DIN EN ISO 22510

DIN

ICS 35.240.67; 91.040.01

Entwurf

Einsprüche bis 2018-07-18
Vorgesehen als Ersatz für
DIN EN 13321-2:2013-03

Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement – Elektrische Systemtechnik für Heim und Gebäude – KNXnet/IP-Kommunikation (ISO/DIS 22510:2018); Deutsche und Englische Fassung prEN ISO 22510:2018, nur auf CD-ROM

Open data communication in building automation, controls and building management – Home and building electronic systems – KNXnet/IP communication (ISO/DIS 22510:2018); German and English version prEN ISO 22510:2018, only on CD-ROM

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment – Systèmes électroniques pour les foyers domestiques et les bâtiments – Communication KNXnet/IP (ISO/DIS 22510:2018); Version allemande et anglaise prEN ISO 22510:2018, seulement en CD-ROM

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-05-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nhrs@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Heiz- und Raumlufttechnik sowie deren Sicherheit (NHRS), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 516 Seiten

DIN-Normenausschuss Heiz- und Raumlufttechnik sowie deren Sicherheit (NHRS)

© DIN Deutsches Institut für Normung e. V. · Jede Art der Vervielfältigung, auch auszugsweise, nur mit Genehmigung des DIN Deutsches Institut für Normung e. V., Berlin, gestattet.
Alleinverkauf der Normen durch Beuth Verlag GmbH, 10772 Berlin

Preisgruppe 42
www.din.de
www.beuth.de

Documents
Document Sharing Hub
2827800

Full document details: E DIN EN ISO 22510:2018-06

Nationales Vorwort

Dieses Dokument (prEN ISO 22510:2018) wurde vom Technischen Komitee ISO/TC 205 „Building environment design“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 247 „Gebäudeautomation und Gebäudemanagement“ erarbeitet, dessen Sekretariat von SNV (Schweiz) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 041-03-65 AA „Gebäudeautomation: Produkte, Systeme und Kommunikation (SpA CEN/TC 247 und ISO/TC 205/WG 3)“ im DIN-Normenausschuss DIN-Normenausschuss Heiz- und Raumlufttechnik sowie deren Sicherheit (NHRS)

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Änderungen

Gegenüber DIN EN 13321-2:2013-03 wurden folgende Änderungen vorgenommen:

a) neue Begriffe wurden hinzugefügt;

b) Abschnitt 5, Anforderungen, wurde überarbeitet;

c) Unterabschnitt 5.7 zu abgesicherter Kommunikation wurde hinzugefügt;

d) Anhänge A, C und D wurden überarbeitet.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

– Entwurf –

CEN/TC 247

Datum: 2018-04

prEN ISO 22510:2018

CEN/TC 247

Sekretariat: SNV

Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement — Elektrische Systemtechnik für Heim und Gebäude — KNXnet/IP-Kommunikation (ISO/DIS 22510:2018)

Réseau ouvert de communication de données pour l'automatisation, la régulation et la gestion technique du bâtiment — Systèmes électroniques pour les foyers domestiques et les bâtiments — Communication KNX/IP (ISO/DIS 22510:2018)

Open data communication in building automation, controls and building management — Home and building electronic systems — KNXnet/IP communication (ISO/DIS 22510:2018)

ICS:

Deskriptoren:

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokumentstufe: parallele Umfrage
Dokumentsprache: D

STD Version 2.9d

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Inhalt

Seite

Europäisches Vorwort **5**

Vorwort **6**

Einleitung **7**

1 Anwendungsbereich **10**

2 Normative Verweisungen **11**

3 Begriffe **11**

4 Symbole und Abkürzungen **14**

5 Anforderungen **16**
5.1 Abschnitt 1: Überblick **16**
5.1.1 Abschnitte des KNXnet/IP-Dokuments **16**
5.1.2 Obligatorische und optionale Implementierungen von IP-Protokollen **18**
5.2 Abschnitt 2: Core **21**
5.2.1 Anwendungsbereich **21**
5.2.2 KNXnet/IP-Frames **21**
5.2.3 Host-Protokoll-Unabhängigkeit **23**
5.2.4 Erkennung und Selbstbeschreibung **24**
5.2.5 Kommunikationskanäle **26**
5.2.6 Allgemeine Implementierungsrichtlinien **29**
5.2.7 Datenpaketstrukturen **33**
5.2.8 IP-Netzwerke **54**
5.2.9 Mindestanforderungen an unterstützte Dienste **64**
5.3 Abschnitt 3: Device Management **65**
5.3.1 Anwendungsbereich **65**
5.3.2 KNXnet/IP Device Management **65**
5.3.3 Implementierungsregeln und -richtlinien **78**
5.3.4 Datenpaketstrukturen **80**
5.3.5 Mindestprofile **83**
5.4 Abschnitt 4: Tunnelling **84**
5.4.1 Anwendungsbereich **84**
5.4.2 Tunnelling von KNX-Telegrammen **84**
5.4.3 Konfiguration und Management **88**
5.4.4 Frame-Strukturen **90**
5.4.5 Mindestprofile **98**
5.5 Abschnitt 5: Routing **99**
5.5.1 Anwendungsbereich **99**
5.5.2 KNXnet/IP-Routing von KNX-Telegrammen **99**
5.5.3 Implementierungsregeln und -richtlinien **110**
5.5.4 Konfiguration und Management **113**
5.5.5 Datenpaketstrukturen **113**
5.5.6 Mindestprofile **115**
5.6 Abschnitt 6: Ferndiagnose und Konfiguration **117**
5.6.1 Anwendungsbereich **117**
5.6.2 Ferndiagnose von KNXnet/IP-Geräten **117**
5.6.3 Konfiguration und Management **118**
5.6.4 Datenpaketstrukturen **118**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.6.5 Zertifizierung ... 123
5.7 Abschnitt 7: Gesicherte Kommunikation ... 124
5.7.1 Anwendungsbereich ... 124
5.7.2 Stapel und Kommunikation ... 125
5.7.3 Management-Prozeduren ... 171
5.7.4 Synchronisation von Timern ... 174

Anhang A (normativ) Liste der Codes ... 176
A.1 Einleitung ... 176
A.2 Übliche Konstanten ... 176
A.3 KNXnet/IP-Dienste ... 176
A.3.1 Nummernbereiche für Dienstarten ... 176
A.3.2 KNXnet/IP-Core-Dienste ... 177
A.3.3 Device-Management-Dienste ... 177
A.3.4 Tunnelling-Dienste ... 178
A.3.5 Routing-Dienste ... 178
A.3.6 Remote-Logging-Dienste ... 178
A.3.7 Ferndiagnose und Konfiguration ... 179
A.3.8 Object-Server-Dienste ... 179
A.4 Verbindungsarten ... 179
A.4.1 KNXnet/IP-Secure-Dienste ... 180
A.5 Fehlercodes ... 180
A.5.1 Übliche Fehlercodes ... 180
A.5.2 CONNECT_RESPONSE-Statuscodes ... 180
A.5.3 CONNECTIONSTATE_RESPONSE-Statuscodes ... 181
A.5.4 CONNECT_ACK-Fehlercodes für Tunnelling ... 181
A.5.5 DEVICE_CONFIGURATION_ACK-Statuscodes für Device Management ... 181
A.6 DIB (Description Information Block) ... 182
A.7 Host-Protokoll-Codes ... 183
A.8 Zeitüberschreitungskonstanten ... 184
A.9 IP-Konstanten ... 184

Anhang B (informativ) Beispiele von KNXnet/IP-IP-Frames im Binärformat ... 185
B.1 SEARCH_REQUEST ... 185
B.2 SEARCH_RESPONSE ... 186
B.3 DESCRIPTION_REQUEST ... 188
B.4 DESCRIPTION_RESPONSE ... 189
B.5 CONNECT_REQUEST ... 192
B.6 CONNECT_RESPONSE ... 193
B.7 CONNECTIONSTATE_REQUEST ... 194
B.8 CONNECTIONSTATE_RESPONSE ... 194
B.9 DISCONNECT_REQUEST ... 195
B.10 DISCONNECT_RESPONSE ... 195
B.11 DEVICE_CONFIGURATION_REQUEST ... 196
B.12 DEVICE_CONFIGURATION_ACK ... 196
B.13 TUNNELLING_REQUEST ... 197
B.14 TUNNELLING_ACK ... 197
B.15 ROUTING_INDICATION ... 198
B.16 ROUTING_LOST_MESSAGE ... 198
B.17 ROUTING_BUSY ... 199
B.18 REMOTE_DIAGNOSTIC_REQUEST ... 200
B.19 REMOTE_DIAGNOSTIC_RESPONSE ... 201
B.20 REMOTE_BASIC_CONFIGURATION_REQUEST ... 203
B.21 REMOTE_RESET_REQUEST ... 204

