



SLOVENSKI STANDARD

SIST EN 14908-1:2014

01-julij-2014

Nadomešča:
SIST EN 14908-1:2006

Odperta izmenjava podatkov v avtomatizaciji stavb in izvršnih elementov ter pri upravljanju stavb - Protokol regulacijske mreže - 1. del: Protokolarni sklad

Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 1: Protocol Stack

Firmenneutrale Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Gebäudedatennetzprotokoll - Teil 1: Datenprotokollschichtenmodell

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment - Protocole de bâtiment du réseau - Partie 1 : Spécifications du protocole

Ta slovenski standard je istoveten z: EN 14908-1:2014

ICS:

35.240.99	Uporabniške rešitve IT na drugih področjih	IT applications in other fields
97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

SIST EN 14908-1:2014

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 14908-1:2014](#)

<https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014>

EUROPEAN STANDARD

EN 14908-1

NORME EUROPÉENNE

EUROPÄISCHE NORM

April 2014

ICS 35.240.99; 91.140.01; 97.120

Supersedes EN 14908-1:2005

English Version

Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 1: Protocol Stack

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment - Protocole de contrôle du réseau - Partie 1: Niveaux du protocole

Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Gebäude-Netzwerk-Protokoll - Teil 1: Datenprotokollschichtenmodell

This European Standard was approved by CEN on 12 April 2013.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Foreword.....	5
Introduction	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions.....	7
4 Symbols and abbreviations	9
4.1 Symbols and graphical representations.....	9
4.2 Abbreviations	10
5 Overview of protocol layering	11
6 MAC sublayer	13
6.1 General.....	13
6.2 Service provided	13
6.3 Interface to the link layer.....	13
6.4 Interface to the physical layer	14
6.5 MPDU format	15
6.6 Predictive p -persistent CSMA — overview description.....	15
6.7 Idle channel detection	16
6.8 Randomising	17
6.9 Backlog estimation	17
6.10 Optional priority	18
6.11 Optional collision detection	19
6.12 Beta1, Beta2 and Preamble Timings	20
7 Link layer	22
7.1 Assumptions	22
7.2 Service provided	22
7.3 CRC.....	22
7.4 Transmit algorithm.....	23
7.5 Receive Algorithm.....	23
8 Network layer.....	23
8.1 Assumptions	23
8.2 Service provided	25
8.3 Service interface	25
8.4 Internal structuring of the network layer	26
8.5 NPDU format.....	26
8.6 Address recognition	27
8.7 Routers.....	27
8.8 Routing algorithm	28
8.9 Learning algorithm — subnets	28
9 Transaction control sublayer.....	28
9.1 Assumptions	28
9.2 Service provided	29
9.3 Service interface	29
9.4 State variables.....	30

9.5	Transaction control algorithm	30
10	Transport layer	31
10.1	Assumptions	31
10.2	Service provided	31
10.3	Service interface	31
10.4	TPDU types and formats	32
10.5	Protocol diagram.....	33
10.6	Transport protocol state variables	34
10.7	Send algorithm.....	34
10.8	Receive algorithm	34
10.9	Receive transaction record pool size and configuration engineering	34
11	Session layer	37
11.1	Assumptions	37
11.2	Service Provided	37
11.3	Service interface	38
11.4	Internal structure of the session layer.....	38
11.5	SPDU types and formats	39
11.6	Protocol timing diagrams.....	40
11.7	Request-response state variables.....	43
11.8	Request-response protocol — client part	43
11.9	Request-response protocol — server part	43
11.10	Request-response protocol timers	44
11.11	Authentication protocol.....	44
11.12	Encryption algorithm	44
11.13	Retries and the role of the checksum function.....	44
11.14	Random Number Generation	45
11.15	Using Authentication	45
12	Presentation/application layer	45
12.1	Assumptions	45
12.2	Service provided	45
12.3	Service interface	46
12.4	APDU types and formats	47
12.5	Protocol diagrams.....	48
12.6	Application protocol state variables	50
12.7	Request - response messaging in offline state	50
12.8	Network variables	51
12.9	Error notification to the application program	52
13	Network management & diagnostics	53
13.1	Assumptions	53
13.2	Services provided	53
13.3	Network management and diagnostics application structure	53
13.4	Node states	53
13.5	Using the network management services	54
13.6	Using router network management commands	58
13.7	NMPDU formats and types	59
13.8	DPDU types and formats	80
Annex A	(normative) Reference implementation	85
A.1	General	85
A.2	Predictive CSMA algorithm	85
Annex B	(normative) Additional Data Structures.....	380
B.1	General	380

