SLOVENSKI STANDARD
SIST EN 14908-7:2020

01-februar-2020

Odprta izmenjava podatkov v avtomatizaciji stavb, regulaciji in upravljanju stavb - Protokol regulacijske mreže - 7. del: Komunikacija preko spletnega protokola

Open communication in building automation, controls and building management - Control Network Protocol - Part 7: Communication via internet protocols

Firmenneutrale Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Gebäude-Netzwerk-Protokoll - Teil 7: Kommunikation über Internetprotokolle

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion techniques du bâtiment - Protocol de bâtiment de réseau - Partie 7 : Communication via des protocoles internet

Ta slovenski standard je istoveten z: **EN 14908-7:2019**

ICS:

35.240.67	Uporabniške rešitve IT v gradbeništvu	IT applications in building and construction industry
91.140.01	Napeljave v stavbah na splošno	Installations in buildings in general
97.120	Avtomatske krmilne naprave za dom	Automatic controls for household use

SIST EN 14908-7:2020 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 14908-7

December 2019

ICS 35.240.67; 91.140.01; 97.120

English Version

Open communication in building automation, controls and building management - Control Network Protocol - Part 7: Communication via internet protocols

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment - Protocole de contrôle du réseau - Partie 7 : Communication via les protocoles internet

Firmenneutrale Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Gebäude-Netzwerk-Protokoll - Teil 7: Kommunikation über Internetprotokolle

This European Standard was approved by CEN on 13 July 2019.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 14908-7:2019 E

Contents

Page

European foreword 4
Introduction 5
1 Scope 6
2 Normative references 6
3 Terms and definitions 6
4 Addressing 9
4.1 Overview 9
4.2 Network Address Mapping 10
4.2.1 General 10
4.2.2 IP-70 10
4.2.3 IP-100 11
4.3 Network Address Translation 13
4.4 Network Address Assignment with DHCP and ISI 13
4.5 Unique Node ID 14
4.6 Non-unique ID 14
5 Protocol Modes 15
6 Packet Format 15
6.1 CNP/IP-AN Packet Format 15
6.2 CNP/IP-CN Packet Format 20
6.2.1 General 20
6.2.2 CNP/IP-CN Protocol Version 0 Packet Format 20
6.2.3 CNP/IP-CN Protocol Version 1 Packet Format 20
6.2.4 CNP/IP-CN Protocol Version 2 Packet Format 21
7 Domain Configuration 23
8 Network Management Messages 23
8.1 General 23
8.2 Expanded Network Management Messages 24
8.2.1 General 24
8.2.2 Query Network Management Command Version and Capabilities (Code 1) 24
8.2.3 Join OMA Domain (Code 7) 25
8.2.4 Query OMA Domain (Code 8) 25
8.2.5 Query OMA Key (Code 9) 26
8.2.6 Update OMA Key (Code 10) 27
8.2.7 Node NAT Announcement (Code 21) 28
8.2.8 Subnet NAT Announcement (Code 22) 28
8.2.9 Set NAT Announcement Period (Code 23) 29
8.2.10 Query NAT Announcement Period (Code 24) 29
8.2.11 Query IP Address (Code 25) 30
8.3 ISI Network Management Messages 31
8.3.1 General 31
8.3.2 Domain Resource Usage (ISI Code 0) 31
8.3.3 Extended Domain Resource Usage (ISI Code 1) 32
8.3.4 Open Enrollment (ISI Code 2) 33

8.3.5 Extended Open Enrollment (ISI Code 3) 34
8.3.6 Automatic Enrollment (ISI Code 4) 35
8.3.7 Extended Automatic Enrollment (ISI Code 5) 36
8.3.8 Automatic Enrollment Reminder (ISI Code 6) 38
8.3.9 Extended Automatic Enrollment Reminder (ISI Code 7) 39
8.3.10 Domain ID Request (ISI Code 8) 40
8.3.11 Domain ID Response (ISI Code 9) 41
8.3.12 Domain ID Confirmation (ISI Code 10) 42
8.3.13 Enrollment Cancellation (ISI Code 12) 42
8.3.14 Enrollment Cancellation (ISI Code 12) 43
8.3.15 Enrollment Confirmation (ISI Code 13) 43
8.3.16 Enrollment Acceptance (ISI Code 14) 44
8.3.17 Connection Deletion Request (ISI Code 15) 45
8.3.18 Connection Status Information (ISI Code 16) 45
8.3.19 Control Request (ISI Code 17) 46
8.3.20 Control Response (ISI Code 18) 47
8.3.21 Connection Table Read Request (ISI Code 19) 47
8.3.22 Connection Table Read Success (ISI Code 20) 48
8.3.23 Connection Table Read Failure (ISI Code 21) 48

Bibliography 49

European foreword

This document (EN 14908-7:2019) has been prepared by Technical Committee CEN/TC 247 “Buildings 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 June 2020 and conflicting national standards shall be withdrawn at the latest by June 2020.

