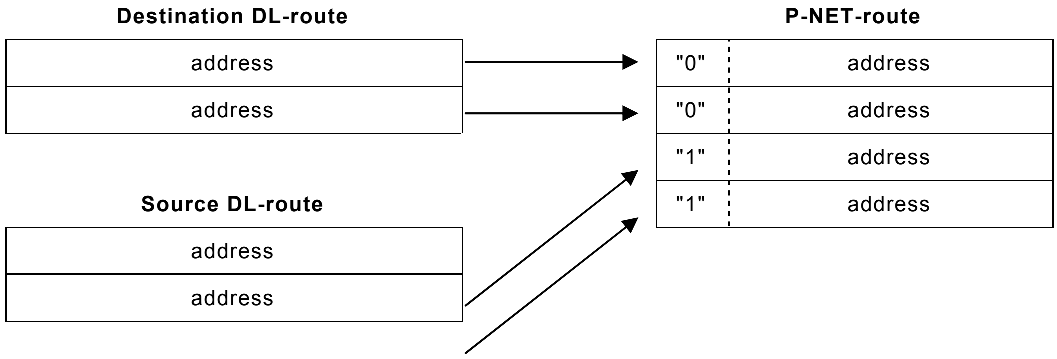

Figure 4 – Extended P-NET-route generation

c) If the Destination DL-route holds at least two elements, and the total DL-route (the combination of Destination and Source DL-route) holds more than four elements, the P-NET-route shall be of Complex or IP format.

The first two elements of the P-NET-route shall be a copy of the first two elements in the Destination DL-route. The third element shall be the total number of elements in the DL-route minus two. A copy of the remaining elements of the Destination DL-route (if any) shall follow the third element of the P-NET-route. They shall be followed by all of the elements of the Source DL-route. Figure 5 illustrates this.

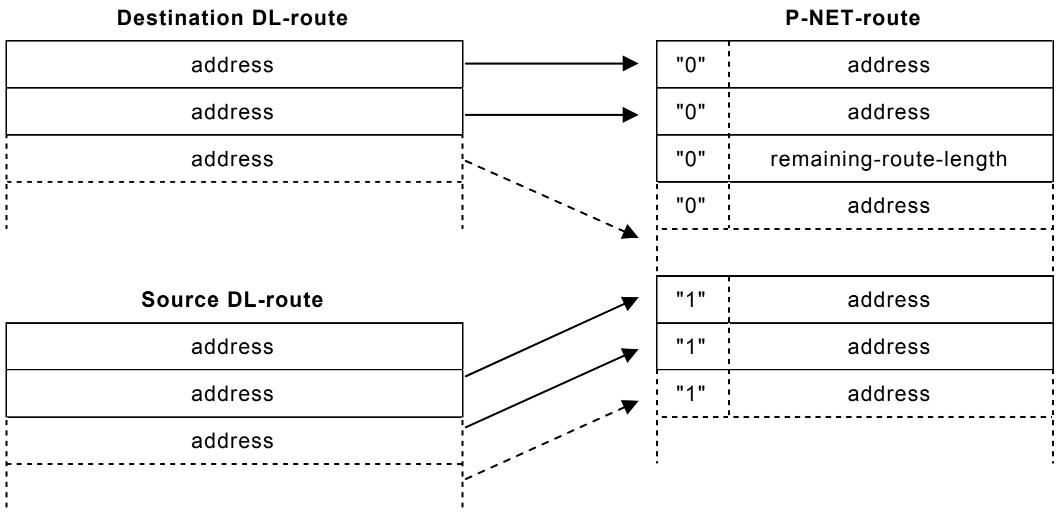

Figure 5 – Complex and IP P-NET-route generation

---------------------------------- Replace end -------------------------------

5.7.3 DL-route generation

The following paragraphs are to be replaced in 24.5.2, Type 4: Data Link Protocol Definition:

---------------------------------- Replace begin -------------------------------

DL-route generation is performed by the DLE when it has received a Confirmed or Unconfirmed DLPDU, as part of generating an indication service primitive to inform the local DLS-user of the receipt.

The four different P-NET-route formats Simple, Extended, Complex and IP are supported in Normal class DLEs. Only Simple route format is supported in Simple class DLEs.

