FINAL
DRAFT

INTERNATIONAL STANDARD

ISO/FDIS 14908-4

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 4: IP communication

Interconnexion des équipements des technologies de l'information — Protocole de réseau de contrôle —

Partie 4: Communication IP

Please see the administrative notes on page iii

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/FDIS 14908-4:2011(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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 14908-4 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 part of ISO 14908-4 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 part of ISO 14908-4 is 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 4: IP communication

1 Scope

This part of ISO 14908 specifies the transporting of the Control Network Protocol (CNP) packets for commercial local area control networks over Internet Protocol (IP) networks using a tunnelling mechanism wherein the CNP packets are encapsulated within IP packets. It applies to both CNP nodes and CNP routers.

The purpose of this part of ISO 14908 is to ensure interoperability between various CNP devices that wish to use IP networks to communicate using the CNP protocol.

The main body of this part of ISO 14908 is independent of the CNP protocol being transported over the IP network. The reader is directed to Annex A and Annex B, respectively, for the normative and informative aspects of this specification that are specific to ISO 14908-1.

Figure 1 shows a possible configuration of such CNP devices and networks connected to an IP network.

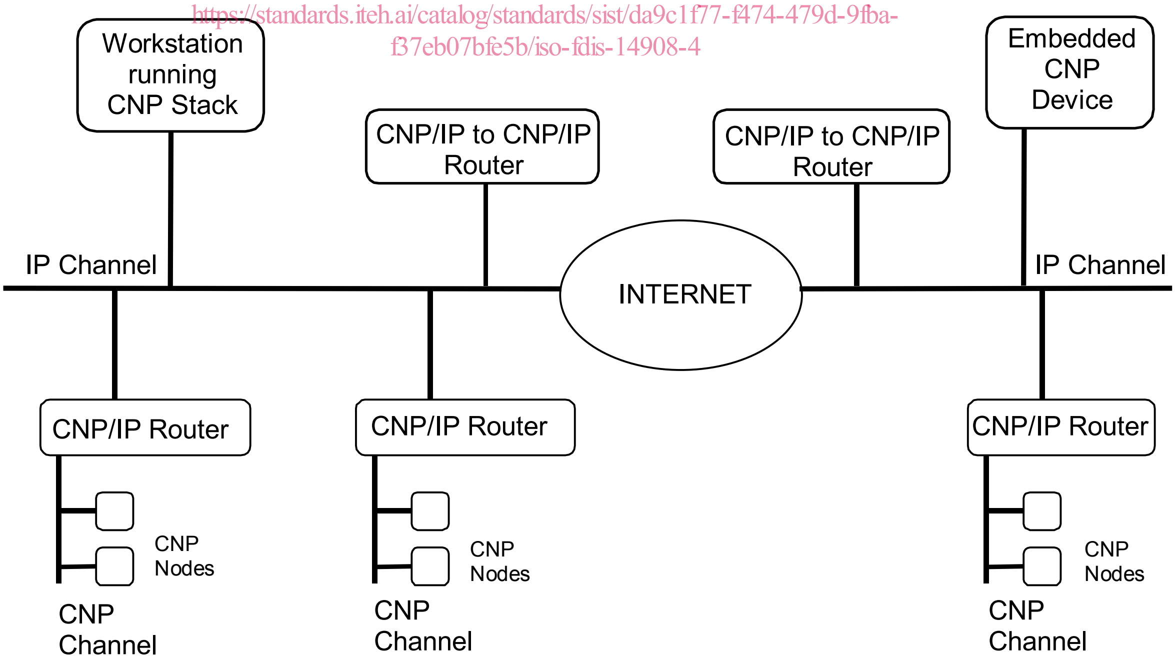

Figure 1 — Typical CNP/IP application

Figure 1 depicts two types of CNP devices: CNP nodes and CNP routers. It should be noted that the routers shown can route packets between typical CNP channels (such as twisted pairs or power lines) and an IP channel or it can route CNP packets between two IP channels. In this part of ISO 14908, the IP channel will be defined in such a way as to allow it to be used like any other CNP channel.

In the above diagram, the IP network can be considered to be one or more IP channels. This part of ISO 14908 covers only how CNP packets are transported over IP channels. It does not cover how CNP packets are routed between standard CNP channels and IP channels. This specification is not intended to cover the lower layers (physical, MAC and link layers) of either standard CNP or IP channels.

2 Terms, definitions and abbreviations

2.1 Terms and definitions

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

2.1.1
tunneling
encapsulation of one protocol's packet within the payload of another protocol's packets

2.1.2
channel
common communications transport mechanism that a specific collection of CNP devices share and communicate over without the use of a router

NOTE 1 Channels are used to transport CNP packets below the link layer of the CNP protocol stack.

NOTE 2 Typically, this refers to some types of physical media such as power lines, RFs, or twisted pairs, but in the case of IP networks, this channel is not physical, but a protocol tunnel.

2.1.3
CNP device
device that uses the CNP protocol to communicate with other CNP devices

NOTE Specifically, a CNP/IP device is a CNP device that communicates with other CNP devices over an IP channel.

2.1.4
CNP router
special type of CNP device that routes CNP protocol packets between two or more channels

NOTE Specifically, a CNP/IP router is a CNP router in which at least one of the channels it routes packets over is an IP channel.

2.1.5
CNP node
special type of CNP device that can send or receive CNP protocol packets, but does not route them between channels

NOTE 1 Specifically, a CNP/IP node is a CNP node in which at least one of the channels it sends and receives packets over is an IP channel.

NOTE 2 All CNP devices are either routers, nodes or both.

2.1.6
CNP group
collection of CNP devices that share a common multicast address

2.1.7
node ID
logical network address that differentiates nodes within the same subnet or domain

2.1.8
Must Be Zero
MBZ
reserved field that may be used in the following versions of the protocol

NOTE Such fields shall be sent as zero and ignored by the receiver in implementations conforming to the current version of this part of ISO 14908.

2.2 Abbreviations

CTP	Channel Timeout Period
CNP	Control Network Protocol
LFS	Last Forwarded Sequence
MBZ	Must Be Zero
NTP	Network Time Protocol
PSN	Packet Sequence Number
SA/DA	Source Address / Destination Address
SID	Session Identifier
SNTP	Simple Network Time Protocol
UDP	User Datagram Protocol

3 Requirements

The following is a set of general requirements for the transporting of CNP packets over IP channels:

- be as efficient as possible to allow quasi real-time operation;
- be independent of the application level interface used to receive the packets. For example the tunnelling protocol should not rely on the existence of a socket interface or how that interface may be used;
- insure that CNP packet ordering is preserved;
- insure that CNP packets that are “stale” (outside the maximum timeout characteristics of the IP channel) are not forwarded;
- detect packets that get duplicated in the IP network;
- support IP routing devices that prioritise IP packets;
- optional security measures to prevent malicious users from tampering with devices;
- scalable;
- allow status information to be extracted from CNP/IP devices;
- support the exchange of configuration information between CNP/IP devices and configuration servers.

4 CNP/IP device specification

4.1 IP-related device specifications

A CNP/IP device shall behave like any standard IP host capable of exchanging IP packets with any other IP host either on the same IP subnet or anywhere else in the Internet cloud. A CNP/IP device shall have a single unicast IP address and may be capable belonging to as many as 32 multi-cast groups. It is optional that a CNP/IP device support multi-casting. This document does not address the routing of IP packets between subnets or through the Internet. The CNP/IP devices shall be compatible with whatever standard mechanisms (IP routers, switches etc.) are required to perform the IP routing functions.

4.2 CNP-related device specifications

4.2.1 Packet formats

The general format of CNP packets which are tunnelled over the IP channel are those packets that are received from or sent to the Link layer (layer 2) of the CNP protocol stack. Refer to Annex A for a precise specification of the packet formats corresponding to the CNP protocol.

4.2.2 Addressing schemes

Different CNP protocols generally use different addressing schemes to exchange packets. Although it is generally not necessary to understand the contents of a CNP packet or its addresses in order to tunnel CNP packets over IP, some aspects of the CNP addressing scheme are reflected in the process of configuration. This is especially true when it comes to setting up the IP channels that are used for tunnelling. Since CNP protocols use different addressing schemes the terminology used in the main body of this specification for describing addresses are meant to be general and rich enough to describe the superset of addressing schemes used in all CNP protocols. The following CNP addressing terms are used in this specification.

— Unique ID. This refers to an ID that is globally unique to all devices within a specific protocol. Unique ID's are generally fixed in nature in that they never change through the life of a device.

— Domain. This is the highest level of a three level hierarchical addressing scheme. Domain ID's should be unique within a particular network. This means that in a particular network where Domains are used if two devices have the same Domain ID they belong to the same Domain. Domain ID's are generally logical in nature and can be changed and configured.

— Subnet. This is the middle level of a three level hierarchical addressing scheme. Subnet ID's should be unique within a particular domain. This means that in a particular network where subnet ID's are used if two devices have the same Domain ID and the same Subnet ID then they belong to the same Subnet. Some CNP's do not use Domains in which case the Subnet may be the highest level of address for a device. Subnet ID's are generally logical in nature and can be changed and configured.

— Node. This is the lowest level of any hierarchical addressing scheme. Node ID's should be unique within a particular Subnet. No two devices within the same subset should have the same Node ID. Node ID's are generally logical in nature and can be changed and configured.

— Group. Groups are an orthogonal addressing scheme to the hierarchical Domain/Subnet/Node triplet just described. Groups are used to allow multi-casting of messages. Some CNP's may not support group addresses and even those that do will have different rules for how they relate to the other addressing schemes. These considerations are not relevant to this specification.

The definitions above are fairly general and are provided as a guideline for how to map the CNP protocol to these terms. In general how the various addressing schemes work within a CNP protocol are not relevant to this specification. It is only necessary to know what the various addressing terms refer to.

Of special note is how these addresses are used for routing within the CNP protocol. Therefore a table is given in the appendix that specifies how the appropriate addresses used in that protocol map to the terms given above.

5 IP channel

5.1 Specification

IP channels are not like typical CNP channels that currently exist. Typical CNP channels are physical busses by nature. This implies that all devices on the channel will by default receive all packets transmitted on that channel. In addition when a new device is added to the channel it is not necessary that other devices on the channel become aware of it before they can exchange packets. To transmit a packet on a channel it is only necessary that a device be capable of physically transmitting the packet on the channel, nothing more. If a device is simply physically connected to a channel it is capable of exchanging packets with other devices on the channel.

By contrast an IP channel is not physical, but logical in nature. There are a number of different physical media that can support IP communications and any of them should be capable of supporting a CNP channel. Because we are dealing with a logical channel it is necessary to “construct” the channel by informing each device on the channel of the existence of the other devices on that channel. In other words before a device can transmit a packet to some other device on an IP channel it shall be made aware of how to specifically send a packet to that device, i.e. its IP address.

Another significant difference between physical and logical channels is that in the case of typical physical channels it is possible to calculate fixed upper bounds on the length of time it will take a packet to traverse from one device to another once the packet is transmitted on the channel. This is not always possible for IP networks. The deviation of packet delivery times between CNP devices on an IP channel are much higher than those experienced with typical CNP channels.

As depicted in Figure 1 the IP channel is used as an intermediary transport mechanism for the CNP packets by a variety of CNP/IP devices. When a CNP packet is transported on an IP channel, an IP message encapsulating the CNP packets is sent to other CNP/IP devices on that IP channel. On reception of one of the IP messages by a CNP/IP device the CNP packets are extracted and processed. A single IP message may contain more than one CNP packet. Therefore the IP messages shall be formatted in such a way to allow the extraction of the individual CNP packets. This is referred to a packet “bunching”. CNP/IP devices shall support the reception of bunched packets. Likewise the bunching shall be done in such a fashion that each CNP packet contained within a bunched IP message is complete, i.e. CNP packets should not cross IP message boundaries as a result of bunching. It is also a requirement that intermediate IP devices be capable of unbundling bunched CNP packets and bunching them in a different manner before forwarding them.

The IP channel is specified by the list of unicast IP addresses, exactly one for each CNP/IP device. There is no maximum to the number of CNP/IP devices on a single IP channel.

If every CNP/IP device on an IP channel contained a list of unicast IP addresses for every other CNP/IP device on that IP channel, this is all that would be required to enable the tunnelling of CNP packets. In the most brute force approach, for each CNP packet to be forwarded on the IP channel a separate unicast IP message could be sent to each CNP/IP device in the channel. This does not scale very well so the following techniques will be used to reduce the IP traffic:

- IP multi-cast groups;
- selective forwarding.

IP multi-cast groups allow a single IP message to be sent to more than one CNP/IP device. Therefore a complete definition of a CNP/IP channel should contain not only the unicast IP addresses of all the CNP/IP devices on the channel but also the IP multi-cast groups to which they belong. Each CNP/IP device can belong to up to 32 multi-cast addresses.

Selective forwarding refers to examining the contents of the CNP packet before forwarding it to determine if it should be sent to a particular CNP/IP device. In order to do this additional CNP specific information shall be known about each potential destination. If the CNP/IP device is a router then the information necessary to perform selective forwarding is the routing tables of the CNP/IP router. If the device is simply a node then the domain, subnet, node id, unique id, and CNP groups that the node belongs to should be known. Therefore all this information is also part of a complete IP channel definition. In short a complete IP channel definition contains all known information that may be relevant to the forwarding of packets to the other CNP/IP devices in the IP channel. It is the universe of all relevant knowledge about the IP channel.

It is important that whatever forwarding scheme is used by a CNP/IP device the following conditions are always true:

a) CNP protocol packets are always received by all CNP/IP devices on the IP channel that need to receive them regardless of whether they are routers or nodes. If there is any ambiguity or uncertainty concerning which CNP/IP devices should receive a CNP packet then that packet may or may not be discarded depending upon specific implementation considerations of the device. The device may either forward the packet to all devices on the channel or it may simply discard it and not forward it to any;

b) a specific CNP packet should never be transmitted twice to the same CNP/IP device unless it is because of some retry mechanism above the link layer of the CNP protocol stack. Due to the nature of IP networks it may happen that a CNP/IP device may receive duplicate IP messages, but this should never be the result of the message being transmitted more than once from another CNP/IP device.

In addition selective forwarding can be performed on multi-cast groups if the groups were formed based upon some criteria. For example multi-cast group ‘A’ may contain all CNP/IP devices belonging to domain ID ‘W’. If a CNP packet is destined for domain ‘W’ then it would be sufficient to forward it only to multi-cast group ‘A’. In order to perform the selective forwarding on multi-cast addresses it is necessary to know if these groups were formed based upon some criteria.

In recognition of the fact that the complete IP channel definition can be unwieldy to use and maintain it is not a requirement that a CNP/IP device use it to forward packets. An alternative data structure called the “send list” can be maintained within each CNP/IP device. The send list may contain both unicast and multi-cast addresses and is subject to the same conditions given above. It can be created and loaded into the CNP/IP device with third party configuration tools that are better suited to creating multi-cast groups based upon some criteria. The send list represents the minimum amount of information required to allow proper forwarding of CNP packets and is structured to simplify the forwarding process such that the CNP/IP device need only forward packets to every address (unicast or multi-cast) in the send list. In order to allow a CNP/IP device to blindly forward packets to each address in the list the following conditions shall be true:

i) CNP protocol packets shall be received by all CNP/IP devices that need to receive them regardless of whether they are routers or nodes (same as above);

ii) a specific CNP packet is never transmitted twice to the same CNP/IP device (same as above);

iii) if device A is a destination in device B’s send list then device B should be a destination in device A’s send list. This is necessary to support the acknowledged service of the CNP protocol.

It should be possible to perform simple forms of selective forwarding using the send list by associating characteristics with the multi-cast entries in the list.

In general it is important to note that the IP channel definition represents complete global information about the IP channel while the send list is derived and may result from an intelligent grouping of devices based upon some characteristic. The send list’s main purpose is to allow fairly efficient operation of CNP/IP devices without requiring them to do extensive processing of the complete channel definition list. It is also important to note that the send list is a configured property of a CNP/IP device meaning that it is controlled and input to a device through some explicit configuration process. Although the send list is a configured property it does not preclude a CNP/IP device from doing self-configuration and calculating its own send list.

In order to have tight controls over the behaviour of CNP/IP devices and how they forward packets it should be possible to configure a CNP/IP device to use an explicit send list and ignore any IP channel configuration information it may have.

5.2 IP transport mechanisms

5.2.1 General

IP is a Network level protocol as shown in Figure 2. It is designed to operate over a wide range of physical media and link layer protocols. As such this document does not specify anything about the link or physical layers of the IP stack.

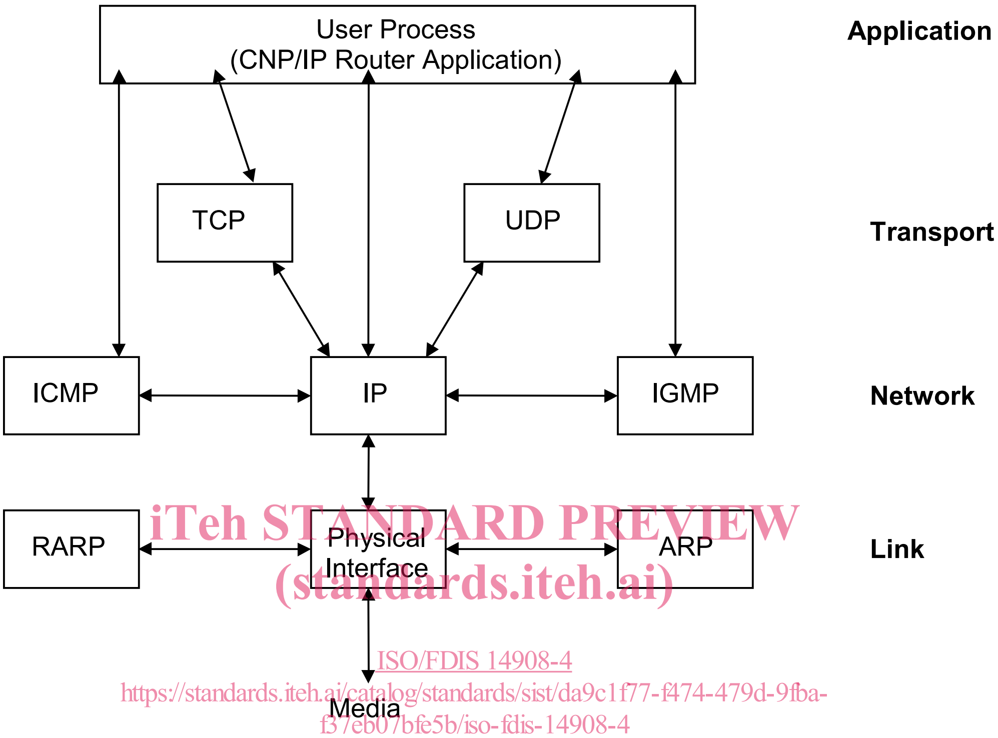

Figure 2 — IP protocol stack

As depicted in Figure 2 the three most common mechanisms used to transport IP packets are the following:

- raw IP;
- TCP;
- UDP.

TCP (refer to RFC 793) and UDP (refer to RFC 768) are transport protocols built on top of IP (refer to RFC 791). Given the increased efficiencies of UDP regarding the transport of CNP data messages and its support of multi-cast addressing, it will be used to communicate between CNP/IP devices. All CNP/IP devices shall support UDP. TCP has some advantages for use in the configuration process and may be supported for certain types of messages in addition to UDP. TCP support in CNP/IP devices is optional.

To address the sequencing issue there will be a sequence number added to the header of packets to help in sequencing them. All UDP datagrams shall be transmitted with valid checksums.

In order to send a packet via TCP/UDP it is necessary to define a port number in addition to the IP address. In general port numbers are configurable and will be used for different purposes as defined below. Refer to Annex B for recommendations on port number to use for CNP.

Using UDP, datagrams can be sent using either unicast or multi-cast addressing. Unicast is point-to-point meaning that a datagram is sent from one IP host to a single other IP host. It is much more efficient to use multi-cast addressing when sending the same datagram to multiple IP hosts. Therefore it is recommended that CNP/IP devices support both unicast and multi-cast IP addressing. Recall that an IP channel is defined by a list of IP addresses. A channel definition or send list can contain any combination of unicast and multi-cast addresses. It is not required that a CNP/IP device support multi-cast in order to inter-operate with a CNP/IP device that does.

In order for a CNP/IP router to use multi-cast addressing across IP routers it will be necessary for the CNP/IP device to inform the IP router of its intention to join the multi-cast group. There are well-established methods for doing this and it is beyond the scope of this document to specify how it is done. The reader should consult RFC 1112.

5.2.2 Informative considerations

Some IP networks contain NAT routers. These routers cannot handle protocols which embed IP addresses in their payloads unless they are specifically designed to do so. The same will be true of the tunnelling protocol specified in this document. In general this protocol will not work across NAT routers. The protocol can still be used in a network that uses NAT routers, as long there exists a router that is capable of handling this protocol. That could either be the NAT router itself or another CNP/IP to CNP/IP router that sits in the same area of the network as the NAT router.

6 CNP/IP device

6.1 Configuration of a CNP/IP device

The CNP/IP device has a dual personality. From a CNP point of view, it is a CNP node on a CNP channel and has all such characteristics. These parameters can be configured and managed using the standard CNP network management procedures and messages.

From the IP point of view, the CNP/IP device is an IP host on an IP network and thus has to be configured like any other host on an IP network.

In addition, there is configuration information that defines the logical IP channel associated with that CNP/IP device.

This clause describes only those elements relevant to configuring the IP host and IP channel parameters.

In general all IP host and channel parameters will be configurable using a number of techniques and protocols. As a minimum all CNP/IP devices shall support manual configuration of the forwarding mechanism for that device in order to guarantee a minimum level of interoperability between devices that may be configured in different ways. By forwarding we mean the act of tunnelling as described above to the other devices on the IP channel.

6.2 Configuration parameters

6.2.1 General

This subclause identifies the parameters that a CNP/IP uses (or may use) to operate. This subclause is not intended to define the data structures used to store the information or define the messages that are used to exchange them. Its only purpose is to have a consolidated section in which all the parameters of a CNP/IP device are identified and defined. Subsections discuss mechanisms for communicating this information between devices.

There are three relevant data sets that form the parameters contained within a CNP/IP device:

- CNP/IP channel definition as described in Clause 5;
- send list as described in Clause 5;
- device parameters relevant to its existence on a CNP/IP channel.

6.2.2 Channel definition parameters

A complete channel definition is logically a list of every CNP/IP device on the channel. Each of the devices on the channel can be associated with the following type of information:

- multi-cast support (yes or no). Since this is optional there shall be an indication of whether it is supported;
- TCP support (yes or no). Since this is optional there shall be an indication of whether it is supported;
- CNP/IP device type (router, node, proxy etc.);
- CNP router type (repeater, learning, configured etc.);
- CNP “Wants all Broadcasts” flag;
- name. Simple text string used for identification purposes;
- channel timeout. This parameter is global to the channel. Each device has this value but it is the same for all devices;
- IP address. This is the unicast IP address of the device.
- unicast port for listening to data;
- list of multi-cast address/port number pairs a CNP/IP device listens on;
- CNP specific unique device ID 1 (router near side or node);
- CNP specific unique device ID 2 (router far side);
- CNP specific unique device ID 3 (auxiliary for configuration);
- CNP Domain length and ID, subnet, node address for each domain;
- the parameters specific to nodes are: CNP group membership info;
- the parameters specific to routers are: CNP routing table.

Note that this list is representative in nature. Complete details as required are left to later clauses of this International Standard.

The tunnelling protocol defined in this specification does not require any specific CNP addressing scheme. The following CNP address types are supported:

- unique device ID;
- domain ID;
- subnet ID;
- node ID;
- group ID.

Refer to Annex A for the specific addressing conventions that correspond to the address types listed above.

6.2.3 Send List arameters

The following parameters are used to define the Send List:

- list of unicast IP addresses and ports;
- list of multi-cast IP addresses and ports.

6.2.4 Device parameters

- IP gateway address;
- IP subnet mask;