FINAL DRAFT

INTERNATIONAL STANDARD

ISO/FDIS 14908-1

ISO/TC **205**

Secretariat: **ANSI**

Voting begins on:
2011-01-04

Voting terminates on:
2011-03-04

Interconnection of information technology equipment — Control Network Protocol —

Part 1:
Protocol Stack

Interconnexion des équipements des technologies de l'information — Protocole de réseau de contrôle — Partie 1: Pile de protocole

Please see the administrative notes on page iii

Reference number
ISO/FDIS 14908-1:2011(E)

In accordance with the provisions of Council Resolution 15/1993, this document is **circulated in the English language only**.

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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

ISO 14908-1 was prepared by CEN/TC 247, was adopted, under the fast track procedure, by joint Technical Committee ISO/IEC JTC 1, *Information technology*, and was assigned to SC 25, *Interconnection of information technology equipment*. It was then transferred to ISO/TC 205, *Building environment design*.

ISO 14908 consists of the following parts, under the general title *Interconnection of information technology equipment — Control Network Protocol*:

— *Part 1: Protocol Stack*

— *Part 2: Twisted-pair communication*

— *Part 3: Power line channel specification*

— *Part 4: IP communication*

Introduction

This International Standard has been prepared to provide mechanisms through which various vendors of local area control networks may exchange information in a standardized way. It defines communication capabilities.

This International Standard is to be used by anyone involved in design, manufacture, engineering, installation and commissioning activities.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents held by Echelon Corporation.

ISO and the IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and the IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of the patent rights is registered with ISO and the IEC. Information may be obtained from:

Echelon Corporation, 4015 Meridian Avenue, San Jose, CA 94304, USA, phone +1-408-938-5234, fax: +1-408-790-3800, http://www.echelon.com.

Interconnection of information technology equipment — Control Network Protocol —

Part 1: Protocol Stack

1 Scope

This part of ISO 14908 applies to a communication protocol for local area control networks. 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 part of ISO 14908 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 Terms and definitions

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

NOTE Most of the terms are commonly used and 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 International 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.

2.1
channel
physical unit of bandwidth linking one or more communication nodes

NOTE See Annex E for further explanation of the relationship between a channel and a subnet.

2.2
physical repeater
device that reconditions the incoming physical layer signal on one channel and transmits it on to another channel

2.3
store-and-forward repeater
device that stores and then reproduces data packets on a second channel

2.4
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) to which the bridge belongs

2.5
configuration
non-volatile information used by the device to customise its operation

NOTE 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.

2.6
domain
virtual network that is the network unit of management and administration

NOTE Group (2.10) and subnet (2.8) addresses are assigned by the administrator responsible for the domain and have meaning only in the context of that domain.

2.7
flexible domain
transitory domain entry at a node used in conjunction with Unique_Node_ID and broadcast addressing

NOTE 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 must be sent on the domain in which it was received. Furthermore, this domain must be remembered for the duration of the transaction so that duplicate detection of any retries is possible. How many flexible domain entries a node supports is up to the implementation. However, a minimum of one is required.

2.8
subnet
set of nodes accessible through the same link layer protocol; a routing abstraction for a channel

NOTE In this International Standard, subnets are limited to a maximum of 127 nodes.

2.9
node
abstraction for a physical node that represents the highest degree of address resolvability on a network

NOTE A node is identified (addressed) within a subnet by its (logical) node identifier. A physical node can 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 can belong to at most two subnets; these subnets must be in different domains. A node can also be identified (absolutely) within a network by its Unique_Node_ID.

2.10
group
uniquely identifiable set of nodes within a domain

NOTE Within this set, individual members are identified by their member number. Groups facilitate one-to-many communication and are intended to support functional addressing.

2.11
router
device that routes data packets to their respective destinations by selectively forwarding from subnet to subnet

NOTE A router always connects two (sets of) subnets; routers may modify network layer address fields. Routers can 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 of which the router is a member. 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.

2.12
(application) gateway
gateway that interconnects networks at their highest protocol layers (often two different protocols)

NOTE Two domains can also be connected through an application gateway.

2.13
Beta1
β_1
period immediately following the end of a packet cycle

NOTE A node attempting to transmit data packets monitors the state of the channel and, if it detects no transmission during the Beta1 period, determines the channel to be idle.