Generally, a P-NET-route-element is copied to a DL-route-element by copying the value from the address subfield of the P-NET-route-element.

One of three alternatives apply:

a) If the P-NET-route in the received DLPDU is of Simple format, the Destination DL-route shall be empty. The source element of the received P-NET-route shall be copied to the Source DL-route. Figure 6 illustrates this.

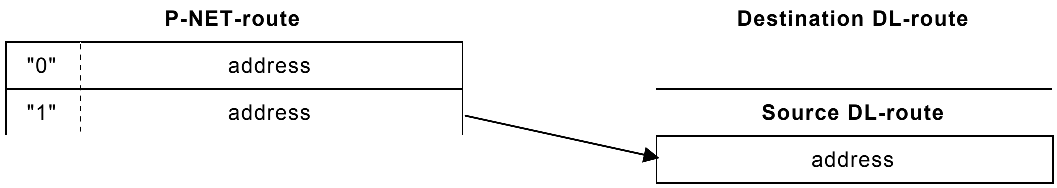

Figure 6 – Simple DL-route generation

b) If the route in the received DLPDU is of Extended format, the second destination element of the received P-NET-route shall be copied to the first and only element in the Destination DL-route. The Source DL-route shall be a copy of the two source elements in the received P-NET-route. Figure 7 illustrates this.

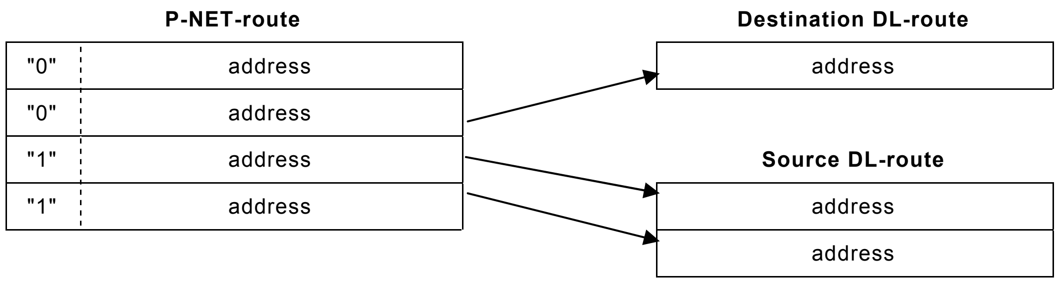

Figure 7 – Extended DL-route generation

c) If the P-NET-route in the received DLPDU is of Complex or IP format, the second element of the received P-NET-route shall be copied to the first element of Destination DL-route. The remaining destination elements of the received P-NET-route shall be copied to the Destination DL-route. All of the source elements of the received P-NET-route shall be copied to the Source DL-route. Figure 8 illustrates this.

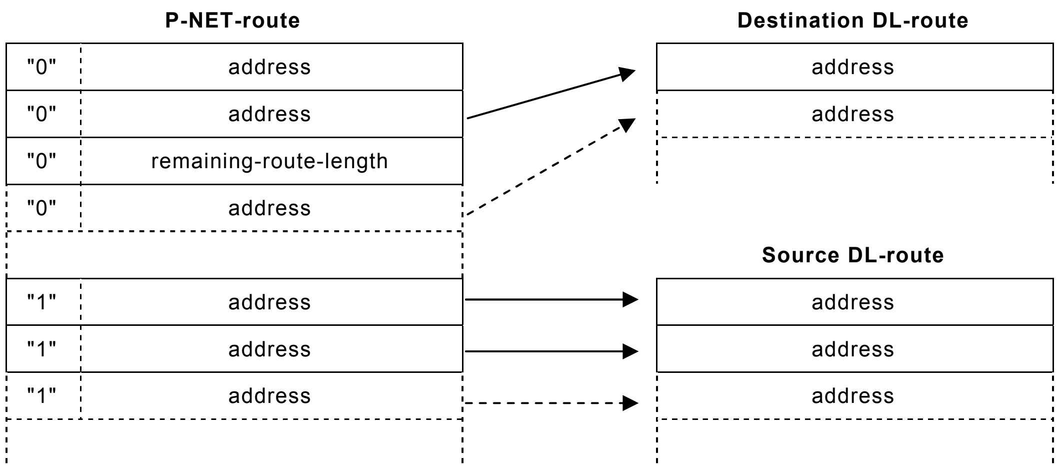

Figure 8 – Complex and IP DL-route generation

---------------------------------- Replace end --------------------------------

6 61158-5 Application Layer service definition

6.1.1.1 Route Endpoint Model

The following paragraphs are to be replaced in 9.2.5.2, Type 4 communication model specification:

---------------------------------- Replace begin --------------------------------

Formal Model

FAL ASE:			**Route Endpoint ASE**
CLASS:		Route Endpoint	
CLASS ID:			1
PARENT CLASS:			TOP
ATTRIBUTES:			
1.	(m)	Key Attribute:	Endpoint Address
2.	(m)	Attribute:	Role (Proxy object / Real object)
3.	(m)	Attribute:	REP State
4.	(m)	Attribute:	Priority
5.	(m)	Attribute:	Confirmation
6.	(m)	Attribute:	Destination Route
7.	(m)	Attribute:	Source route
8.	(m)	Attribute:	Progress
9.	(m)	Attribute:	Capabilities
10.	(m)	Attribute:	Flat addressing
SERVICES:			
1.	(m)	OpsService:	REQUEST
2.	(m)	OpsService:	RESPONSE
3.	(m)	OpsService:	Reserve REP
4.	(m)	OpsService:	Free REP
5.	(m)	OpsService:	Get REP Attribute
6.	(m)	OpsService:	Set REP Attribute

6.1.1.1.1 Attributes

6.1.1.1.1.1 Endpoint Address

This key attribute holds the Endpoint address identifying the REP.

6.1.1.1.1.2 ROLE

This attribute specifies the role of the REP. The valid values are:

Proxy container	Endpoints of this type are used for sending requests to servers and receive responses from them. The objects contained in REPs of this role are proxy objects for the real objects in the server.
Real container	Endpoints of this type are used for receiving confirmed and unconfirmed requests from clients and sending responses to them. The objects contained in REPs of this role are the real Variable Objects.

6.1.1.1.1.3 REP State

This attribute indicates the state of the REP. The values for this attribute are: IDLE RESERVED, WAITING FOR RESPONSE, RESPONSE RECEIVED or NOT IN USE.

6.1.1.1.1.4 Priority

The DLL may provide the possibility to send high priority APDUs before APDUs of lower priority. The priority only refers to the request on the local link, not requests passing gateways and not the response.

6.1.1.1.1.5 Confirmation

This attribute indicates whether the request has to be to confirmed or unconfirmed. The response is always returned unconfirmed. If the Destination Route contains one or more broadcast addresses (126) this attribute must be set to unconfirmed.

6.1.1.1.1.6 Destination Route

The Destination Route describes the Route to the destination REP. It is a sequence of Endpoint addresses and DL-addresses. On its way to the destination, the first part always indicates the address of the next DLE, AREP or REP to receive the APDU. In a request, the Destination Route holds the Route to the REP to respond. In a response, Destination Route holds the Route to the requesting REP.

6.1.1.1.1.7 Source Route

The Source Route describes the Route to the source REP. It is a sequence of endpoint addresses and DL-addresses. On its way to the destination, the first element always indicates the address of the DLE, AREP or REP endpoint from where the APDU was conveyed. In a request, the Source Route holds the Route to the requesting REP. In a response, Source Route holds the Route to the responding REP.

6.1.1.1.1.8 Progress

This attribute is only relevant in proxy container REPs. It indicates the progress of a request. It indicates number of segments that has been delivered divided with the total number of segments. This means for non-segmented requests the value is zero while waiting for the response, and one when the response is received. For segmented requests, the value will start from zero and gradually increase till it reaches the value of one.

6.1.1.1.1.9 Capabilities

This attribute defines the capabilities of the REP addressed by Destination Route. It is a local attribute, which must be set up by the user application, to reflect the capabilities of the REP containing the real Variable Objects. The value of Capabilities is used by the requesting REP to build the APDU. The attribute indicates, whether the responding REP is capable of handling bit addressing or not.

6.1.1.1.1.10 Flat addressing

This attribute indicates, whether the REP should be seen as a container of individual Variable Objects, or as a container of one, flat memory area. If Flat addressing is selected, the Variable Object ID parameter of the REQUEST service indicates the offset in octets from the beginning of the memory area.