This European Standard is part of a series of European Standards for open data transmission in building automation, control and in building management systems. The content of this standard covers the data communications used for management, automation/control and field functions. This European Standard is based on the American standards EIA/CEA-709.1-B Control Network Protocol Specification.

EN 14908-7 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: Project Implementation Guideline*

— *Part 6: Application elements*

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

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 standardized way. It defines communication capabilities.

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

This European Standard has been made in response to the essential requirements of the Construction Products Regulation.

The European Committee for Standardization (CEN)] draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning Patent No. US 9521219 B2, “Systems, methods, and apparatuses using common addressing” and Patent No. US 8374104 B2, “Simple installation of devices on a network” which is claimed to be relevant for the following clauses of this document:

Clause 4 – Addressing

Clause 8 – Network Management Messages

CEN takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured CEN that he/she is 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 this patent right is registered with CEN. Information may be obtained from:

Adesto Technologies Corporation

3600 Peterson Way

Santa Clara, CA 95054, USA

phone +1–408–938–5224

www.adestotech.com

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

1 Scope

This document specifies a communication protocol for networked control systems. The protocol provides peer-to-peer communication for networked control using web-services. The document describes services in layer 2 and layer 3.

The layer 2 (data link layer) specification also describes the MAC sub-layer interface to the physical layer. The physical layer provides a choice of transmission media. The layer 3 (network layer), as described in EN 14908-1, is integrated in UDP/IP communication using IPv4 and IPv6 protocols.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

EN 14908-1, *Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 1: Protocol Stack*

EN 14908-2, *Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 2: Twisted Pair Communication*

EN 14908-3, *Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 3: Power Line Channel*

EN 14908-4, *Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 4: IP Tunneling*

EN 14908-6, *Open Data Communication in Building Automation, Controls and Building Management - Control Network Protocol - Part 6: Application elements*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

NOTE For the purposes of this document, the following subclauses define the basic terminology employed throughout this document. Some of them are used as normal English terms and have the same meaning as in the context of the standard. 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, and in some cases also do network address mapping or translation as described in *4.2 Network Address Mapping* and *4.3 Network Address Translation*

3.1
channel
logical link between one or more communication nodes

Note 1 to entry: Usually used interchangeably with a link. However, multiple channels can be multiplexed on a given link. For example, IP 70, IP 100, and IP 852 can be used to implement three different channels on the same Ethernet link. Likewise, a single IP 70, IP 100, or IP 852 channel can span multiple native IP links.

3.2
CNP UDP
UDP messages on a CNP/IP channel that are not used for CNP/IP control services

3.3
CNP/IP
control network protocol with control services defined by EN 14908-1 Layers 4 through 7, and transport services based on the link protocol as defined in this standard

3.4
CNP/IP-AN
CNP/IP on a link that natively supports IP communication including Ethernet and Wi-Fi

Note 1 to entry: The CNP/IP-AN protocol is based on Layers 4 to 7 of the EN 14908-1 Control Network Protocol on top of UDP and IPv4 or IPv6.

3.5
CNP/IP-CN
CNP/IP on a native CNP link such as a link hosting a TP/FT-10 channel defined by EN 14908-2, a PL-20 channel defined by EN 14908-3, or an IP-852 channel defined by EN 14908-4

3.6
CNP/IP control services
defined by EN 14908-1 Layers 4 through 7, including reliable transport, request/response, multicast, authentication, and network variables

3.7
CNP/IP internetwork address
internetwork address as defined by IPv4 or IPv6

Note 1 to entry: A CNP/IP device shall have a CNP/IP internetwork address. If the internetwork address can be mapped from the CNP/IP network address, the internetwork address is a mapped IP address. If not, it is a translated IP address. The CNP/IP internetwork address may be the same as the host IP address, but it can be different.

3.8
CNP/IP network address
network address as defined by the EN 14908-1 protocol

Note 1 to entry: All CNP/IP devices in a network domain have an EN 14908-1 network address and use CNP/IP network addressing to communicate with other CNP/IP devices in the same domain.