Anhang C (normativ) KNXnet/IP-Parameterobjekt ... 205

Anhang D (normativ) cEMI (Common External Messaging Interface) ... 209

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

D.1 cEMI 209
D.1.1 cEMI: Nachrichtenformat und Dienste 209
D.1.2 Common EMI: Lokales Gerätemanagement 240

Anhang E (normativ) Koppler-Ressourcen 245
E.1 Einleitung 245
E.2 Geräteobjekt 245
E.2.1 PID_SERVICE_CONTROL (PID = 8) 246
E.2.2 PID_DEVICE_CONTROL (PID = 14) 246
E.2.3 PID_ROUTING_COUNT (PID = 51) 246
E.2.4 PID_ERROR_FLAGS (PID = 53) 247
E.2.5 PID_PROGMODE (PID = 54) 247
E.3 Router-Objekt 247
E.3.1 Allgemeines 247
E.3.2 PID_LOAD_STATE_CONTROL (PID = 5) 248
E.3.3 PID_LINE_STATUS (PID = 51) 249
E.3.4 PID_MAIN_LCCONFIG (52)/PID_SUB_LCCONFIG (PID = 53) 249
E.3.5 PID_MAIN_LCGRPCONFIG (54)/PID_SUB_LCGRPCONFIG (PID = 55) 251
E.3.6 PID_ROUTETABLE_CONTROL (PID = 56) 251
E.3.7 PID_COUPL_SERV_CONTROL (PID = 57) 255

Literaturhinweise 257

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Europäisches Vorwort

Dieses Dokument (prEN ISO 22510:2018) wurde vom Technischen Komitee ISO/TC 205 „Building environment design“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 247 „Gebäudeautomation und Gebäudemanagement“ erarbeitet, dessen Sekretariat von SNV gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 22510:2018 wurde von CEN als prEN ISO 22510:2018 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Eine Erläuterung zum freiwilligen Charakter von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, enthält der folgende Link: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 205, *Building environment design* erarbeitet.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Einleitung

Diese Internationale Norm wurde für den Entwurf neuer Gebäude und die Sanierung vorhandener Gebäude entwickelt, um ein angenehmes Raumklima sowie Energieerhaltung und Energieeffizienz zu erzielen.

KNXnet/IP ist ein Protokoll, das für die Übertragung von KNX-Kontroll-Frames von elektrischer Systemtechnik für Heim und Gebäude (ESHG) über ein IP-Netzwerk vorgesehen ist. Es wird als Infrastruktur-Backbone für die Verbindung von KNX-Subnetzen, als Kommunikationsmedium für KNX-IP-Geräte und für die Bereitstellung von IP-basierten Diensten für Clients (z. B. Verbinden einer Tool-Software mit einer KNX-Installation) verwendet. Die Vorteile der Verwendung von IP für diese Zwecke liegen in der kostengünstigen Infrastruktur von IP-Netzwerken, ihrer Verfügbarkeit an fast allen Standorten und der nahezu unbegrenzten Überbrückung von Distanzen zwischen zwei Kommunikationspartnern.

KNXnet/IP unterscheidet zwischen Unicast- und Multicast-Diensten. Mit KNXnet/IP-Unicast-Diensten kann ein einzelner Client mit einem einzelnen KNXnet/IP-Server verbunden werden (z. B. KNXnet/IP Tunnelling). KNXnet/IP-Multicast-Dienste werden hauptsächlich dazu benutzt, verschiedene KNX-Subnetze, die IP-Kommunikation verwenden, auf dem KNX-Backbone zu verbinden. Zu diesem Zweck werden KNXnet/IP-Routing-Dienste definiert. KNXnet/IP-Multicast-Dienste setzen auf IP-Multicast auf.

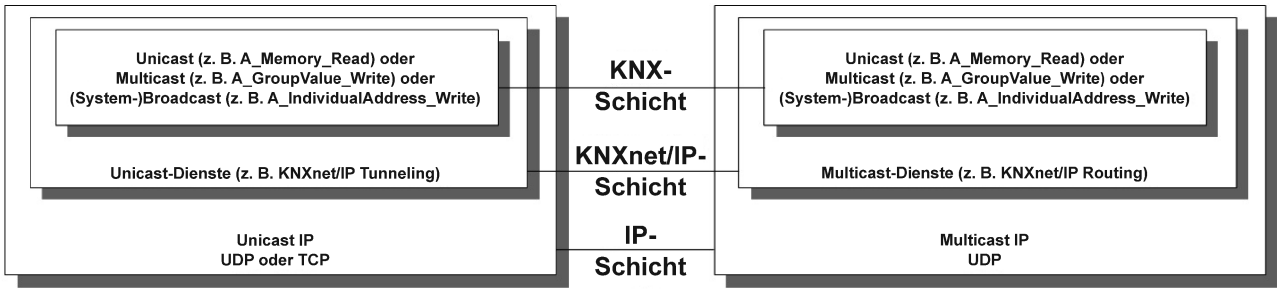


Bild 1 — Unicast und Multicast im Zusammenhang mit KNX, KNXnet/IP und IP

Diese Norm legt die Einbindung von KNX-Protokoll-Implementierungen innerhalb von Internet Protocol (IP) namens KNXnet/IP fest. Sie legt ein Standardprotokoll fest, das innerhalb von KNX-Geräten, der ETS (Engineering Tool Software) und anderen Implementierungen eingesetzt wird, um den KNX-Datenaustausch über IP-Netzwerke zu unterstützen. KNXnet/IP stellt im Grunde genommen ein allgemeines System bereit, das mehrere spezialisierte „Dienstprotokolle“ in einer modularen und erweiterbaren Form einschließt.

Die KNXnet/IP-Spezifikation umfasst die folgenden Abschnitte, welche in Abschnitt 5 „Anforderungen“ ausführlicher beschrieben werden:

— Abschnitt 1, Überblick;

— Abschnitt 2, Core;

— Abschnitt 3, Device Management;

— Abschnitt 4, Tunnelling;

— Abschnitt 5, Routing;

— Abschnitt 6, Ferndiagnose und Konfiguration;

— Abschnitt 7, Gesicherte Kommunikation.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

In der Zukunft werden der KNXnet/IP-Spezifikation möglicherweise zusätzliche Abschnitte hinzugefügt; dann müssen auch der Abschnitt 1 „Überblick“ sowie Anhang A aktualisiert werden.

KNXnet/IP unterstützt unterschiedliche Software-Implementierungen, die auf dem Protokoll aufsetzen. Im Einzelnen können diese Software-Implementierungen Gebäudemanagement-, Facility-Management-, Energiemanagement- oder einfach Datenbank- und SCADA-Pakete (Supervisory Control and Data Acquisition) sein.

Die meisten dieser Pakete müssen für die spezifische Benutzeranwendung konfiguriert werden. Um diesen Prozess zu vereinfachen und Engineering-Kosten zu senken, stellt KNXnet/IP einfache Engineering-Schnittstellen, nämlich eine „Beschreibungssprache“ für das zugrunde liegende KNX-System, bereit. Die Konfiguration kann offline durchgeführt werden, z. B. indem eine ETS-Exportdatei generiert wird, oder online mithilfe eines Mechanismus, der das zugrunde liegende KNX-System selbst beschreibt (d. h. Daten aus dem System selbst liest).

Im Zusammenhang mit der Abbildung von EIB/KNX auf BACnet, die in EN ISO 16484-5 beschrieben wird, können EIB/KNX-Installationen auf einfache Weise in BACnet-Systemumgebungen integriert werden.

KNXnet/IP unterstützt

— die schnelle Umschaltung zwischen Betriebsmodi (Konfiguration, Betrieb),

— ereignisgesteuerte Mechanismen,

— Verbindungen mit einer Verzögerungszeit größer als $t_{\text{KNX\_Übertragung\_Zeitüberschreitung}}$ (z. B. eine Netzwerkverbindung über Satellit).

Abschnitt 1, Überblick

Abschnitt 1 „Überblick“ gibt einen allgemeinen Überblick über KNXnet/IP.

Abschnitt 2, Core

Abschnitt 2 „Core“ legt ein Standardprotokoll fest, das innerhalb von KNXnet/IP-Geräten und der Engineering Tool Software implementiert wird, um den KNX-Datenaustausch über IP-Netzwerke zu unterstützen.