---------------------------------- Replace end --------------------------------

6.1.1.2 Application relationship formal model

The following paragraphs are to be replaced in 9.3.2.1, Type 4 communication model specification:

---------------------------------- Replace begin --------------------------------

The functionality of the AR ASE is described in 10.1.

The application ASE defines one class, the AREP class.

FAL ASE: **Application Relationship ASE**
CLASS: **AREP**
CLASS ID: 1
PARENT CLASS: TOP

ATTRIBUTES:

1.	(m)	Key Attribute:	Endpoint Address
2.	(m)	Attribute:	Role (Client, Server, Peer)
3.	(m)	Attribute:	DLL Reference
4.	(m)	Attribute:	MaxPDUSize
5.	(m)	Attribute:	MaxDataSize
6.	(m)	Attribute:	Acknowledgement
7.	(m)	Attribute:	MaxIndicationDelay
8.	(m)	Attribute:	Local DLE address
9.	(o)	Attribute:	MaxRetryTime
10.	(o)	Attribute:	MaxRetries
11.	(o)	Attribute:	MaxOutstandingRequests
12.	(o)	Attribute:	BaudRate
13.	(o)	Attribute:	NumberOfClientDLEs

6.1.1.2.1.1 SERVICES:

1	(m)	OpsService:	AR-Get Attribute
2	(m)	OpsService:	AR-Set Attribute
3	(m)	OpsService:	AR-Send
4	(m)	OpsService:	AR-Acknowledge

6.1.1.2.1.2 Endpoint Address

This attribute specifies the numeric identifier of the AREP. It is used by the FAL to select the AREP, and implicitly the DLE for a request.

6.1.1.2.1.3 Role

This attribute specifies the role of the AREP. The valid values are:

Client Endpoints of this type send confirmed and unconfirmed Request APDUs to servers and receive Response APDUs.

Server Endpoints of this type receive confirmed and unconfirmed Request APDUs from clients and send unconfirmed Response APDUs.

Peer Endpoints of this type act as both Clients and Servers.

6.1.1.2.1.4 MaxPDUSize

This attribute specifies the maximum PDU size that can be sent by the DLL.

6.1.1.2.1.5 MaxDataSize

This attribute specifies the maximum data size that can be sent by the DLL. If the data length exceeds MaxDataSize, the VARIABLE ASE shall segment the request.

6.1.1.2.1.6 DLL Reference

This attribute contains the necessary context to convey the DLL relations.

6.1.1.2.1.7 Acknowledgement

This attribute describes the type of Acknowledgement to be used by DLL: Acknowledged or Unacknowledged transfer of Confirmed APDUs, and Acknowledged or Unacknowledged transfer of Unconfirmed APDUs.

6.1.1.2.1.8 MaxIndicationDelay

This attribute indicates to the user application, how long time a Variable Object can use to prepare a response after receiving an indication requiring that. If the Variable Object is unable to prepare a response within MaxIndicationDelay, it must issue an AR-Acknowledge. The value of MaxIndicationDelay is calculated by the DLE.

6.1.1.2.1.9 Local DLE address

This attribute reflects the DL address of the related DLE. In some situations it may be a read-only attribute.

6.1.1.2.1.10 MaxRetryTime

This attribute indicates the maximum time the DLE should try to re-transmit a request as a result of Acknowledge responses from the remote Variable Object.

6.1.1.2.1.11 MaxRetries

This attribute indicates the maximum number of re-transmissions carried out by the DLE as a result of transmission errors.

6.1.1.2.1.12 MaxOutstandingRequests

This attribute indicates the maximum number of requests that the AREP may initiate without receiving the related responses.

6.1.1.2.1.13 BaudRate

This attribute specifies the baud rate used by the physical layer. It is conveyed to/from the physical layers by the DLEs.

6.1.1.2.1.14 NumberOfClientDLEs

This attribute only relates to a DLE using the P-NET protocol in the client role. It specifies the number of participants in a token round.