3.9
CNP/IP transport services
layer 1 to 3 services for the CNP/IP protocol

Note 1 to entry: The transport services are defined based on the link protocol. For native IP channels such as Ethernet and Wi-Fi, the transport services are defined by the RFC 768 User Datagram Protocol (UDP) and the RFC 791/793 IPv4 protocol or RFC 2460 IPv6 protocol, and the CNP/IP protocol is referred to as CNP/IP-AN. For EN 14908-1 native CNP channels such as the TP/FT 10 channel type defined by EN 14908-2, the layer 2 through 3 transport services are defined by the EN 14908-1 protocol standard and the protocol is referred to as CNP/IP CN.

3.10
configuration
non-volatile information used by the device to customize its operation

Note 1 to entry: 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.

3.11
domain
virtual network that is the network unit of management and administration

Note 1 to entry: 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.

3.12
gateway
interconnects networks at their highest protocol layers (often two different protocols)

Note 1 to entry: Two domains can also be connected through an application gateway.

3.13
group
uniquely identifiable set of nodes within a domain

Note 1 to entry: Within this set, individual members are identified by their member number. Groups facilitate one-to-many communication and support functional addressing.

3.14
link
physical layer 1 and 2 link

3.15
network variable
data value within a node with a value that is automatically propagated over the network whenever a new value is assigned to it by the node application

3.16
node
abstraction for a physical communicating device that represents the highest degree of address resolvability on a network

Note 1 to entry: 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 (UNID).

3.17
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

Note 1 to entry: 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.

3.18
service request message
network management message containing a node's Unique Node ID

Note 1 to entry: Used by a network management device that receives this message to install and configure the node. May be generated by application or system code, or may be triggered by an external hardware event, e.g. driving a service request input to a node low.

3.19
Standard Network Variable Types
SNVTs
variable types with agreed-upon semantics

Note 1 to entry: Variables with these types are interpreted by all applications in the same way, and are the basis for interoperability. SNVTs are defined in EN 14908-6.

3.20
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

3.21
transaction
sequence of messages that are correlated together

Note 1 to entry: 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 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 Addressing

4.1 Overview

A CNP/IP device shall use layer 3 network addresses as defined by EN 14908-1 to communicate with other CNP/IP and native CNP devices. These network addresses are assigned by network management tools in managed networks, and are assigned by the devices themselves in self-installed networks.

When communicating with network variables as defined by EN 14908-1, a CNP/IP device shall use layer 6 selectors as defined by EN 14908-1 combined with network addresses to exchange network variable updates with other CNP/IP and native CNP devices. Network variables enable peer-to-peer data exchanges between a pair of devices, a group of devices, all devices in a subnet, or all devices in a network.

A CNP/IP device may have one or more IPv4 or IPv6 CNP/IP internetwork addresses and one or more IPv4 or IPv6 host IP addresses. If a CNP/IP internetwork address can be mapped to a host IP address as described in *4.2 Network Address Mapping*, it is called a *mapped host IP address*. If it cannot be mapped, it is called a *translated host IP address*. Network address translation is described in *4.3 Network Address Translation.*

A CNP/IP message can be sent to a device with a mapped IP address by specifying the CNP/IP internetwork address as the destination address. If the host IP address is translated, a CNP/IP message shall be sent to the translated host IP address, and the IP address shall be translated to the CNP/IP internetwork address by an intermediate router, making a mapped IP address more efficient than a translated address. However, a device may be constrained to use a host IP address that cannot be mapped to a CNP/IP internetwork address. For example a workstation may be installed in an environment that requires assignment of its address by a DHCP server that is configured to assign IP addresses in an IP subnet than is not compatible with the CNP/IP internetwork address, and as a result a translated IP address is required.

4.2 Network Address Mapping

4.2.1 General

A CNP/IP device may have multiple EN 14908-1 layer 3 addresses. There are two types of CNP/IP layer 3 addresses. They are *unicast* and *multicast* addresses. Unicast addresses are used to uniquely identify an individual CNP/IP device. If a unicast address can be mapped to a host IP address as described in this section, it is called a *mapped IP address*. If a unicast address cannot be mapped to a host IP address, it shall be translated as described in *4.3 Network Address Translation*. Multicast addresses are used to identify a group of CNP/IP devices. Multicast addresses can always be mapped to IP addresses.

The format of the IP address is channel-type dependent. For CNP/IP-AN IP-70 channels, a standard IPv4 network address format shall be used. For CNP/IP-AN IP-100 channels, a standard IPv6 network address format shall be used. For CNP/IP-CN and native CNP channels, a standard EN 14908-1 network address format shall be used. An address can be converted from CNP/IP-AN format to CNP/IP-CN format and vice versa using a stateless algorithm as described in the next two sections. A CNP/IP-AN to CNP/IP-CN router shall use this algorithm to route packets between the CNP/IP-AN and CNP/IP-CN channels, automatically converting the addresses as required. Since the algorithm is stateless, CNP/IP routers do not require special provisioning or configuration to perform the network address format conversion. The following sections describe the formats and requirements for unicast and multicast CNP/IP network addresses.

4.2.2 IP-70

4.2.2.1 Introduction

IP-70 is the CNP/IP-AN channel using IPv4 addressing. All devices communicating on the IP-70 channel shall implement the IPv4 addressing scheme described in this sub-chapter. The CNP/IP domain length for networks with an IP-70 channel can be 0, 1, or 3 bytes. CNP/IP on an IP-70 channel does not support 6-byte domains—an IP-100 channel is required for CNP/IP-AN on a CNP network with a 6-byte domain.

4.2.2.2 Unicast Address Mapping

Network address conversion for IPv4 unicast addresses is dependent on the CNP/IP domain length and value. The following Table 1 summarizes the conversion between a CNP/IP-AN channel and a CNP/IP-CN channel for a CNP/IP address with a domain of up to 3 bytes (*D1*, *D2*, and **00**), a one-byte subnet ID (*S*), and a one-byte node ID (*N*).

Table 1 — Conversion between a CNP/IP-AN channel and a CNP/IP-CN channel

CNP/IP Domain Length	CNP/IP Domain ID Value	LAN IPv4 Address	CNP EN 14908-1 Address
0		**192.168**.*S.N*	*S, N*
1	*D1*	**10**.*D1.S.N*	*D1, S, N*
3	*D1D2***00**	*D1.D2.S.N*	*D1D2***00**, *S, N*

The CNP/IP domain, subnet, and node IDs for all nodes in a CNP network with an IP-70 channel shall meet the following requirements:

— The domain ID length shall be 0, 1, or 3 bytes. A 6-byte CNP/IP domain ID is not valid for a CNP network with an IP-70 channel.

— The first byte of a 3-byte domain ID shall not be 10 (0x0A), or a value between 224 (0xE0) and 239 (0xEF).

— The first two bytes of 3 byte domain ID shall not be 192, 168 (0xC0, 0xA8).

— The third byte of a 3-byte domain ID shall be 0.

— The subnet ID shall be a value between 1 and 254, inclusive. The subnet ID cannot be 0 or 255.

— The node ID shall be a value between 1 and 127, inclusive. The node ID cannot be 0 or a value greater than 127.

Other domain IDs may not be valid in a particular IP infrastructure as they may conflict with existing IP addresses.

4.2.2.3 Multicast Address Mapping

There are three types of CNP/IP multicast addresses. They are *domain broadcast*, *subnet broadcast*, and *group* addresses. Network address conversion for IPv4 multicast addresses is dependent on the type of multicast, as shown in the Table 2 below:

Table 2 — Type of multicast

CNP/IP Multicast Address Type	CNP/IP Address Value	LAN IPv4 Address	CNP EN 14908-1 Address
Domain Broadcast		**239.192.0.0**	14908–1 Domain Broadcast
Subnet Broadcast	*S*	**239.192.0.***S*	14908–1 Subnet Broadcast to Subnet *S*
Group	*G*	**239.192.**1.*G*	14908–1 Group *G*

4.2.3 IP-100

4.2.3.1 Introduction

IP-100 is the CNP/IP-AN channel using IPv6 addressing. All devices communicating on the IP-100 channel shall implement the IPv6 addressing scheme described in this sub-chapter. The CNP/IP domain length for networks with an IP-100 channel shall be 6 bytes. CNP/IP on an IP-100 channel does not support 0, 1, or 3-byte domains—an IP-70 channel is required for CNP/IP-AN on a CNP network with a 0, 1, or 3-byte domain.

4.2.3.2 Unicast Address Mapping

Network address conversion for IPv6 unicast addresses maps the CNP/IP domain, subnet, and node ID directly into an IPv6 address as follows:

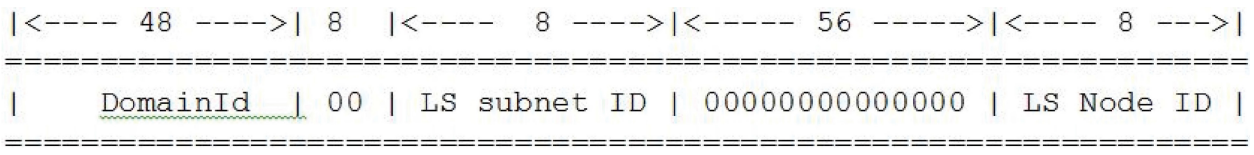

Figure 1 — Unicast Address Mapping

The CNP/IP domain, subnet, and node IDs for all nodes in a CNP network with an IP-100 channel shall meet the following requirements:

— The domain ID length shall be 6 bytes. A 0, 1, or 3-byte CNP/IP domain ID is not valid for a CNP network with an IP-100 channel.

— The subnet ID shall be a value between 1 and 254, inclusive. The subnet ID cannot be 0 or 255.

— The node ID shall be a value between 1 and 127, inclusive. The node ID cannot be 0 or a value greater than 127.

4.2.3.3 Multicast Address Mapping

A CNP multicast address is mapped into an IPv6 multicast address with 0xFF18 scope as follows:

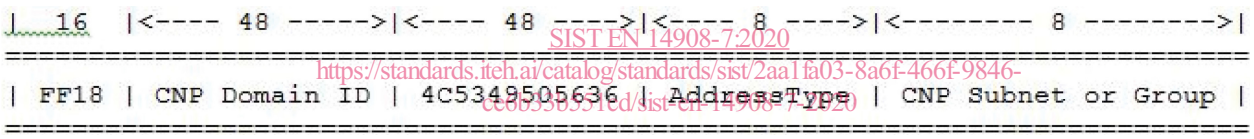

Figure 2 — Multicast Address Mapping

AddressType	CNP address type for multicast addresses.
0:	Subnet or domain broadcast. Specifies a domain broadcast if the CNP Subnet or Group field is zero; specifies a subnet broadcast to the specified subnet if the CNP Subnet or Group field is not zero.
1:	Group multicast to the group specified in the CNP Subnet or Group.

Unique Node ID (UNID) Address Mapping

A 48-bit CNP Unique Node ID (UNID) is mapped into an IPv6 unicast address as follows:

```
|<---- 48 ----->|  8  |      8      |<-------------- 64 ------------->|
======================================================================
| CNP Domain ID | 00  | CNP Subnet | EUI-64 derived from CNP/IP UNID |
======================================================================

          |0       0|       1|1       2|2       3|3       3|4       4|
          |0       7|       5|6       3|4       1|2       9|0       7|
          +--------+--------+--------|--------+--------+--------+
          |mmmmmmmm|ssssssss|ssssssss|ssssssss|ssssssss|bbbbbbbb| CNP/IP UNID
          +--------+--------+--------+--------+--------+--------+
           || /       /        /          \         \       \
           ||/       /        /            \         \       \
           ||       /        /              \         \       \
           ||      /        /                \         \       \
          /||     /        /                  \         \       \
         / ||    /        /                    \         \       \
     |0 /  ||   /    1|1  |           3|3       \     4|4 \       \    6|
     |0v   vv  v     5|6  v           1|2        v    7|8  v       v   3|
     +----------------+----------------+----------------+----------------+
     |mmmmmmugssssssss|ssssssss11111111|11111110ssssssss|ssssssssbbbbbbbb| IID
     +----------------+----------------+----------------+----------------+
```

Figure 3 — 48-bit CNP Unique Node ID (UNID) mapped into an IPv6 unicast address

4.3 Network Address Translation

When a CNP/IP device with a translated source address sends a message, it shall embed its CNP/IP internetwork address within the UDP payload as the source address. This enables the destination device or devices and any intermediate routers to determine the CNP/IP source address.

Nodes with a translated address shall send periodic Node NAT Announcement messages as defined in *8.1.1 Query Network Management Command Version and Capabilities (Code 1)*, at the rate configured by Set NAT Announcement Period messages as defined in *8.1.8 Set NAT Announcement Period*.

Routers with a translated subnet address shall send periodic Subnet NAT Announcement messages as defined in *8.1.7 Subnet NAT Announcement*, at the rate configured by Set NAT Announcement Period messages as defined in *8.1.8 Set NAT Announcement Period*.

4.4 Network Address Assignment with DHCP and ISI

A CNP/IP device shall support CNP/IP network address assignment by a network management tool as described in EN 14908-1. On startup, a CNP/IP node shall take the following steps to configure its CNP/IP network and internetwork addresses:

1) If a CNP/IP network address has been configured, the network and internetwork addresses shall be set based on the configured network address and the remaining steps shall be skipped.

2) If a CNP/IP network address has not been configured, the device shall initially be configured to use the domain or domains in the following table, and shall send DRUM broadcast messages as described in the following table. The secondary domain and DRUM broadcast source address in the following table cannot be used as a destination address, but shall be used as the source address when sending Service messages and responses.