2.14
Beta2
β_2
randomising slot

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

2.15
network variable
variable in an application program whose value is automatically propagated over the network whenever a new value is assigned to it

2.16
Standard Network Variable Types
SNVTs
variables with agreed-upon semantics

NOTE 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 International Standard.

2.17
manual service request message
network management message containing a node's Unique_Node_ID

NOTE 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 an external hardware event, e.g. driving a “manual service request” input low.

2.18
transaction
sequence of messages that are correlated together

NOTE 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 International 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.

3 Symbols and abbreviations

3.1 Symbols and graphical representations

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

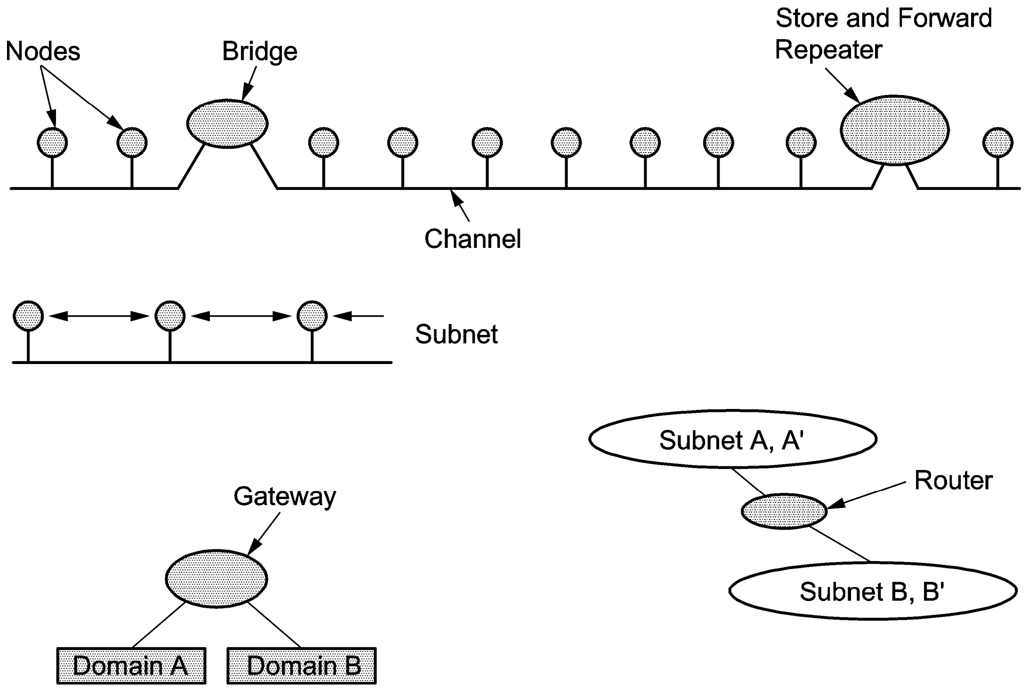

Figure 1 — Network topology & symbols

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

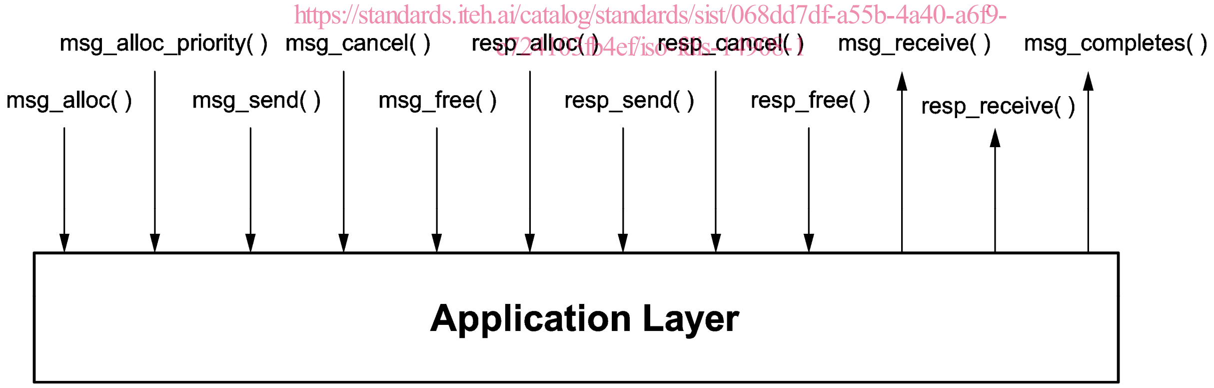

Figure 2 — Protocol terminology

3.2 Abbreviations

— CNP Control Network Protocol

The Protocol Data Unit (PDU) abbreviations used throughout this International 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.