----------------------------------- Replace end --------------------------------

6.1.1.3 Common parameter definition

The following paragraphs are to be replaced in 9.3.3.2, Type 4 communication model specification:

----------------------------------- Replace begin --------------------------------

Parameters used in more AR ASE services are defined below:

6.1.1.3.1.1 Route info

The complete DL Route contains the following elements:

6.1.1.3.1.2 Destination Route

The Destination-Route describes how to reach the destination REP. It is a sequence of Endpoint addresses and DL-addresses. On its way to the destination, the first part always indicates the address of the next DLE, AREP or REP to receive the APDU.

6.1.1.3.1.3 Source Route

The Source Route in the same way describes how to find the way back to the endpoint that initiated the request. It is a sequence of endpoint addresses and DL-addresses. On its way to the destination, the first element always indicates the address of the DLE, AREP or REP endpoint from where the APDU was sent.

6.1.1.3.1.4 Priority

The underlying layer may provide the possibility to send high priority APDUs before APDUs of lower priority. This priority only refers to the request on the local link, not requests passing gateways and not the response.

6.1.1.3.1.5 Confirmation

This parameter indicates whether the request has to be to confirmed or unconfirmed. A response is always returned unconfirmed. If the destination route contains one or more broadcast addresses (126) this attribute must be set to unconfirmed.

6.1.1.3.1.6 APDU Header

The APDU Header parameter holds a Control/Status subfield indicating the Variable Service, an APDU format subfield, indicating whether the APDU holds an offset, and finally an APDU length subfield, indicating the octet length of the APDU.

6.1.1.3.1.7 APDU Body

This parameter holds the APDU Body to send or receive.

---------------------------------- Replace end --------------------------------

7 Addressing conventions for P-NET on IP

Nodes on an IP-network are addressed with two P-NET Route elements, but this is entirely handled by the IP-node. It means that any P-NET client (master) can access servers on an IP-network without knowing anything about IP-addresses. Figure 9 gives an example of P-NET route elements for normal addressing, whereas Figure 10 gives an example of P-NET route elements for IP addressing.

Dest.1	**Dest.2**	**Lgt**	**Dest.3**	**Src.1**	**Src.2**
Node addr	Port		Node addr	Node addr	CtrlCard
04	02	03	33	03'	31'

Figure 9 – "Normal" addressing

Dest.1	**Dest.2**	**Lgt**	**Dest.3**	**Dest.4**	**Src.1**	**Src.2**	**Src.3**
IPNetID	Node addr		Port	Node addr	IPNetID	Node addr	CtrlCard
11	04	05	02	33	11'	03'	31'

Figure 10 – "IP" addressing

Since the route elements are constructed in the same way for all types of addressing, it is possible to send packages from any P-NET master via an IP network, without the master need to know anything about IP addresses. The IPNetID and the node address are translated into an IP address in the device that is connected to the IP network. The translation is performed using a table called IPNetTable.

A server can receive packages on two different UDP port numbers, Normal and Secure. A simple password system is introduced in relation to Secure UDP port number. All packages that are sent to the Secure UDP port number shall contain an 8 byte password, which is to be checked by the server. If the server does not recognize the password, the package is not accepted and will be rejected.

When using NAT routers and configuring these to use Secure UDP port for passing on packages from the Internet to the local servers, it is ensured that packages from the Internet would only be accepted when they contain the right password.

The subnet mask is always 255.255.255.0. The last byte in the IP address has the same value as the P-NET node address.

The IP nets are split into two types: IPRange net and UDPRange net. See definitions above in Terms and Definitions. The use of these types is illustrated in Figure 11.

- Nodes within the same “Plant section” are addressed by using an IPRange net, which also is the node’s own subnetwork. The nodes are communicating directly, the UDP port number is “Normal” and the packages are not using password.
- Nodes within one “Plant section” are addressing nodes on another “Plant section” via a local router by using an IPRange net. The UDP port number is “Normal” and the packages are not using password.
- The “remote client” is addressing nodes in the two “plant sections” by using an UDPRange net. The IP address of the UDPRange net is the IP address of the “Local NAT router” when seen from the Internet side. A table is configured in the “Local NAT router” holding one element for each UDP port number, i.e. for each server node that should be addressed from the Internet. The table translates the UDP port number to an IP address and “Secure” UDP port number of the node in question. The packages are using password.