Diese spezifische Implementierung des Protokolls über Internet Protocol (IP) wird „KNXnet/IP“ genannt.

Diese Spezifikation befasst sich mit

— der Festlegung von Datenpaketen, die über das IP-Host-Protokoll-Netzwerk für KNXnet/IP-Kommunikation gesendet werden,

— der Erkennung und Selbstbeschreibung von KNXnet/IP-Servern,

— der Konfiguration und des Aufbaus eines Kommunikationskanals zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server.

Abschnitt 3, Device Management

Abschnitt 3 „Device Management“ legt Dienste für die Fernkonfiguration und die Fernverwaltung von KNXnet/IP-Servern fest.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Abschnitt 4, Tunnelling

Abschnitt 4 „Tunnelling“ legt Dienste für einen Punkt-zu-Punkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen einem KNXnet/IP-Gerät, das als Server agiert, und einem KNXnet/IP-Client fest. Dieser Punkt-zu-Punkt-Austausch kann mithilfe eines übergeordneten Systems für Funktionen der Gebäudeautomation oder des Gebäudemanagements oder mithilfe einer Engineering Tool Software eingerichtet werden. Er unterstützt alle ETS-Funktionen für den Download, die Prüfung und die Analyse von KNX-Geräten in KNX-Netzwerken, die über KNXnet/IP-Server verbunden sind. Dies schließt Änderungen einzelner Objekteigenschaften der KNX-Geräte ein.

Tunnelling setzt voraus, dass ein Datenübertragungsrundlauf zwischen einem KNXnet/IP-Tunnelling-Client und KNXnet/IP-Servern weniger als $t_{\text{KNX\_Übertragung\_Zeitüberschreitungen}}$ benötigt.

Abschnitt 5, Routing

Abschnitt 5 „Routing“ legt Dienste für einen Punkt-zu-Multipunkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen KNXnet/IP-Routern und/oder KNX IP-Geräten fest.

Abschnitt 6, Ferndiagnose und Konfiguration

Abschnitt 6 „Ferndiagnose und Konfiguration“ legt Dienste für einen Punkt-zu-Punkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen KNXnet/IP-Routern und/oder KNX IP-Geräten fest. Die Dienste stellen ein Mittel zur Ermittlung von Kommunikationseinstellungen und ihrer Änderung bei Fernbetrieb bereit.

Abschnitt 7, Gesicherte Kommunikation

Abschnitt 7 „Gesicherte Kommunikation“ der KNXnet/IP-Spezifikation legt den Sicherheits-Wrapper zum Schutz des KNXnet/IP-Unicast- und -Multicast-Verkehrs fest, indem eine für alle vorhandenen KNXnet/IP-Dienste sichtbare zusätzliche Sicherungsschicht um den kompletten KNXnet/IP-Verkehr gelegt wird.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

1 Anwendungsbereich

Diese Internationale Norm legt die Einbindung von KNX-Protokoll-Implementierungen, die auf IP-Netzwerken (Internet-Protocol) aufsetzen, namens KNXnet/IP, fest. Sie beschreibt ein Standardprotokoll für KNX-Geräte, die mit einem IP-Netzwerk verbunden sind, sogenannte KNXnet/IP-Geräte. Das IP-Netzwerk agiert in KNX-Installationen als schneller Backbone (im Vergleich zur KNX-Twisted-Pair-Übertragungsgeschwindigkeit).

Der weit verbreitete Einsatz von Datennetzwerken über Internet Protocol (IP) stellt eine Möglichkeit zur Erweiterung der Kommunikation im Bereich Gebäudesteuerung über den lokalen KNX-Steuerbus hinaus dar, wodurch Folgendes möglich wird:

— Fernkonfiguration;

— Fernbetrieb (einschließlich Steuerung und Meldung);

— schnelle Schnittstelle von LAN auf KNX und umgekehrt;

— WAN-Verbindungen zwischen KNX-Systemen (bei denen ein installiertes KNX-System mindestens eine Linie darstellt);

— Schnittstelle zu übergeordneten Gebäudemanagement- und Energiemanagementsystemen.

Ein KNXnet/IP-System besteht mindestens aus den folgenden Elementen:

— einer EIB-Linie mit bis zu 64 (255) EIB-Geräten,
ODER
einem KNX-Segment (KNX-TP1, KNX-RF, KNX-PL110),

— einem Netzwerkverbindungsgerät von KNX zu IP (einem sogenannten KNXnet/IP-Server),

und üblicherweise aus zusätzlicher

— Software für entfernte Funktionen, z. B. auf einer Workstation (dies kann eine Datenbankanwendung, ein BACnet-Gebäudemanagementsystem, ein Browser usw. sein).

Bild 1 zeigt ein typisches Szenario, in dem ein KNXnet/IP-Client (z. B. eine installierte ETS) auf mehrere installierte KNX-Systeme oder KNX-Subnetze über ein IP-Netzwerk zugreift. Der KNXnet/IP-Client kann auf mehrere KNXnet/IP-Server gleichzeitig zugreifen. Durch Subnetz-Routing ist eine Kommunikation zwischen Servern möglich.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

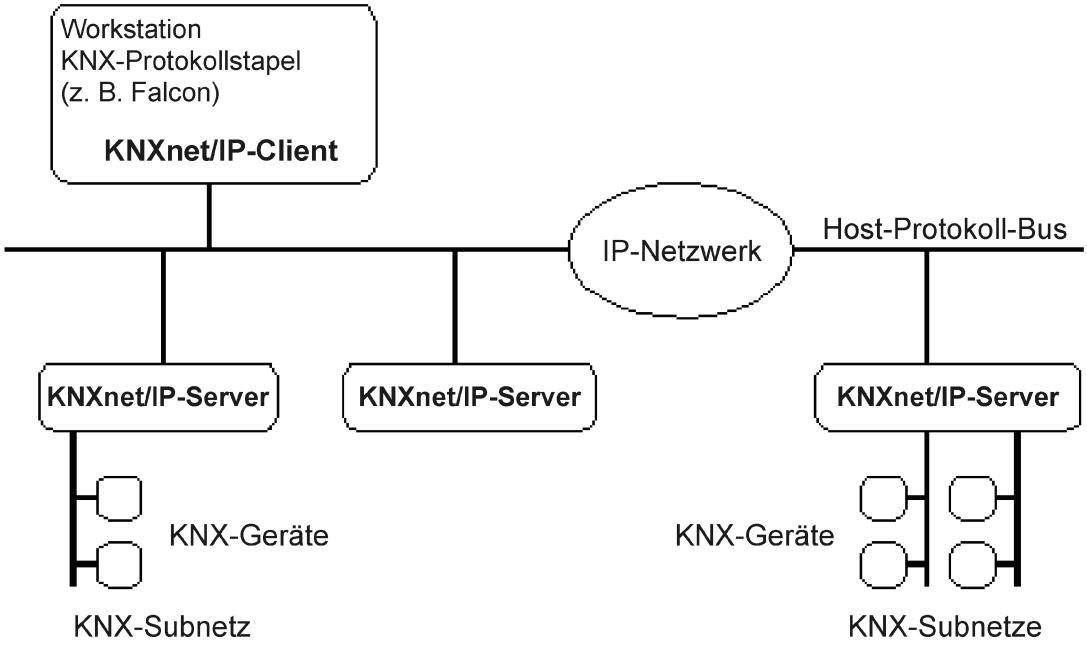


Bild 2 — Gerätetypen und Konfigurationsbeispiele

2 Normative Verweisungen

Nicht anwendbar.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1
Backbone-Schlüssel
Schlüssel, der für die Verschlüsselung und Nachrichtenauthentifizierung sicherer KNXnet/IP-Multicast-Kommunikation innerhalb einer KNXnet/IP-Routing-Multicast-Gruppe verwendet wird. Dieser Schlüssel wird von der ETS konfiguriert und stellt ein gemeinsames Geheimnis aller Mitglieder der sicheren KNXnet/IP-Routing-Multicast-Gruppe dar

3.2
Chiffretext
allgemeine Bezeichnung für verschlüsselte Daten

Anmerkung 1 zum Begriff: Das Gegenteil von Chiffretext ist Klartext.