EN 14908-1:2014 (E)

B.2	Read-only structures	381
B.3	Domain table.....	386
B.4	Address table	386
B.5	Network variable tables - informative	391
B.6	Self-Identification structures	393
B.7	Configuration structure.....	400
B.8	Statistics relative structure	402
Annex C	(informative) Behavioral characteristics	404
C.1	Channel capacity and throughput.....	404
C.2	Network metrics	405
C.3	Transaction metrics	406
C.4	Boundary conditions — power-up	407
C.5	Boundary conditions — high load	407
Annex D	(normative) PDU summary.....	408
Annex E	(normative) Naming and addressing.....	410
E.1	Address types and formats.....	410
E.2	Domains	410
E.3	Subnets and nodes	411
E.4	Groups.....	411
E.5	Unique_Node_ID and node address assignment	412
E.6	NPDU addressing.....	413
Bibliography	415

ITeH STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 14908-1:2014

<http://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014>

Foreword

This document (EN 14908-1:2014) has been prepared by Technical Committee CEN/TC 247 “Building Automation, Controls and Building Management”, the secretariat of which is held by SNV.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by October 2014 and conflicting national standards shall be withdrawn at the latest by October 2014.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 14908-1:2005.

This European Standard is part of a series of standards for open data transmission in building automation, control and in building management systems. The content of this European Standard covers the data communications used for management, automation/control and field functions.

The following is a list of technical changes since the previous edition:

- EN 14908-5 has been added to the normative references;
- the normative Annex A has been re-worked for a better understanding. The reference implementation of the standard shows in detail which part is normative and hardware independent, which one is normative but hardware dependent and which one is not normative because it is hardware dependent. This information supports the development of a protocol stack and the understanding of the specified communication services.

EN 14908-1 is part of a series of European Standards under the general title *Control Network Protocol (CNP)*, which comprises the following parts:

Part 1: *Protocol stack*;

Part 2: *Twisted pair communication*;

Part 3: *Power line channel specification*;

Part 4: *IP communication*;

Part 5: *Implementation*;

Part 6: *Application elements*.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

EN 14908-1:2014 (E)**Introduction**

This European Standard has been prepared to provide mechanisms through which various vendors of building automation, control, and building management systems may exchange information in a standardised way. It defines communication capabilities.

This European Standard will be used by all involved in design, manufacture, engineering, installation and commissioning activities.

**iTeh STANDARD PREVIEW
(standards.iteh.ai)**

SIST EN 14908-1:2014

<https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014>

1 Scope

This European Standard applies to a communication protocol for networked control systems in commercial Building Automation, Controls and Building Management. The protocol provides peer-to-peer communication for networked control and is suitable for implementing both peer-to-peer and master-slave control strategies. This specification describes services in layers 2 to 7. In the layer 2 (data link layer) specification, it also describes the MAC sub-layer interface to the physical layer. The physical layer provides a choice of transmission media. The interface described in this specification supports multiple transmission media at the physical layer. In the layer 7 specification, it includes a description of the types of messages used by applications to exchange application and network management data.

2 Normative references

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

EN 14908-5, *Open Data Communication in Building Automation, Controls and Building Management Implementation Guideline - Control Network Protocol - Part 5: Implementation*

iTeh STANDARD PREVIEW

3 Terms and definitions (standards.iteh.ai)

For the purposes of this document, the following terms and definitions apply.