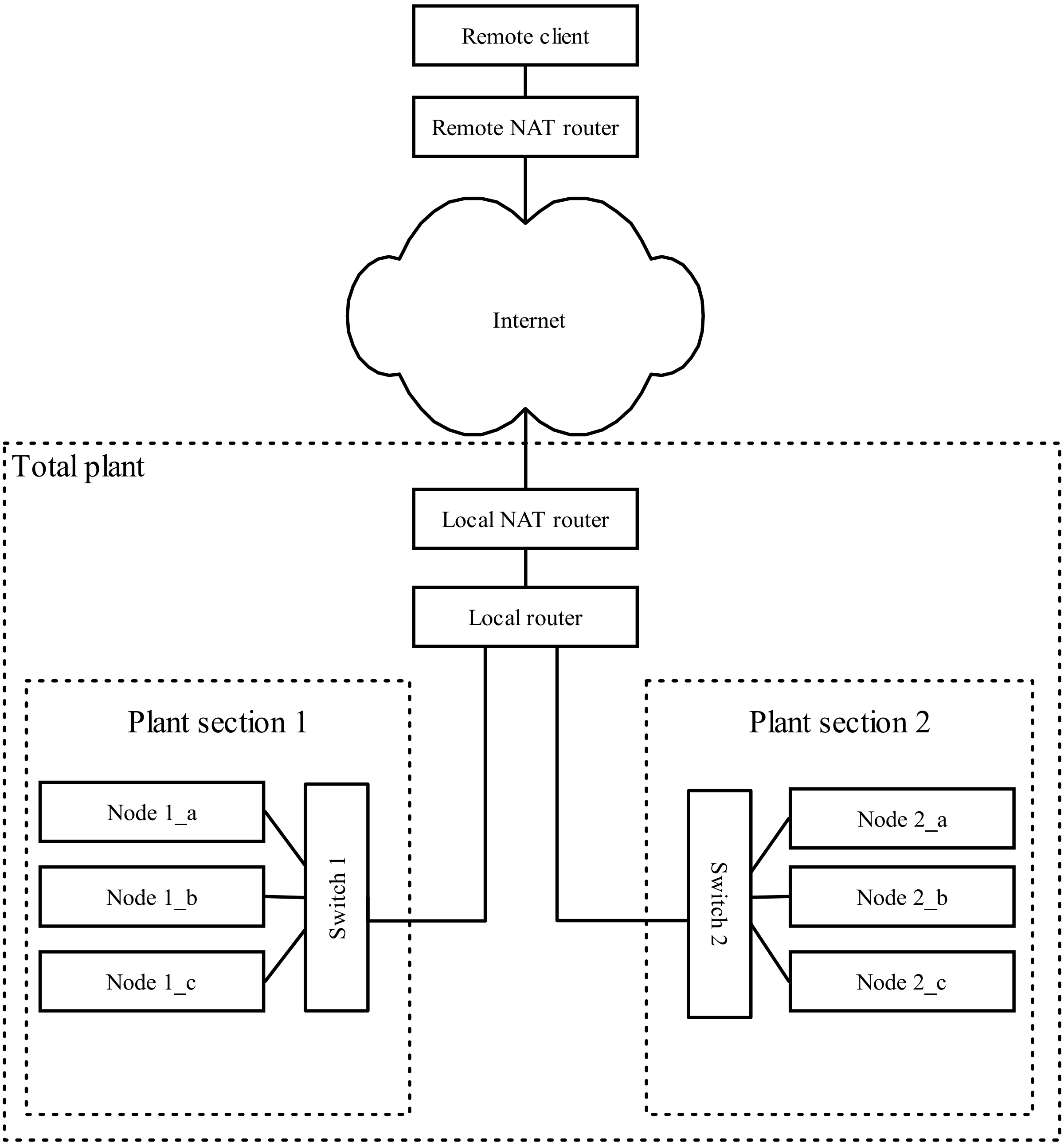

Figure 11 – "IP" net types

8 Translation of P-NET address to IP address

When a P-NET request package is to be sent on an IP network, this shall be done via an IP node. The IP node is able to translate the IPNetID and Node address to an IP address and a UDP port number. This is done via the IPNetTable. Configuration of the table is outside the scope of this specification.

The IPNetTable holds the fields shown in Table 4 (values are only examples).