3.3
common External Message Interface
cEMI
generische Struktur für medienunabhängige KNX-Nachrichten

Anmerkung 1 zum Begriff: cEMI-Frames (übliche EMI-Frames) werden verwendet, um KNX-Nachrichten innerhalb von IP-Paketen einzukapseln.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

3.4
Kommunikationskanal
logische Verbindung zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server (oder, im Fall eines Routings, zwischen zwei oder mehreren KNXnet/IP-Servern)

Anmerkung 1 zum Begriff: Ein Kommunikationskanal besteht aus einer oder mehreren Verbindungen basierend auf der Definition im Host-Protokoll, die für KNXnet/IP verwendet wird.

3.5
Kommunikationskanal
wie in der KNXnet/IP-Core-Spezifikation festgelegt, wird dieser Kanal durch einen oder zwei IP-Kanäle repräsentiert

3.6
Engineering Tool Software
ETS
Software, die für die Konfiguration von KNX-Geräten verwendet wird

3.7
Host Protocol Address Information
HPAI
Struktur, die die Adressinformationen des IP-Host-Protokolls enthält, die für die Adressierung eines KNXnet/IP-Endpunkts auf einem anderen KNXnet/IP-Gerät verwendet werden

3.8
IP-Kanal
logische Verbindung zwischen zwei IP-Host/Port-Endpunkten

Anmerkung 1 zum Begriff: IP-Kanäle sind entweder garantierte, vertrauenswürdige TCP-Verbindungen (Transmission Control Protocol) oder nicht vertrauenswürdige Punkt-zu-Punkt- oder (im Fall von Routing) Multicast-UDP-Verbindungen (User Datagram Protocol).

3.9
KNX-Knoten
Gerät, das einen KNX-Protokollstapel implementiert und die Anforderungen nach dem KNX-Standard erfüllt

3.10
Internet Control Message Protocol
ICMP
Erweiterung von Internet Protocol (IP) um Fehler-, Steuer- und Informationsmeldungen

Anmerkung 1 zum Begriff: ICMP ist in RFC[1)] 92 definiert und unterstützt Pakete, die Fehler-, Steuer- und Informationsmeldungen enthalten. Der Ping-Befehl verwendet ICMP beispielsweise, um eine Internetverbindung zu testen.

3.11
Internet Group Management Protocol
IGMP
Erweiterung von Internet Protocol (IP) um die Verwaltung von IP-Multicasting im Internet

Anmerkung 1 zum Begriff: IGMP ist in RFC 1112 als Standard für das IP-Multicasting im Internet festgelegt. Es wird für die Einrichtung von Host-Mitgliedschaften in bestimmten Multicast-Gruppen in einem einzelnen Netzwerk ver-

1) RFC (Request for Comment): Internetstandards, die durch die Internet Engineering Task Force (IETF) festgelegt werden, werden zunächst als RFCs veröffentlicht.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

wendet. Unter Verwendung von Host-Mitgliedschaftsberichten erlaubt es der Mechanismus des Protokolls einem Host, seinen lokalen Router darüber zu informieren, dass er Nachrichten, die an eine bestimmte Multicast-Gruppe adressiert sind, empfangen möchte. Alle Hosts, die der Stufe 2 der IP-Multicast-Spezifikation entsprechen, benötigen IGMP.

3.12
IP-Domain
alle KNXnet/IP-Geräte in demselben Netzwerk mit derselben Multicast-Adresse und derselben Backbone-Verschlüsselung (entweder keine Verschlüsselung oder Verschlüsselung mit demselben Schlüssel) bilden eine IP-Domain

3.13
KNXnet/IP-Client
Anwendung, die das KNXnet/IP-Client-Protokoll verwendet, um Zugriff auf ein KNX-Subnetz über einen IP-Netzwerkkanal zu erhalten

3.14
KNXnet/IP-Gerät
Implementierung von KNXnet/IP-Diensten auf einem KNX-Knoten (KNXnet/IP-Server) oder anderer Hardware (KNXnet/IP-Client)

3.15
KNXnet/IP-Router
spezieller Typ eines KNXnet/IP-Gerätes, das KNX-Protokollpakete zwischen KNX-Subnetzen hin- und herleitet

3.16
KNXnet/IP-Server
KNX-Gerät mit physikalischem Zugriff auf ein KNX-Netzwerk, das das KNXnet/IP-Server-Protokoll implementiert, um mit KNXnet/IP-Clients oder (im Fall eines Routings) mit anderen KNXnet/IP-Servern über einen IP-Netzwerkkanal zu kommunizieren

Anmerkung 1 zum Begriff: Ein KNXnet/IP-Server ist seiner Konstruktion nach immer auch ein KNX-Knoten.

3.17
KNXnet/IP Tunnelling
Dienste für einen Punkt-zu-Punkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen einem KNXnet/IP-Gerät, das als Server agiert, und einem KNXnet/IP-Client

3.18
Klartext
allgemeine Bezeichnung für unverschlüsselte Daten. Der Inhalt des Klartexts hängt von dem Dienst und dem Benutzer ab und unterliegt nicht der Vertraulichkeit und Authentifizierung. Klartext ist das Gegenteil von Chiffretext

3.19
sichere Sitzung
authentifizierter, autorisierter und verschlüsselter Kommunikationskanal zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server für Unicast-Kommunikation

3.20
Sitzungsschlüssel
Schlüssel, der für die Verschlüsselung und Nachrichtenauthentifizierung in einer sicheren Sitzung zwischen zwei KNXnet/IP-Kommunikationspartnern verwendet wird. Dieser Schlüssel wird im Rahmen der Aufbauprozedur der sicheren Sitzung mithilfe von ECDH erstellt (Perfect Forward Secrecy vorausgesetzt) und ist nur für diese einzelne Sitzung gültig

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

3.21
Subnetz
Teil eines Netzwerkes, der eine gemeinsame Adresskomponente verwendet, die sogenannte „Subnetz-adresse“

Anmerkung 1 zum Begriff: Die verschiedenen Netzwerkprotokolle geben die Subnetzadresse auf unterschiedliche Weise an.

3.22
Time To Live (de: Lebenszeit)
TTL
maximale Anzahl von IP-Routern, durch die ein Multicast-UDP/IP-Datagramm geleitet werden kann

Anmerkung 1 zum Begriff: Jeder IP-Router, durch den das Datagramm geleitet wird, verringert die TTL um eins; der lokale Hostadapter führt dies gleichermaßen durch. Wenn die TTL null erreicht, verwirft der Router das Datagramm. Wenn ein Datagramm von einem lokalen Hostadapter mit einer TTL von null gesendet wird, bedeutet dies, dass das Datagramm den Host nie verlässt. Eine TTL von eins bedeutet, dass das Datagramm das lokale Netzwerk nie verlässt (es wird nicht weitergeleitet).

4 Symbole und Abkürzungen

Für die Anwendung dieses Dokuments sind die Symbole, Abkürzungen und Akronyme unten aufgeführt.

Tabellen, die Implementierungsanforderungen auflisten, verwenden folgende Abkürzungen.

Symbol	Beschreibung
M	Obligatorisch
C^n	Bedingungen sind in der Anmerkung „n“ angegeben.
O	Optional
X	Nicht zulässig
n/a	Nicht anwendbar
R	Erforderlich
MC	Nachrichtencode
AddIL	Länge der zusätzlichen Informationen

4.1
AES
Advanced Encryption Standard

4.2
CBC
Cipher Block Chaining

4.3
CCM
Counter-Betrieb mit CBC-MAC

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

4.4
CTR
Counter-Betrieb(smodus)

4.5
DDoS
verteilter Überlastangriff
(en: Distributed Denial of Service)

4.6
DHCP
Dynamic Host Configuration Protocol
Kommunikationsprotokoll für die automatische Zuordnung von IP-Adresseinstellungen

4.7
DNS
Domain Name Service
weist IP-Adressen Internetnamen zu

4.8
DoS
Überlastangriff
(en: Denial of Service)

4.9
ECDH
Elliptic Curve Diffie–Hellman

4.10
EIB
Europäischer Installationsbus
Standard für die Gebäudesteuerung (EN 50090)

4.11
FDSK
Factory Default Setup Key

4.12
IA
individuelle Adresse
eindeutige KNX-Adresse eines KNX-Gerätes in einem KNX-System

4.13
IP
Internet Protocol

4.14
IV
Initialisierungsvektor

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

4.15
KNX
Standard für die Gebäudesteuerung (EN 50090, ISO/IEC 14543-3-1 bis 14543-3-7)

4.16
MAC
Nachrichtenauthentifizierungscode
(en: Message Authentication Code)

4.17
MiM
Man-in-the-Middle

4.18
PBKDF2
Password-Based Key Derivation Function 2

4.19
SHA
sicherer Hash-Algorithmus

4.20
TCP/IP
Transmission Control Protocol over Internet Protocol
verbindungsorientierte Kommunikation über das Internet

4.21
UDP/IP
User Datagram Protocol over Internet Protocol
verbindungslose Kommunikation über das Internet

5 Anforderungen

5.1 Abschnitt 1: Überblick

5.1.1 Abschnitte des KNXnet/IP-Dokuments

5.1.1.1 Allgemeines

Diese Internationale Norm legt die Einbindung von KNX-Protokoll-Implementierungen innerhalb von Internet Protocol (IP) namens KNXnet/IP fest.

Diese Internationale Norm legt ein Standardprotokoll fest, das innerhalb von KNX-Geräten, der Engineering Tool Software und anderen Implementierungen eingesetzt wird, um den KNX-Datenaustausch über IP-Netzwerke zu unterstützen. KNXnet/IP stellt im Grunde genommen ein allgemeines System bereit, das mehrere spezialisierte „Dienstprotokolle“ in einer modularen und erweiterbaren Form einschließt.

Die KNXnet/IP-Spezifikation umfasst die folgenden Abschnitte:

— Abschnitt 1, Überblick;

— Abschnitt 2, Core;

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

— Abschnitt 3, Device Management;

— Abschnitt 4, Tunnelling;

— Abschnitt 5, Routing;

— Abschnitt 6, Ferndiagnose und Konfiguration;

— Abschnitt 7, Gesicherte Kommunikation.

In der Zukunft werden der KNXnet/IP-Spezifikation möglicherweise zusätzliche Abschnitte hinzugefügt; dann muss auch der Abschnitt 1 „Überblick“ aktualisiert werden.

KNXnet/IP unterstützt unterschiedliche Software-Implementierungen, die auf dem Protokoll aufsetzen. Im Einzelnen können diese Software-Implementierungen Gebäudemanagement-, Facility-Management-, Energiemanagement- oder einfach Datenbank- und SCADA-Pakete (Supervisory Control and Data Acquisition) sein.

Die meisten dieser Pakete müssen für die spezifische Benutzeranwendung konfiguriert werden. Um diesen Prozess zu vereinfachen und Engineering-Kosten zu senken, stellt KNXnet/IP einfache Engineering-Schnittstellen, nämlich eine „Beschreibungssprache“ für das zugrunde liegende KNX-System, bereit. Die Konfiguration kann offline durchgeführt werden, z. B. indem eine ETS-Exportdatei generiert wird, oder online mithilfe eines Mechanismus, der das zugrunde liegende KNX-System selbst beschreibt (d. h. Daten aus dem System selbst liest).

KNXnet/IP unterstützt

— die schnelle Umschaltung zwischen Betriebsmodi (Konfiguration, Betrieb),

— ereignisgesteuerte Mechanismen,

— Verbindungen mit einer Verzögerungszeit größer als $t_{\text{KNX\_Übertragung\_Zeitüberschreitung}}$ (z. B. eine Netzwerkverbindung über Satellit).

5.1.1.2 Abschnitt 1, Überblick

Abschnitt 1 „Überblick“ beschreibt die Inhalte der einzelnen Abschnitte dieser Norm.

5.1.1.3 Abschnitt 2, Core

Abschnitt 2 „Core“ legt ein Standardprotokoll fest, das innerhalb von KNXnet/IP-Geräten und der Engineering Tool Software (ETS) implementiert wird, um den KNX-Datenaustausch über IP-Netzwerke zu unterstützen.

Diese spezifische Implementierung des Protokolls über Internet Protocol (IP) wird „KNXnet/IP“ genannt.

Diese Spezifikation dient

— der Festlegung von Datenpaketen, die über das IP-Host-Protokoll-Netzwerk für KNXnet/IP-Kommunikation gesendet werden;

— der Erkennung und Selbstbeschreibung von KNXnet/IP-Servern;

— der Konfiguration und des Aufbaus eines Kommunikationskanals zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.1.1.4 Abschnitt 3, Device Management

Abschnitt 3 „Device Management“ legt Dienste für die Fernkonfiguration und die Fernverwaltung von KNXnet/IP-Servern fest.

5.1.1.5 Abschnitt 4, Tunnelling

Abschnitt 4 „Tunnelling“ legt Dienste für einen Punkt-zu-Punkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen einem KNXnet/IP-Gerät, das als Server agiert, und einem KNXnet/IP-Client fest. Dieser Punkt-zu-Punkt-Austausch kann mithilfe eines übergeordneten Systems für Funktionen der Gebäudeautomation oder des Gebäudemanagements oder mithilfe einer Engineering Tool Software eingerichtet werden. Er unterstützt alle ETS-Funktionen für den Download, die Prüfung und die Analyse von KNX-Geräten in KNX-Netzwerken, die über KNXnet/IP-Server verbunden sind. Dies schließt Änderungen einzelner Objekteigenschaften der KNX-Geräte ein.

Tunnelling setzt voraus, dass ein Datenübertragungsrundlauf zwischen der ETS oder einem KNXnet/IP-Tunnelling-Client und KNXnet/IP-Servern weniger als $t_{KNX\_Übertragung\_Zeitüberschreitungen}$ benötigt.

5.1.1.6 Abschnitt 5, Routing

Abschnitt 5 „Routing“ legt Dienste fest, die KNX-Telegramme zwischen KNXnet/IP-Servern über das IP-Netzwerk hin- und herleiten.

5.1.1.7 Abschnitt 6, Ferndiagnose und Konfiguration

Abschnitt 6 „Ferndiagnose und Konfiguration“ legt Dienste für einen Punkt-zu-Punkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen KNXnet/IP-Routern und/oder KNX IP-Geräten fest. Die Dienste stellen ein Mittel zur Ermittlung von Kommunikationseinstellungen und ihrer Änderung bei Fernbetrieb bereit.

5.1.1.8 Abschnitt 7, Gesicherte Kommunikation

Abschnitt 7 „Gesicherte Kommunikation“ legt Dienste für einen gesicherten Punkt-zu-Punkt-Austausch von KNX-Telegrammen über ein IP-Netzwerk zwischen einem KNXnet/IP-Client und einem KNX IP-Server fest. Die Dienste stellen ein Mittel zum Aufbau gesicherter Kommunikationssitzungen durch autorisierte KNXnet/IP-Clients bereit.

5.1.2 Obligatorische und optionale Implementierungen von IP-Protokollen

5.1.2.1 Allgemeines

KNXnet/IP verwendet, wo möglich, vorhandene IP-Protokolle, sofern ihre Verwendung nicht eine unzulässige Belastung im Hinblick auf den Speicherplatz und die Implementierungsanforderungen für den vorgesehenen Dienst einschließt.

Die folgende Tabelle zeigt obligatorische (M) und optionale (O) Implementierungen von IP-Protokollen nach KNXnet/IP-Dienstarten. Obwohl sich diese Tabelle auf den KNXnet/IP-Server bezieht, ist ebenfalls angegeben, welche IP-Protokolle vom KNXnet/IP-Client implementiert werden müssen. Nicht anwendbare IP-Protokolle sind mit „n/a“ markiert.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Tabelle 1 — KNXnet/IP-Dienstarten und IP-Protokolle

IP-Protokoll	Dienstart					
	Core	Device Management	Tunnelling	Routing	Ferndiagnose und Konfiguration	Gesicherte Kommunikation
ARP	M	M	M	M	M	M
RARP	O	O	O	O	O	O
Unterstützung einer festen IP-Adresse	M	M	M	M	M	M
BootP (Client)[a]	M	M	M	M	M	M
DHCP (Client)[a]	M	M	M	M	M	M
UDP	M	M	M	M	M	M
TCP	O	O	O[b]	n/a	n/a	M
ICMP	M	M	M	M	M	M
IGMP	M	M	n/a	M	O	M

[a] BootP/DHCP: Es muss einer der beiden Dienste auf einem KNXnet/IP-Gerät implementiert sein.

[b] TCP ist für Tunnelling v2 obligatorisch, das wiederum für die gesicherte Kommunikation erforderlich ist.

Andere Internetprotokolle wie NTP (Network Time Protocol), FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), SMTP (Simple Message Transfer Protocol), DNS (Domain Name System) und SNMP (Simple Network Management Protocol) können verwendet werden, liegen aber nicht im Anwendungsbereich des KNXnet/IP-Protokolls.

5.1.2.2 Mindestanforderungen an KNXnet/IP-Geräte

KNXnet/IP-Dienstarten, wie in dieser Norm festgelegt, erfordern die Implementierung einer Mindestanzahl von IP-Protokollen für die Interaktion.

KNXnet/IP-Server müssen die folgenden IP-Protokolle implementieren: ARP, BootP, UDP, ICMP und IGMP. Für spezifische Dienste können weitere IP-Protokolle erforderlich sein.

Ein KNXnet/IP-Client darf nicht voraussetzen, dass ein KNXnet/IP-Server KNXnet/IP-Frames mit einer Gesamtlänge von mehr als 508 unterstützt.

5.1.2.3 Netzwerkumgebung

Da KNXnet/IP-Server IP verwenden, ist nach dieser Norm kein spezifisches Medium, das die IP-Datagramme überträgt, erforderlich.

Es wird empfohlen, ein Medium zu verwenden, das mindestens die zweifache Bitrate aller KNXnet/IP-Router, die mit diesem Medium verbunden sind, überträgt. Bei einer Punkt-zu-Punkt-Verbindung, z. B. einer PPP-Verbindung, müsste diese mindestens 19 200 bit/s betragen; bei einem Netzwerk mit bis zu 400 KNXnet/IP-Servern müsste diese mindestens 8 Mbit/s betragen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Für KNXnet/IP-Server, die Ethernet als physikalisches Medium verwenden, wird 10BaseT als Minimum empfohlen.

5.1.2.4 Adressierung

KNXnet/IP-Server sind üblicherweise mit einem KNX-Subnetz und mit einem IP-Netzwerk verbunden. Aus diesem Grund verfügen KNXnet/IP-Server für jedes Netzwerk, mit dem sie verbunden sind, über eine eindeutige Adresse: eine individuelle KNX-Adresse und eine IP-Adresse.

Zusätzlich werden KNXnet/IP-Server einer KNXnet/IP-Projektinstallation zugewiesen, wobei für alle KNXnet/IP-Server in einer KNXnet/IP-Installation dieselbe IP-Multicast-Adresse verwendet wird.

5.1.2.5 KNXnet/IP-Geräteklassen

Ein KNXnet/IP-Gerät kann eine Softwareinstallation sein, die auf einem PC ausgeführt wird. Eine ETS oder eine andere Software, die KNXnet/IP-Dienste implementiert, wird daher als KNXnet/IP-Gerät betrachtet.

Die Festlegung von KNXnet/IP-Geräteklassen stellt die Interoperabilität zwischen KNXnet/IP-Geräten sowie eine Mindestmenge an unterstützten KNXnet/IP-Diensten für eine bestimmte KNXnet/IP-Geräteklasse sicher.

Tabelle 2 listet obligatorische und optionale Dienstarten für Geräteklassen auf.

Die Geräteklasse A umfasst Tools für die Konfiguration und Systemwartung. Mit der Ausnahme von Object-Server-Diensten müssen alle anderen KNXnet/IP-Dienste implementiert werden. ETS gehört zu dieser Geräteklasse.

Die Geräteklasse B legt eine Mindestmenge von KNXnet/IP-Diensten für KNXnet/IP-Router fest.

Die Geräteklasse C legt eine Mindestmenge von KNXnet/IP-Diensten für alle anderen KNXnet/IP-Geräte fest. Zu dieser KNXnet/IP-Geräteklasse gehören Gebäudemanagement-, Energiemanagement- und Facility-Management-Systeme.

Tabelle 2 — KNXnet/IP-Geräteklassen

Geräteklasse	Dienstart					
	Core	Device Management	Tunnelling	Routing	Ferndiagnose und Konfiguration	Gesicherte Kommunikation
A (Tools für die Konfiguration und Systemwartung)	M	M	M	M	M	M
B (KNXnet/IP-Router)	M	M	M	M	O[a]	O[a]
C (alle anderen KNXnet/IP-Geräte)	M	M	O	O	O	O

[a] Wird die gesicherte Kommunikation unterstützt, ist eine Unterstützung der Ferndiagnose und -konfiguration nicht zulässig.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.2 Abschnitt 2: Core

5.2.1 Anwendungsbereich

Dieser Abschnitt „Core“ der KNXnet/IP-Spezifikation stellt ein allgemeines, vom Host-Protokoll unabhängiges System bereit, das mehrere spezialisierte „Dienstprotokolle“ in einer modularen und erweiterbaren Form einschließt.

Diese Spezifikation dient

— der Festlegung von Datenpaketen, die für die KNXnet/IP-Kommunikation über das „Host-Protokoll“-Netzwerk (nicht KNX) gesendet werden,

— der Erkennung und Selbstbeschreibung von KNXnet/IP-Servern, und

— der Konfiguration, des Aufbaus und der Wartung eines Kommunikationskanals zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server.

5.2.2 KNXnet/IP-Frames

5.2.2.1 Allgemeine Festlegungen

5.2.2.1.1 Datenformat

Die in dieser Norm beschriebenen KNXnet/IP-Frames sind binär codiert.

Datenstruktur-Spezifikationen sind immer im Binärformat angegeben.

5.2.2.1.2 Byte-Reihenfolge

Bei binären Strukturen muss die Byte-Reihenfolge dem Big-Endian-Modus (Motorola, keine Vertauschung) entsprechen, wenn nichts anderes angegeben ist. Bei Klartextformaten müssen die Byte-Reihenfolge und die Formatierung den Angaben in den zugehörigen Protokoll-Spezifikationen entsprechen.

5.2.2.1.3 Strukturen

Alle KNXnet/IP-Strukturen folgen einer gemeinsamen Regel: das erste Oktett entspricht immer der Länge der gesamten Struktur (einige Strukturen können über Felder mit variabler Länge, z. B. für Zeichenketten, verfügen) und das zweite Oktett stellt immer eine Kennung dar, die den Typ der Struktur angibt. Ab dem dritten Oktett folgen die Strukturdaten. Übersteigt die Menge der Daten 252 Oktette, muss das Längen-Oktett den Wert FFh erhalten und die nächsten beiden Oktette entsprechen der Länge eines 16-Bit-Werts. Die Strukturdaten beginnen dann im fünften Oktett.

5.2.2.2 Frame-Format

Die Kommunikation zwischen KNXnet/IP-Geräten beruht auf KNXnet/IP-Frames. Ein KNXnet/IP-Frame ist ein Datenpaket, das über das Netzwerkprotokoll (nicht KNX) gesendet wird und aus einer Kopfzeile (vergleichbar mit dem IP-Header eines IP-Datenpakets) und einem optionalen Textkörper (Body) von variabler Länge besteht.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

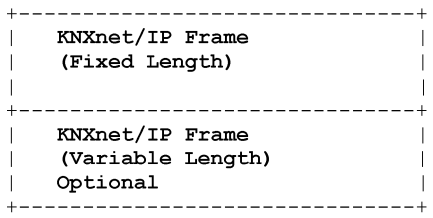


Bild 3 — KNXnet/IP-Frame im Binärformat

Der Typ des KNXnet/IP-Frames wird mithilfe einer KNXnet/IP-Dienstartkennung in der Kopfzeile beschrieben. KNXnet/IP-Dienste schließen unter anderem Informationen bezüglich der Erkennung und Beschreibung, des (Verbindungs-)Managements des Kommunikationskanals sowie der KNX-Datenübertragung ein.

5.2.2.3 Header

5.2.2.3.1 Beschreibung

Jeder KNXnet/IP-Frame umfasst ausnahmslos mindestens den allgemeinen KNXnet/IP-Header, der Informationen zur Protokollversion, dem Header und der Gesamtpaketlänge sowie die KNXnet/IP-Dienstartkennung enthält. Dem KNXnet/IP-Header kann ein KNXnet/IP-Body folgen; dies hängt von dem KNXnet/IP-Dienst ab.

Zeitstempelinformationen und Frame-Zähler sind nicht in dem allgemeinen Header des KNXnet/IP-Frames enthalten, da diese Informationen sehr stark mit bestimmten KNXnet/IP-Dienstarten verknüpft sind und daher als zusätzliche Informationen für bestimmte Kommunikations- und Kanalarten in den Body dieser Dienste eingeschlossen werden.

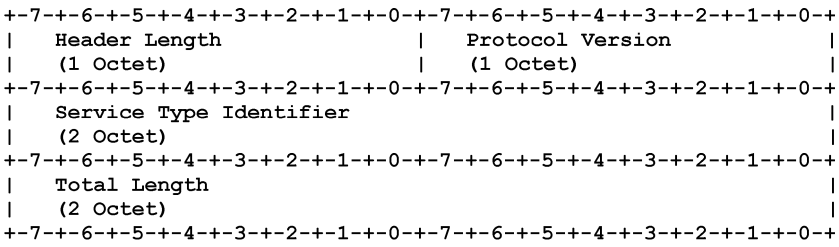


Bild 4 — KNXnet/IP-Header im Binärformat

5.2.2.3.2 Header-Länge

Obwohl die Länge des Headers stets festgelegt ist, kann sich die Größe des Headers mit einer neuen Version des Protokolls ändern. Die Header-Länge kann als Anzeiger der KNXnet/IP-Frame-Daten verwendet werden, um den Anfang des KNXnet/IP-Bodys zu finden.

5.2.2.3.3 Protokollversion

Die Informationen zur Protokollversion geben die Überarbeitung des KNXnet/IP-Protokolls an, auf der der sich anschließende KNXnet/IP-Frame basiert. Sie werden im binär codierten Dezimalformat abgespeichert. Die derzeit einzige gültige Protokollversion ist 1.0 (als Hexadezimalwert 10h dargestellt).

5.2.2.3.4 KNXnet/IP-Dienst

Die KNXnet/IP-Dienstartkennung definiert die Art der Aktion, die ausgeführt werden soll, und den Typ der Nutzdaten, die im KNXnet/IP-Body enthalten sind, wenn anwendbar. Das hohe Oktett der KNXnet/IP-Dienstartkennung kennzeichnet die Dienstartfamilie und das niedrige Oktett die eigentliche Dienstart innerhalb dieser Familie. Für eine ausführliche Beschreibung der Dienste, siehe unten.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5.2.2.3.5 Gesamtlänge

Die Gesamtlänge drückt die gesamte Länge des KNXnet/IP-Frames in Oktetten aus. Die Länge schließt den gesamten KNXnet/IP-Frame, d. h. die Header-Länge des KNXnet/IP-Headers und den gesamten KNXnet/IP-Body, ein.

5.2.3 Host-Protokoll-Unabhängigkeit

5.2.3.1 Host-Protokoll

Die KNXnet/IP-Core-Spezifikation legt die Einbindung von KNX-Protokoll-Implementierungen, die auf Internet Protocol (IP) aufsetzen, fest. Sie beschreibt allgemeine und vom Host-Protokoll unabhängige sowie die bezüglich des Host-Protokolls spezifischen Teile der KNXnet/IP-Kommunikation.

5.2.3.2 Endpunkte

KNXnet/IP legt die HPAI-Struktur (Host Protocol Address Information) fest, die die Kombination aus der IP-Adresse und der Portnummer ist. HPAI sind Daten, die erforderlich sind, um einen KNXnet/IP-Frame an ein anderes Gerät zu senden. Die KNXnet/IP-Spezifikation verwendet die Bezeichnung „KNXnet/IP-Endpunkt“ als logische Sicht einer HPAI, um ein anderes KNXnet/IP-Gerät für bestimmte eindeutige Zwecke zu adressieren.

Jedes KNXnet/IP-Gerät muss genau einen zum Gerät gehörenden, bidirektionalen und verbindungslosen Endpunkt für die Erkennung unterstützen, wenn für das Host-Protokoll Erkennungsdienste erforderlich sind. Es muss mindestens einen bidirektionalen und verbindungslosen Endpunkt für die Kontrolle und mindestens einen bidirektionalen und verbindungsorientierten Endpunkt für die Übertragung von zur Dienstart gehörenden Daten unterstützen.

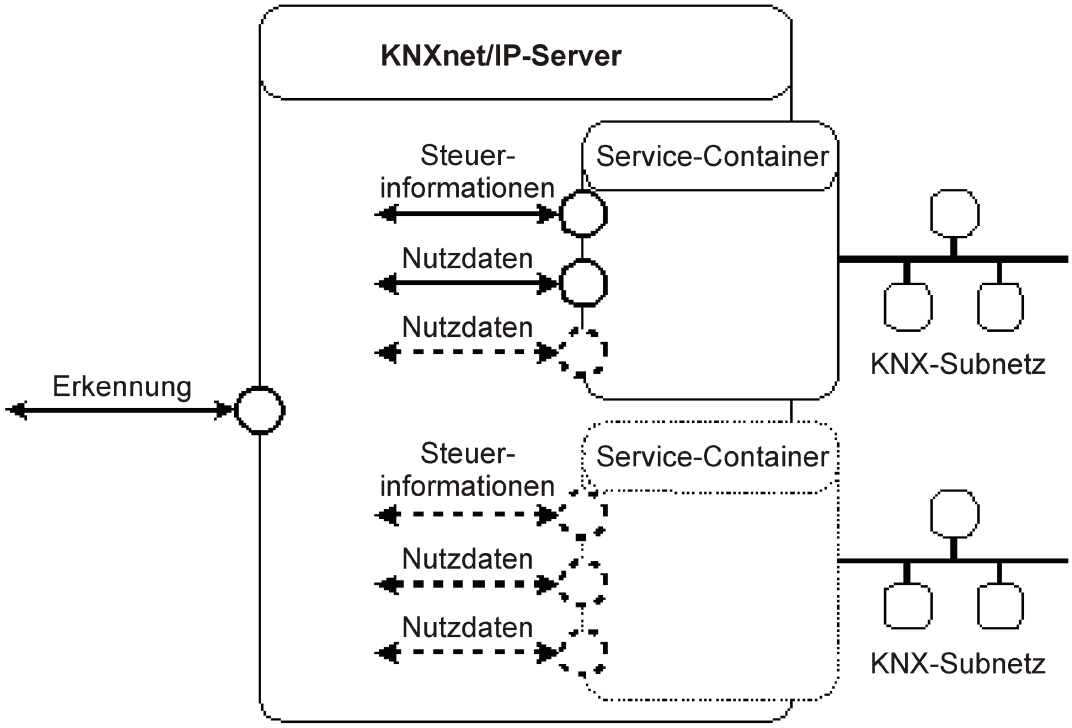


Bild 5 — Beispielkonfiguration für KNXnet/IP-Server-Endpunkte

Der Kontrollendpunkt adressiert eindeutig eine Instanz innerhalb des KNXnet/IP-Servergerätes, die mindestens eine KNXnet/IP-Dienstart bereitstellen muss.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Diese Instanz, der sogenannte Dienst-Container, kann mit einem KNX-Subnetz verbunden sein. Wenn das KNXnet/IP-Servergerät mehr als eine KNX-Subnetzverbindung unterstützt, ist es erforderlich, dass jedes KNX-Subnetz durch einen anderen Kontrollendpunkt abgebildet wird. Der KNXnet/IP-Client betrachtet somit jeden Dienst-Container, der durch einen Kontrollendpunkt abgebildet wird, als unabhängige Instanz, unabhängig davon, ob die Dienst-Container in nur einem oder in zwei getrennten KNXnet/IP-Servergeräten implementiert sind.

Diese KNXnet/IP-Endpunkte stellen eine logische Sicht auf die Kommunikation eines KNXnet/IP-Gerätes dar. Für die eigentliche Implementierung dieser Endpunkte mit verschiedenen Host-Protokollen können transportmedienunabhängige Ansätze, die sich von der logischen Sicht unterscheiden, verwendet werden. Die bidirektionalen KNXnet/IP-Endpunkte könnten z. B. mithilfe von zwei unidirektionalen Kanälen mit dem Host-Protokoll implementiert werden. Es ist daher möglich, dass ein KNXnet/IP-Endpunkt durch mehrere HPAIs repräsentiert wird.

5.2.4 Erkennung und Selbstbeschreibung

5.2.4.1 Einleitung

Insbesondere bei Netzwerken, die Hot-Plug unterstützen und bei denen selbst die Adresszuweisung während der Laufzeit stattfinden kann (z. B. IP-Adresszuweisung über BootP oder DHCP), ist es von großer Bedeutung, nach Geräten innerhalb eines Subnetzes suchen zu können, ohne Netzwerkparameter auf unkonventionellem Weg abrufen und manuell in das Client-Tool eingeben zu müssen, um eine Verbindung aufzubauen. Des Weiteren ist ein Selbstbeschreibungsmechanismus eine wichtige Funktion, um ein genaues Bild der vom KNXnet/IP-Server unterstützten Dienste zu erhalten, ohne das Prinzip „Versuch und Irrtum“ anwenden zu müssen.