4 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 International 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.

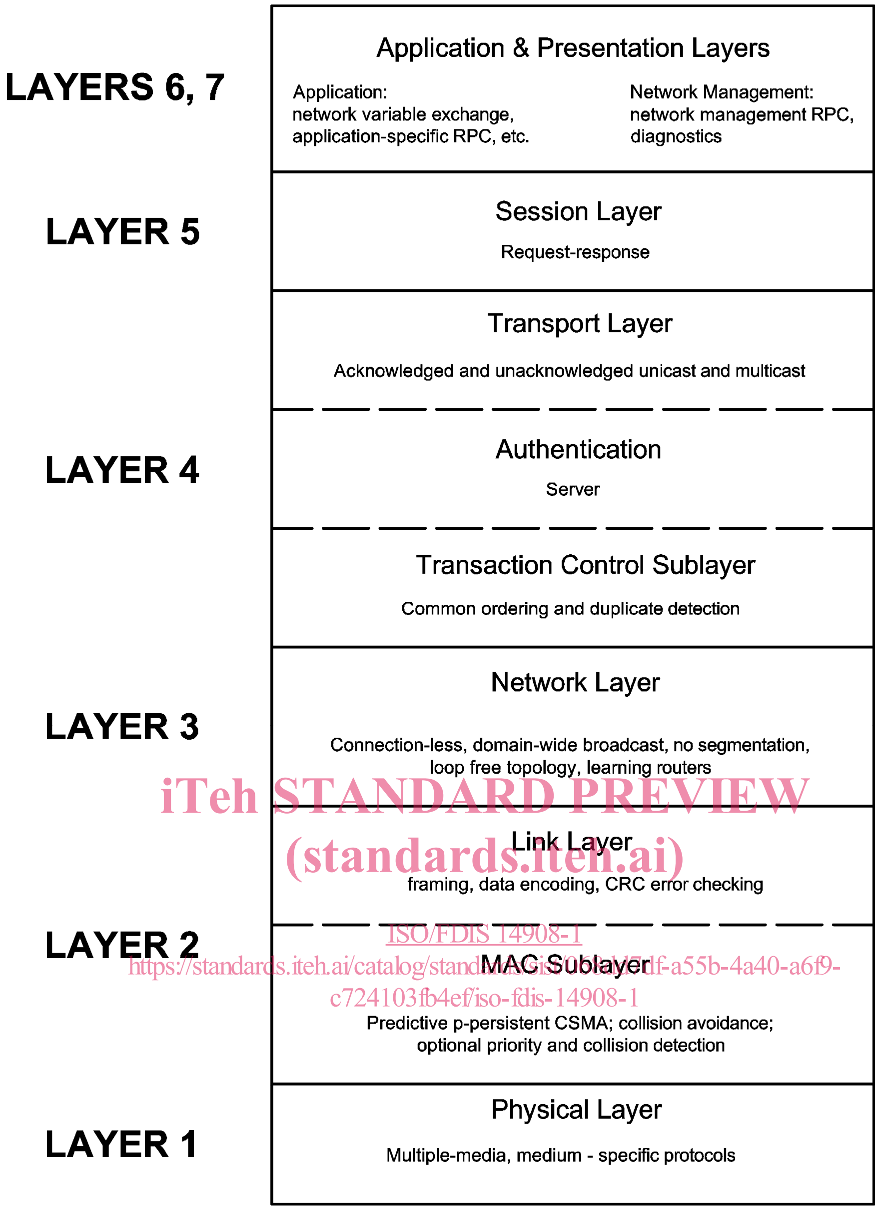

Figure 3 — Protocol layering

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 12). 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.

5 MAC sublayer

In this International 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 International Standard.

5.1 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:

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

where

W_{base} is the base window size. W_{base} is measured in time. Its duration, derived from Beta2 (see 5.7), equals 16 Beta2 slots.

5.2 Interface to the link layer

The MAC sublayer is closely coupled to the Link layer, described in clause 6. 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.