Table 4 – IPNetTable fields

IPNetID	IPAddr	UDPPort	UsePW	Router	Nettype
1	IP Range1 start.0	34378	0	Router NA (1)	IPRange
2	NAT 1 IP	UDPRange1start	1	Router NA (1)	UDPRange
3	IP Range2 start.0	34378	0	0	IPRange
4	NAT 2 IP	UDPRange2 start	0	Router NA (2)	UDPRange
.	x.x.x.x	x	x	x	Unused
.	x.x.x.x	x	x	x	Unused
124	x.x.x.x	x	x	x	Unused

A separate variable called NoOfIPNets specifies the number of used indexes in the IPNetTable. IPNetID is reserved for dynamic clients. IPNetID 126 and 127 are reserved for future use and shall not be used.

The example in Table 4 – IPNetTable fields describes four IPNets. A node's own subnet is defined as the net where “Router” is zero, in this case it is the net with IPNetID=3.

The “Router” field holds the node address of the router to which UDP/IP packages to nodes on this net are to be sent. The router is always located on this node’s own IP net.

When P-NET request packages are to be sent, the IP address and UDP port number are determined as described in one of the following methods:

a) IPRange net, router=0: Nodes on this net are located on the same IP subnet as the node itself. The most significant 24 bits of the IP address are found in the IPNetTable, the last 8 bits is the Node address (range 1 to 125). The UDP port number is found directly in the IPNetTable.

b) IPRange net, router<>0: Nodes on this type of net are located on a different IP subnet as the node itself. The most significant 24 bits of the IP address are found in the IPNetTable, the last 8 bits is the Node address (range 1 to 125). The UDP port number is found directly in the IPNetTable. Nodes on this type of net are addressed via a router.

c) UDPRange net, router=0: This combination is not legal.

d) UDPRange net, router<>0: The entire IP address is found in the IPNetTable. UDP port number is calculated as the sum of Start UDP port number, which is found in IPNetTable, and Node address. Nodes on this type of net are addressed via a router.

9 Dynamic clients

An IP server node can receive requests from “known” or “unknown” clients. A “known” client is a client where the IP address and UDP Port number fits to an element within the IPNetTable of the server. The source part of the P-NET address field holds the requestors IPNetID and Node address. Whether a client is “known” or not, is determined from the following set of rules:

- Requestor IPNetID points out an IPRange Net **and**
- Requestor IP address = IPRangeStart from IPNetTable+Requestor Node address **and**
- Requestor UDP port=UDP port from IPNetTable **and**
- The package is without any password

If the client is “known”, then the Requestor IPNetID and Node address are used for sending the response in the same way as when sending a request.

If the client is “unknown” according to the above rules, then IPNetID is set to 125, which indicates that this net is reserved for dynamic clients. IPNetID with index 125 selects an internal table within the IP stack, which holds field for the clients IP address, UDP port, password (several passwords are possible, therefore the currently used is saved and inserted in the response) and a timestamp for when this table element has been used.

Requestor IPNetID is set to 125 as mentioned, and it is checked whether the client already exists within the table. If it exists, the found index is reused. If not, a free element within the table is used.

Consequently the client can receive a response where IPNetID and Node address are changed according to the source information in the request. The optimum is if the client can save the allocated values of IPNetID and Node address and use these as source information in the succeeding requests, but this is not a requirement.

10 Broadcast / Netcast

P-NET Node addresses 126 and 127 are reserved for broadcast. IPRange net shall be used for broadcast for IP on P-NET. When the destination node address is set to Broadcast-Node-address (BNA), the IPNetID shall select an IPRange net, the last byte of the IP address is set to 255 and the receiver MAC address is set to 6*255. Hence, P-NET broadcast is sent using IP netcast.

11 Package format

P-NET UDP packages have the format as shown in Figure 12.

Header	P-NET package	optional password

Figure 12 – P-NET IP package format

The header is four byte, with the value $02000000.

The P-NET package is a standard P-NET package without any checksum.

Password is eight bytes.

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other...

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other...

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other...

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other ....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness ....
quality of writing....................................
technical contents....................................
logic of arrangement of contents ....
tables, charts, graphs, figures...............
other ....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

....
....
....
....
....
....
....
....
....
....
....
....

ISBN 2-8318-8152-8

9 782831 881522

ICS 25.040.40; 35.240.50; 35.100.05

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND