SLOVENSKI STANDARD
SIST EN 13321-2:2013

01-junij-2013

Nadomešča:
SIST EN 13321-2:2007

Odprta izmenjava podatkov v avtomatizaciji stavb in izvršnih elementov ter pri upravljanju stavb - Elektronski sistemi za stanovanja in stavbe - 2. del: Komunikacija KNTnet/IP

Open Data Communication in Building Automation, Controls and Building Management - Home and Building Electronic Systems - Part 2: KNXnet/IP Communication

Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Elektrische Systemtechnik für Heim und Gebäude - Teil 2: KNXnet/IP Kommunikation

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment - Systèmes électroniques pour la maison et le bâtiment - Partie 2: Communication KNXnet/IP

Ta slovenski standard je istoveten z: **EN 13321-2:2012**

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 13321-2:2013 **en,fr,de**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 13321-2

December 2012

ICS 35.240.99; 97.120

Supersedes EN 13321-2:2006

English Version

Open Data Communication in Building Automation, Controls and Building Management - Home and Building Electronic Systems - Part 2: KNXnet/IP Communication

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment - Systèmes électroniques pour la maison et le bâtiment - Partie 2: Communication KNXnet/IP

Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement - Elektrische Systemtechnik für Heim und Gebäude - Teil 2: KNXnet/IP-Kommunikation

This European Standard was approved by CEN on 30 September 2012.

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

Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 13321-2:2012: E

Contents

Page

Foreword

This document (EN 13321-2:2012) 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 June 2013, and conflicting national standards shall be withdrawn at the latest by June 2013.

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 13321-2:2006.

Whereas ENV 13321-2:2000 described the transmission of EIB packets over Ethernet including the frame encoding, this document describes the transmission of HBES packets using the Internet Protocol. Details of the HBES packet frames are covered in part 1 of EN 13321, removing the need to explicitly describe the HBES frames in this document.

This document is Part 2 of the EN 13321 series of European Standards under the general title *Open data communication in building automation, controls and building management — Home and building electronic systems*, which consists of the following parts:

— *Part 1: Product and system requirements*;

— *Part 2: KNXnet/IP communication*.

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, 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.

Introduction

This European Standard is intended for the design of new buildings and the retrofit of existing buildings in terms of acceptable indoor environment, practical energy conservation and efficiency.

This standard defines the integration of KNX protocol implementations within the Internet Protocol (IP) named KNXnet/IP.It defines a standard protocol, which is implemented within KNX devices, Engineering Tool Software (ETS) and other implementations to support KNX data exchange over IP networks. In fact, KNXnet/IP provides a general framework, which accommodates several specialised “Service Protocols” in a modular and extendible fashion.

The KNXnet/IP standard consists of the following clauses:

— Clause 1, Overview

— Clause 2, Core Specification

— Clause 3, Device Management

— Clause 4, Tunnelling

— Clause 5, Routing

— Clause 6, Remote Diagnosis and Configuration

Additional clauses may be added to the KNXnet/IP standard in the future at which time Clause 1 “Overview” as well as Annex A will need to be updated.

KNXnet/IP supports different software implementations on top of the protocol. More specifically, these software implementations can be Building Management, Facility Management, Energy Management, or simply Data Base and SCADA (Supervision, Control and Data Acquisition) packages.

Most of these packages need to be configured for the specific user application. In order to simplify this process and cut costs for engineering, KNXnet/IP provides simple engineering interfaces, namely a description “language” for the underlying KNX system. This may be done off-line, e.g. generated as an ETS export file, or on-line by a mechanism that self-describes the underlying KNX system (reading data from the system itself).

In conjunction with the EIB/KNX-to-BACnet mapping described in EN ISO 16484-5, EIB/KNX installations can very easily be integrated into BACnet system environments.

KNXnet/IP supports:

— on-the-fly change-over between Operational modes (configuration, operation);

— event driven mechanisms;

— connections with a delay time greater than $t_{EIB\_transfer\_timeout}$ (e.g. network connection via satellite).

Clause 1, Overview

Clause 1 “Overview” provides a general overview of KNXnet/IP and covers security considerations.

Clause 2, Core specification

Clause 2 “Core Specification” defines a standard protocol which is implemented within KNXnet/IP devices and Engineering Tool Software to support KNX data exchange over IP networks.

This specific implementation of the protocol over the Internet Protocol (IP) is called KNXnet/IP.

This standard addresses:

— definition of data packets sent over the IP host protocol network for KNXnet/IP communication;

— discovery and self-description of KNXnet/IP servers;

— configuration and establishment of a communication channel between a KNXnet/IP client and a KNXnet/IP server.

Clause 3, Device Management

Clause 3 “Device Management” defines services for remote configuration and remote management of KNXnet/IP servers.

Clause 4, Tunnelling

Clause 4 “Tunnelling” defines services for point-to-point exchange of KNX telegrams over an IP network between a KNXnet/IP device acting as a server and a KNXnet/IP Client. This point-to-point exchange may be established by a super ordinate system for building automation or management functions or by an Engineering Tool Software. It supports all ETS functions for download, test, and analysis of KNX devices on KNX networks connected via KNXnet/IP servers. This includes changes of single KNX device object properties.

Tunnelling assumes that a data transmission round-trip between a KNXnet/IP Tunnelling client and KNXnet/IP servers takes less than $t_{KNX\_transfer\_timeouts}$.

Clause 5, Routing

Clause 5 “Routing” defines services for a point-to-multipoint exchange of KNX telegrams over an IP network between KNXnet/IP routers and/or KNX/IP devices.

Clause 6, Remote Diagnosis and Configuration

Clause 6 “Remote Diagnosis and Configuration” defines services for a point-to-point exchange of KNX telegrams over an IP network between KNXnet/IP routers and/or KNX/IP devices. The services provide means for diagnosing communication settings and for changing these remotely.

1 Scope

This European Standard defines the integration of KNX protocol implementations on top of Internet Protocol (IP) networks, called KNXnet/IP. It describes a standard protocol for KNX devices connected to an IP network, called KNXnet/IP devices. The IP network acts as a fast (compared to KNX transmission speed) backbone in KNX installations.

Widespread deployment of data networks using the Internet Protocol (IP) presents an opportunity to expand building control communication beyond the local KNX control bus, providing:

— remote configuration;

— remote operation (including control and annunciation);

— fast interface from LAN to KNX and vice versa;

— WAN connection between KNX systems (where an installed KNX system is at least one line).

A KNXnet/IP system contains at least these elements:

— one EIB line with up to 64 (255) EIB devices;
OR
one KNX segment (KNX-TP1, KNX-TP0, KNX-RF, KNX-PL110, KNX-PL132);

— a KNX-to-IP network connection device (called KNXnet/IP server);

and typically additional

— software for remote functions residing on e.g. a workstation (may be data base application, BACnet Building Management System, browser, etc.).

Figure 1 shows a typical scenario where a KNXnet/IP client (e.g. running ETS) accesses multiple KNX installed systems or KNX subnetworks via an IP network. The KNXnet/IP client may access one or more KNXnet/IP servers at a time. For subnetwork, routing server-to-server communication is possible.

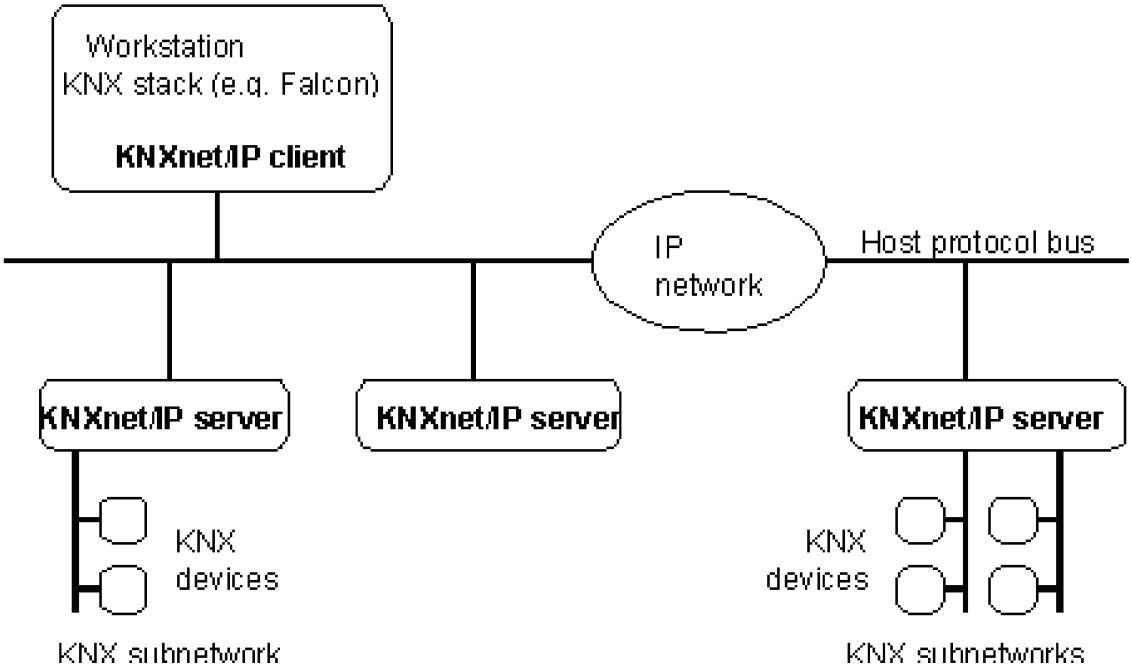

Figure 1 — Device types and configuration examples

2 Normative references

Not applicable.

3 Terms and definitions

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

3.1
subnet
portion of a network that shares a common address component known as the "subnet address"

Note 1 to entry: Different network protocols specify the subnet address in different ways.

3.2
Engineering Tool Software
ETS
software used to configure KNX devices

3.3
Host Protocol Address Information
HPAI
structure holding the IP host protocol address information used to address a KNXnet/IP endpoint on another KNXnet/IP device

3.4
communication channel
logical connection between a KNXnet/IP client and a KNXnet/IP server (or, in case of routing, between two or more KNXnet/IP servers)

Note 1 to entry: A communication channel consists of one or more connections on the definition of the host protocol used for KNXnet/IP.

3.5
KNX node
device implementing a KNX protocol stack and fulfilling the requirements for certification according to the KNX standard

3.6
KNXnet/IP server
KNX device with physical access to a KNX network implementing the KNXnet/IP server protocol to communicate with KNXnet/IP clients or other KNXnet/IP servers (in case of routing) on an IP network channel

Note 1 to entry: A KNXnet/IP server is by design always also a KNX node.

3.7
KNXnet/IP client
application using the KNXnet/IP client protocol to get access to a KNX subnetwork over an IP network channel

3.8
KNXnet/IP device
implementation of KNXnet/IP services on a KNX node (KNXnet/IP server) or any other hardware (KNXnet/IP client)

3.9
KNXnet/IP router
special type of KNXnet/IP device that routes KNX protocol packets between KNX sub-networks

3.10
Time To Live
TTL
maximum number of IP routers a multicast UDP/IP datagram may be routed through

Note 1 to entry: Each IP router the datagram passes decrements the TTL by one; the local host adapter also does this. When the TTL has reached zero, the router discards the datagram. When sending a datagram from the local host adapter, a TTL of zero means that the datagram never leaves the host. A TTL of one means that the datagram never leaves the local network (it is not routed).

3.11
KNXnet/IP Tunnelling
services for point-to-point exchange of KNX telegrams over an IP network between a KNXnet/IP device acting as a server and a KNXnet/IP client

3.12
Internet Control Message Protocol
ICMP
extension to the Internet Protocol (IP) for error, control, and informational messages

Note 1 to entry: ICMP is defined by RFC [1)] 92 and supports packet containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

3.13
Internet Group Management Protocol
IGMP
extension to the Internet Protocol (IP) for management of IP multicasting in the Internet

Note 1 to entry: IGMP is defined in RFC 1112 as the standard for IP multicasting in the Internet. It is used to establish host memberships in particular multicast groups on a single network. By using Host Membership Reports, the

1) Request for Comment: Internet Standards defined by the Internet Engineering Task Force (IETF) are firstly published as RFCs.

mechanisms of the protocol allow a host to inform its local router that it wants to receive messages addressed to a specific multicast group. All hosts conforming to level 2 of the IP multicasting specification require IGMP.

3.14
IP channel
logical connection between two IP host/port endpoints

Note 1 to entry: IP channels are either a guaranteed, reliable TCP (transmission control protocol) or an unreliable point-to-point or multicast (in case of routing) UDP (user datagram protocol) connection.

3.15
communication channel
as defined by the KNXnet/IP Core specification, this is represented by one or two IP channels

3.16
common External Message Interface
cEMI
generic structure for medium independent KNX messages

Note 1 to entry: cEMI (common EMI) frames are used to encapsulate KNX messages within Internet Protocol (IP) packets.

4 Symbols and abbreviations

For the purpose of this document, the symbols, abbreviations and acronyms used are listed below.

Tables listing implementation requirements use the following abbreviations.

Symbol	Description
M	Mandatory
C^n	Conditions are specified under note "n"
O	Optional
X	Not allowed
n/a	Not applicable
R	Required
MC	Message code
AddIL	length of additional information

4.1
DHCP
Dynamic Host Configuration Protocol
communication protocol for automatic assignment of IP address settings

4.2
DNS
Domain Name Service
assigns Internet names to IP addresses

4.3
EIB
European Installation Bus
Standard for Building Controls (EN 50090)

4.4
IP
Internet Protocol

4.5
KNX
Standard for Building Controls (EN 50090)

4.6
TCP/IP
Transmission Control Protocol over Internet Protocol
connection-oriented communication over the Internet

4.7
UDP/IP
User Datagram Protocol over Internet Protocol
connection-less communication over the Internet

5 Requirements

5.1 Clause 1: Overview

5.1.1 KNXnet/IP Document Clauses

5.1.1.1 General

This European Standard defines the integration of KNX protocol implementations within the Internet Protocol (IP) named KNXnet/IP or EIBnet/IP for continuity with ENV 13321-2:2000 (EIBnet) as defined by CEN/TC 247. EIBnet was introduced as an expansion of EIB into the information technology realm and was incorporated as a building controls technology in CEN/TC 247. EIBnet/IP is the logical successor to EIBnet. As EIB has become a part of KNX, this standard is called KNXnet/IP.

This European Standard defines a standard protocol, which is implemented within KNX devices, Engineering Tool Software and other implementations to support KNX data exchange over IP networks. In fact, KNXnet/IP provides a general framework, which accommodates several specialised “Service Protocols” in a modular and extendible fashion.

The KNXnet/IP standard consists of the following clauses:

— Clause 1, Overview;

— Clause 2, Core Specification;

— Clause 3, Device Management;

— Clause 4, Tunnelling;

— Clause 5, Routing.

Additional clauses may be added to the KNXnet/IP standard in the future at which time this Clause 1 “Overview” shall be updated.

KNXnet/IP supports different software implementations on top of the protocol. More specifically, these software implementations can be Building Management, Facility Management, Energy Management, or simply Data Base and SCADA (Supervision, Control and Data Acquisition) packages.

Most of these packages need to be configured for the specific user application. In order to simplify this process and cut costs for engineering, KNXnet/IP provides simple engineering interfaces, namely a

description “language” for the underlying KNX system. This may be done off-line, e.g. generated as an ETS export file, or on-line by a mechanism that self-describes the underlying KNX system (reading data from the system itself).

KNXnet/IP supports:

— on-the-fly change-over between operational modes (configuration, operation);

— event driven mechanisms;

— connections with a delay time greater than $t_{EIB\_transfer\_timeout}$ (e.g. network connection via satellite).

5.1.1.2 Clause 1, Overview

Clause 1 "Overview" is this document.

5.1.1.3 Clause 2, Core specification

Clause 2 “Core Specification” defines a standard protocol, which is implemented within KNXnet/IP devices and the Engineering Tool Software (ETS) to support KNX data exchange over IP networks.

This specific implementation of the protocol over the Internet Protocol (IP) is called KNXnet/IP.

This standard addresses:

— definition of data packets sent over the IP host protocol network for KNXnet/IP communication;

— discovery and self-description of KNXnet/IP servers;

— configuration and establishment of a communication channel between a KNXnet/IP client and a KNXnet/IP server;

5.1.1.4 Clause 3, Device Management

Clause 3 “Device Management” defines services for remote configuration and remote management of KNXnet/IP servers.

5.1.1.5 Clause 4, Tunnelling

Clause 4 “Tunnelling” defines services for point-to-point exchange of KNX telegrams over an IP network between a KNXnet/IP device acting as a server and a KNXnet/IP Client. This point-to-point exchange may be established by a super ordinate system for building automation or management functions or by an Engineering Tool Software. It supports all ETS functions for download, test, and analysis of KNX devices on KNX networks connected via KNXnet/IP servers. This includes changes of single KNX device object properties.

Tunnelling assumes that a data transmission round-trip between ETS or a KNXnet/IP Tunnelling client and KNXnet/IP servers takes less than $t_{KNX\_transfer\_timeouts}$.

5.1.1.6 Clause 5, Routing

Clause 5 “Routing” defines services, which route KNX telegrams between KNXnet/IP servers through the IP network.

5.1.2 Mandatory and optional implementation of IP protocols

5.1.2.1 General

KNXnet/IP uses existing IP protocols where possible unless their use implies an undue burden with regard to memory and implementation requirements for the intended service.

The following table shows mandatory (M) and optional (O) implementation of IP protocols by KNXnet/IP service types. Although this table refers to the KNXnet/IP server, it also indicates which IP protocols shall be implemented by the KNXnet/IP client. Any non-applicable IP protocol is marked as "na".

Table 1 — KNXnet/IP service types and IP protocols

IP protocol	Service Type			
	Core	Device Management	Tunnelling	Routing
ARP	M	M	M	M
RARP	O	O	O	O
Support of fixed IP address	M	M	M	M
BootP (Client)[a]	M	M	M	M
DHCP (Client)[a]	M	M	M	M
UDP	M	M	M	M
TCP	O	O	O	na
ICMP	M	M	M	M
IGMP	M	M	na	M

[a] BootP/DHCP: It is essential that either one be implemented by a KNXnet/IP device.

Other Internet protocols like NTP (network time protocol), FTP (file transfer protocol), HTTP (hypertext transfer protocol), SMTP (simple message transfer protocol), DNS (domain name system), and SNMP (simple network management protocol) may be used but are not within the scope of the KNXnet/IP protocol.

5.1.2.2 Minimum KNXnet/IP device requirements

KNXnet/IP service types as defined in this standard require the implementation of a minimal set of IP protocols for interworking.

KNXnet/IP servers shall implement these IP protocols: ARP, BootP, UDP, ICMP and IGMP. Other IP protocols may be required for specific services.

5.1.2.3 Network environment

Because KNXnet/IP servers use IP, this standard does not require any specific medium carrying the IP datagrams.