For the purposes of this European Standard, the following subclause introduces the basic terminology employed throughout this European Standard. Most of it is commonly used and the terms have the same meaning in both the general and the standard context. However, for some terms, there are subtle differences. For example, in general, bridges do selective forwarding based on the layer 2 destination address. There are no layer 2 addresses in this standard protocol, so bridges forward all packets, as long as the domain address in the packet matches a domain of which the bridge is a member. Routers, in general, perform network address modification so that two protocols with the same transport layer but different network layers can be connected to form a single logical network. Routers of this standard may perform network address modification, but typically, they only examine the network address fields and selectively forward packets based on the network layer address fields.

3.1

channel

physical unit of bandwidth linking one or more communication nodes.

Note 1 to entry: Refer to Annex E for further explanation of the relationship between a channel and a subnet.

3.2

physical repeater

device that reconditions the incoming physical layer signal on one channel and retransmits it onto another channel

3.3

store-and-forward repeater

device that stores and then reproduces data packets onto a second channel

EN 14908-1:2014 (E)**3.4****bridge**

device that connects two channels (x and y); forwards all packets from x to y and vice versa, as long as the packets originate on one of the domain(s) that the bridge belongs to

3.5**configuration**

non-volatile information used by the device to customise its operation. There is configuration data for the correct operation of the protocol in each device, and optionally, for application operation. The network configuration data stored in each device has a checksum associated with the data. Examples of network configuration data are node addresses, communication media parameters such as priority settings, etc. Application configuration information is application specific

3.6**domain**

virtual network that is the network unit of management and administration. Group and subnet (see below) addresses are assigned by the administrator responsible for the domain, and they have meaning only in the context of that domain

3.7**flexible domain**

used in conjunction with Unique_Node_ID and broadcast addressing. A node responds to a Unique_Node_ID-addressed message if the address matches, regardless of the domain on which the message was sent. To respond so that the sender receives it, the response shall be sent on the domain in which it was received. Furthermore, this domain shall be remembered for the duration of the transaction so that duplicate detection of any retries is possible. This transitory domain entry at a node is called the flexible domain. How many flexible domain entries a node supports depends on the implementation. However, a minimum of 1 is required

[SIST EN 14908-1:2014](https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014)

3.8**subnet**

set of nodes accessible through the same link layer protocol; a routing abstraction for a channel; in this standard subnets are limited to a maximum of 127 nodes

<https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014>

3.9**node**

abstraction for a physical node that represents the highest degree of address resolvability on a network. A node is identified (addressed) within a subnet by its (logical) node identifier. A physical node may belong to more than one subnet; when it does, it is assigned one (logical) node number for each subnet to which it belongs. A physical node may belong to at most two subnets; these subnets shall be in different domains. A node may also be identified (absolutely) within a network by its Unique_Node_ID

3.10**group**

uniquely identifiable set of nodes within a domain. Within this set, individual members are identified by their member number. Groups facilitate one-to-many communication and are intended to support functional addressing

3.11**router**

device that routes data packets to their respective destinations by selectively forwarding from subnet to subnet; a router always connects two (sets of) subnets; routers may modify network layer address fields. Routers may be set to one of four modes: repeater mode, bridge mode, learning mode, and configured mode. In repeater mode, packets are forwarded if they are received with no errors. In bridge mode, packets are forwarded if they are received with no errors and match a domain that the router is a member of. Routers in learning mode learn the topology by examining packet traffic, while

routers that are set to configured mode have the network topology stored in their memory and make their routing decisions solely upon the contents of their configured tables

3.12

(application) gateway

interconnects networks at their highest protocol layers (often two different protocols). Two domains can also be connected through an application gateway

3.13

Beta1

period immediately following the end of a packet cycle. A node attempting to transmit monitors the state of the channel, and if it detects no transmission during the Beta1 period, it determines the channel to be idle

3.14

Beta2

randomising slot. A node wishing to transmit generates a random delay T. This delay is an integer number of randomising slots of duration Beta2

3.15

network variable

variable in an application program whose value is automatically propagated over the network whenever a new value is assigned to it

3.16

Standard Network Variable Types (SNVTs)

variables with agreed-upon semantics. These variables are interpreted by all applications in the same way, and are the basis for interoperability. Definition of specific SNVTs is beyond the scope of this European Standard

<https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014>

3.17

manual service request message

network management message containing a node's Unique_Node_ID. Used by a network management device that receives this message to install and configure the node. May be generated by application or system code. May be triggered by external hardware event, e.g., driving a "manual service request" input low

3.18

transaction

sequence of messages that are correlated together. For example, a request and the responses to the request are all part of a single transaction. A transaction succeeds when all the expected messages from every node involved in the transaction are received at least once. A transaction fails in this European Standard if any of the expected messages within the transaction are not received. Retries of messages within a transaction are used to increase the probability of success of a transaction in the presence of transient errors

4 Symbols and abbreviations

4.1 Symbols and graphical representations

Figure 1 shows the basic topology of networks based on this protocol and the symbolic representations used in this European Standard.

EN 14908-1:2014 (E)

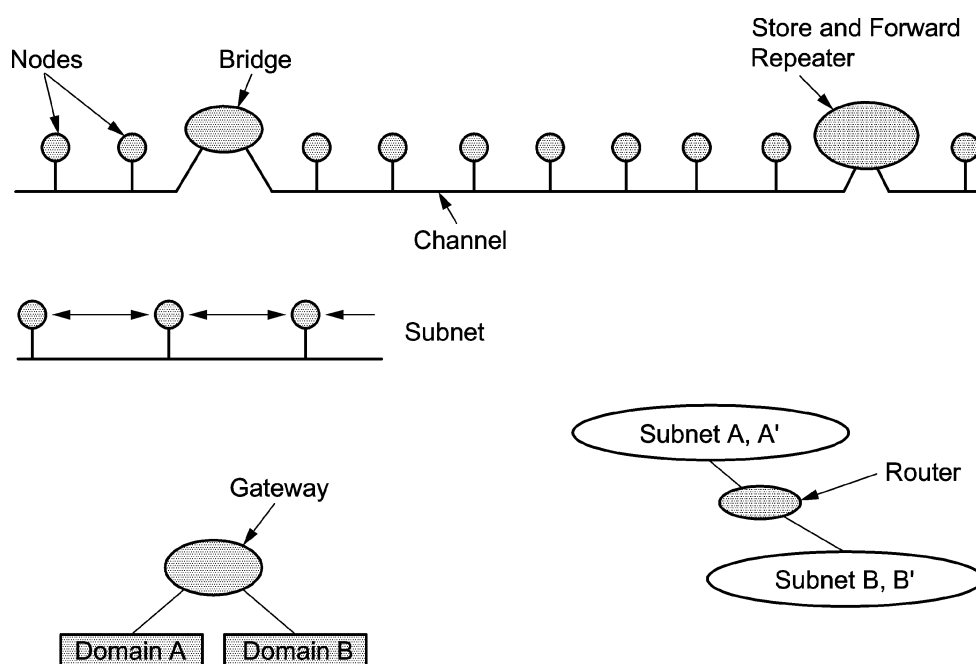


Figure 1 — Network topology & symbols

The layering of this protocol is described using standard OSI terminology, as shown in Figure 2.

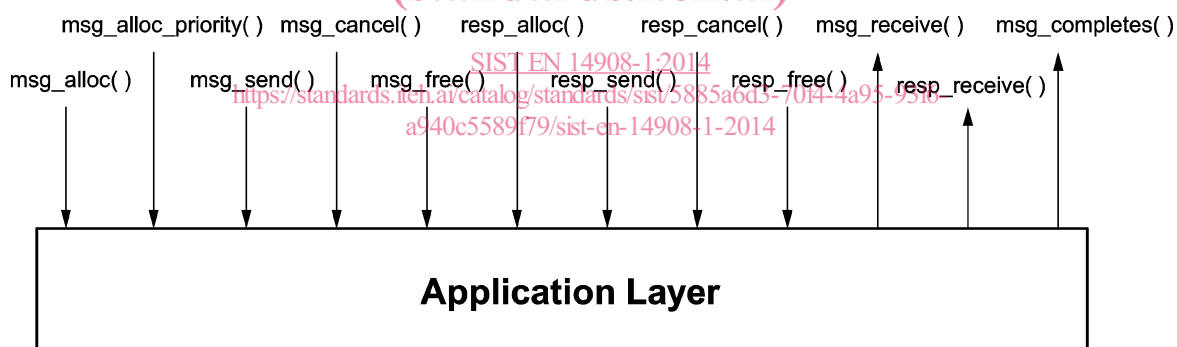


Figure 2 — Protocol terminology

4.2 Abbreviations

CNP Control Network Protocol

The Protocol Data Unit (PDU) abbreviations used throughout this Standard are:

PPDU Physical Protocol Data Unit, or frame
 MPDU MAC Protocol Data Unit, or frame
 LPDU Link Protocol Data Unit, or frame
 NPDU Network Protocol Data Unit, or packet
 TPDU Transport Protocol Data Unit, or a message/ack

SPDU	Session Protocol Data Unit, or request/response
NMPDU	Network Management Protocol Data Unit
DPDU	Diagnostic Protocol Data Unit
APDU	Application Protocol Data Unit
FSM	Finite State Machine (diagram)

Annex D (PDU Summary) contains the details of these PDUs.

5 Overview of protocol layering

The protocol specified by this Standard consists of the layers shown in Figure 3. Each layer is described below.

Multiple physical layer protocols and data encoding methods are allowed in systems based on this European Standard. Each encoding scheme is medium-dependent.

The *MAC* (Medium Access Control) sublayer employs a collision avoidance algorithm called Predictive *p*-persistent CSMA (Carrier Sense, Multiple Access). For a number of reasons, including simplicity and compatibility with the multicast protocol, the link *layer* supports a simple connectionless service. Its functions are limited to framing, frame encoding, and error detection, with no error recovery by re-transmission.

ITeH STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 14908-1:2014](https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014)

<https://standards.iteh.ai/catalog/standards/sist/5885a6d3-70f4-4a95-93f6-a940c5589f79/sist-en-14908-1-2014>

EN 14908-1:2014 (E)

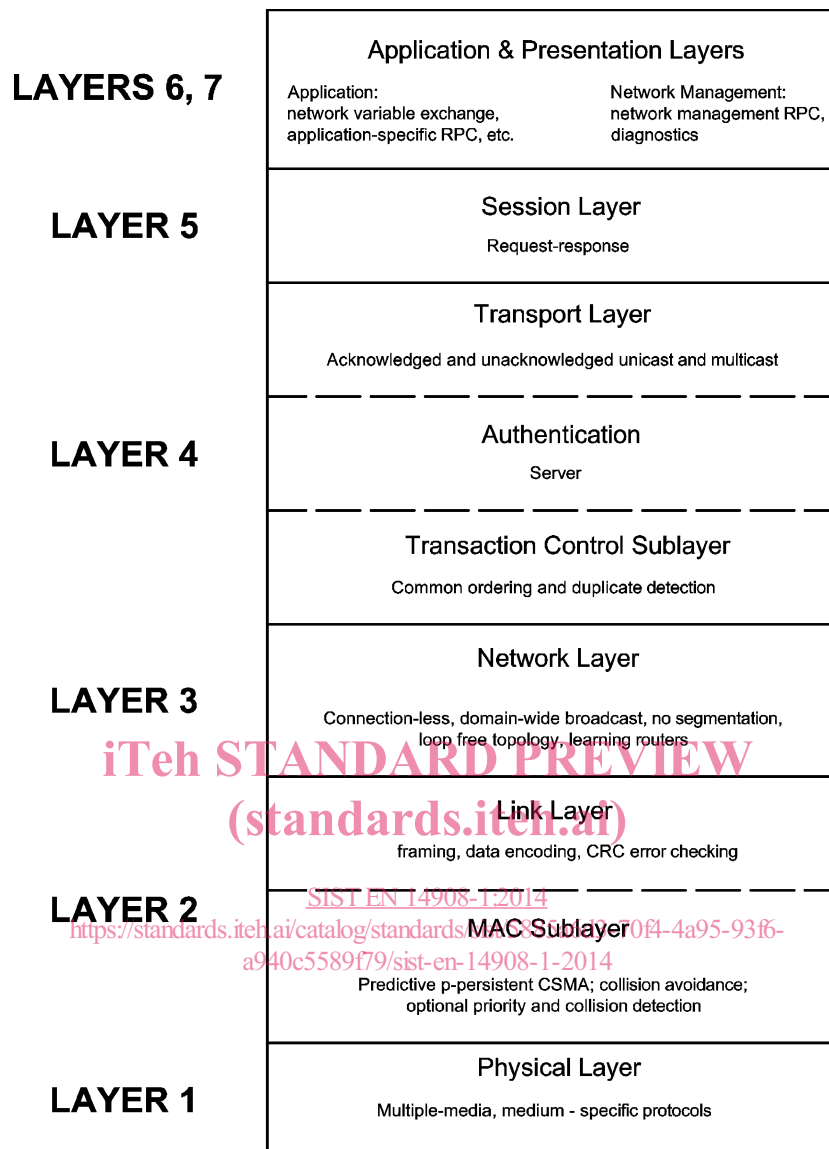


Figure 3 — Protocol layering

The *Network* layer handles packet delivery within a single domain, with no provisions for inter-domain communication. The Network service is connection-less, unacknowledged, and supports neither segmentation nor re-assembly of messages. The routing algorithms employed by the network layer to learn the topology assumes a tree-like network topology; routers with configured tables may operate on topologies with physical loops, as long as the communication paths are logically tree-like. In this topology, a packet may never appear more than once at the router on the side on which the packet originated. The unicast routing algorithm uses learning for minimal over-head and no additional routing traffic. Use of configured routing tables is supported for both unicast and group addresses, although in many applications a simple flooding of group addressed messages is sufficient.

The heart of the protocol hierarchy is the *Transport* and *Session* layers. A common *Transaction Control Sublayer* handles transaction ordering and duplicate detection for both. The *Transport* layer is connection-less and provides reliable message delivery to both single and multiple destinations. Authentication of the message sender's identity is included as a transport layer service, for use when the security of sender authentication is required. The authentication server requires only the

Transaction Control Sublayer to accomplish its function. Thus Transport and Session layer messages may be authenticated using all of the addressing modes other than broadcast.

The session layer provides a simple Request-Response mechanism for access to remote servers. This mechanism provides a platform upon which application specific remote procedure calls can be built. The network management protocol, for example, depends upon the Request-Response mechanism in the Session layer.

A transport layer acknowledged message expects indication of message delivery from remote destination(s). A session layer request message expects indication that application-specific remote task(s) have been completed. A given message uses only one or the other type of service, but not both.

This specification includes the *Presentation Layer* and the lowest level of the *Application Layer*. These layers provide services for sending and receiving application messages including network variables, and other types of messages such as network management and diagnostic messages and foreign frames (see Clause 13). For a network variable update, the APDU header provides information on how to interpret the APDU. This application-independent interpretation of the data allows data to be shared among nodes without prior arrangement.

6 MAC sublayer

6.1 General

In this European Standard the following Media Access Control sublayer is defined. If there is a need for other MAC sublayers they are defined in additional parts of this European Standard.

6.2 Service provided

The Media Access Control (MAC) sublayer facilitates media access with optional priority and optional collision detection/collision resolution. It uses a protocol called Predictive *p*-persistent CSMA (Carrier Sense, Multiple Access), that has some resemblance to the *p*-persistent CSMA protocol family.

Predictive *p*-persistent CSMA is a *collision avoidance* technique that randomises channel access using knowledge of the expected channel load. A node wishing to transmit always accesses the channel with a random delay in the range (0..*w*). To avoid throughput degradation under high load, the size of the randomising window, *w*, is a function of estimated channel backlog BL:

$$w = (BL \times W_{\text{base}}) - 1, \quad (1)$$

where

W_{base} is the base window size. W_{base} is measured in time. Its duration, derived from Beta2 (see 6.8), equals 16 Beta2 slots.

6.3 Interface to the link layer

The MAC sublayer is closely coupled to the Link layer, described in Clause 7. With the MAC sublayer being responsible for media access, the Link layer deals with all other layer 2 issues, including framing and error detection. For explanatory purposes, the interface between the two layers is described in the form shown in Figure 4.