5.2.4.2 Erkennung

Jeder KNXnet/IP-Server muss einen Erkennungsmechanismus nach der folgenden Vorgehensweise implementieren. Wenn es für das Host-Protokoll anwendbar ist, wird empfohlen, einen KNXnet/IP-Client mit Unterstützung der Suche nach KNXnet/IP-Servern anstelle der manuellen Eingabe zu implementieren.

Die Erkennungsoperation besteht aus einem SEARCH_REQUEST-Datenpaket, das über Multicast mithilfe des Erkennungsendpunktes gesendet wird und das die HPAI des Erkennungsendpunktes des KNXnet/IP-Clients enthält. Die HPAI können eine Unicast-IP-Adresse enthalten, um die Antworten von den verschiedenen KNXnet/IP-Servern direkt in Punkt-zu-Punkt-Form zu empfangen. Normalerweise sollten sie die KNXnet/IP-Multicast-Adresse der Systemkonfiguration enthalten, um den Empfang von KNXnet/IP-Servern sicherzustellen, die sich in einem anderen Subnetz befinden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

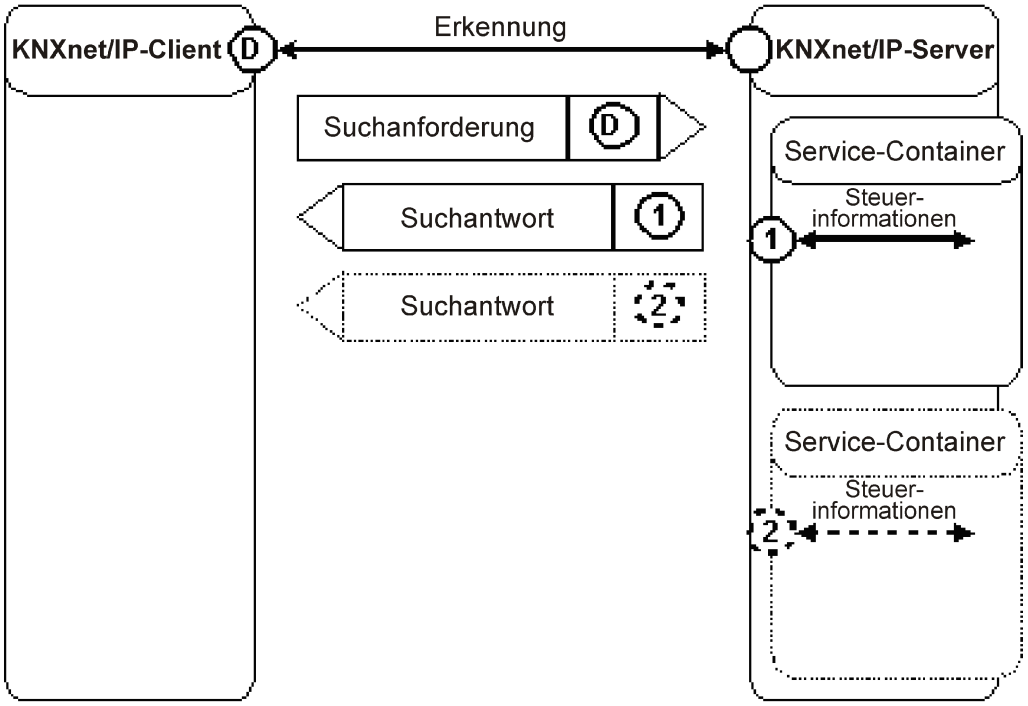


Bild 6 — Erkennungsprozedur

Nach dem Senden der Anforderung muss der KNXnet/IP-Client während der SEARCH_TIMEOUT-Zeit auf SEARCH_RESPONSE-Frames von KNXnet/IP-Servern warten. Nach dieser Zeitdauer muss jeder empfangene SEARCH_RESPONSE-Frame von diesem Client ignoriert werden, bis dieser einen neuen Erkennungszyklus startet. SEARCH_RESPONSE-Frames, die Clients von anderen Clients empfangen, müssen ignoriert werden.

Jeder KNXnet/IP-Server, der einen SEARCH_REQUEST-Dienst empfängt, muss der angegebenen HPAI mithilfe seines Erkennungsendpunktes unverzüglich mit einem SEARCH_RESPONSE-Datenpaket antworten. Eine derartige Antwort enthält nur die HPAI des Kontrollendpunktes des KNXnet/IP-Servers für alle weitere Kommunikation.

Jeder KNXnet/IP-Server muss die Erkennung unterstützten, indem er Suchanforderungen verarbeitet und korrekte Antworten sendet. Ein KNXnet/IP-Server kann Verbindungen mit mehreren KNX-Subnetzen unterstützen; er muss jedoch ein SEARCH_RESPONSE-Datenpaket an den Kontrollendpunkt jedes KNX-Subnetzes senden, mit dem er Verbindungen aufbauen kann, auch dann, wenn er jeweils nur eine Datenverbindung unterstützt.

5.2.4.3 Selbstbeschreibung

Nach dem Erkennen eines KNXnet/IP-Servers sendet der KNXnet/IP-Client normalerweise einen DESCRIPTION_REQUEST über eine Unicast- oder Punkt-zu-Punkt-Verbindung an alle Kontrollendpunkte des KNXnet/IP-Servers. Dazu ist es erforderlich, dass alle KNXnet/IP-Implementierungen Beschreibungsanforderungen unterstützen. Des Weiteren sollte ein KNXnet/IP-Client vor dem Kommunizieren mit einem KNXnet/IP-Server mithilfe des Selbstbeschreibungsmechanismus prüfen, ob der Server die vom Client angeforderten Dienste unterstützt.

Wenn ein KNXnet/IP-Server eine gültige Beschreibungsanforderung empfängt, muss er mit einem DESCRIPTION_RESPONSE-Paket antworten, das Informationen zu dem Bereich unterstützter Protokollversionen und den eigenen Funktionen sowie Statusinformationen und optional einen Anzeigenamen für diese KNX-Verbindung des KNXnet/IP-Servers bereitstellt. Da ein KNXnet/IP-Server Verbindungen mit mehreren KNX-Subnetzen unterstützen kann, muss er das Antworten auf Erkennungsanforderungen für jede potentielle KNX-Subnetzverbindung unterstützen, die durch die Erkennungsantworten gemeldet wird.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.2.5 Kommunikationskanäle

5.2.5.1 Einleitung

Ein Kommunikationskanal ist die Datenendpunktverbindung zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server. Datenendpunktverbindungen werden für Dienste aufgebaut, die eine Punkt-zu-Punkt-Kommunikation erfordern, z. B. Tunnelling oder Device Management. Jede Punkt-zu-Punkt-Verbindung zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server muss vom Client initiiert werden. Jeder KNXnet/IP-Server muss mindestens jeweils eine Client-Verbindung unterstützen. Er kann auch mehrere Client-Verbindungen gleichzeitig unterstützen, muss jedoch sicherstellen, dass vorhandene Verbindungen durch das Annehmen neuer Verbindungen nicht beeinflusst werden (ein KNXnet/IP-Server darf z. B. keine Tunnelling-Verbindung mit demselben physikalischen Zugriff auf ein KNX-Subnetz in verschiedenen Modi, Sicherungsschicht oder Busmonitor-Schicht, annehmen).

5.2.5.2 Verbindung herstellen

Um eine Verbindung zwischen einem KNXnet/IP-Client und einem KNXnet/IP-Server herzustellen, muss der Client einen CONNECT_REQUEST-Frame an den Kontrollendpunkt des Servers senden. Diese Anforderung stellt Informationen zu der angeforderten Verbindungsart (z. B. Daten-Tunnelling oder Fernprotokollierung), allgemeine und in Bezug auf die Verbindungsart spezifische Optionen (z. B. Sicherungsschicht oder Busmonitor-Modus[2)]) sowie die HPAI des Datenendpunktes, die der Client für diesen Kommunikationskanal verwenden möchte, bereit.

Vor dem Senden einer Verbindungsanforderung einer spezifischen Art (mit spezifischen Optionen) sollte der KNXnet/IP-Client mithilfe der vom KNXnet/IP-Server empfangenen Selbstbeschreibungsinformationen prüfen, ob der Server die angeforderte Verbindungsart und/oder alle angeforderten Optionen unterstützt.

Der KNXnet/IP-Server muss dann in jedem Fall einen CONNECT_RESPONSE-Frame an den KNXnet/IP-Client zurücksenden, der den Aufbau der Verbindung anfordert, in dem der Status der Anforderung bereitstellt wird (ACK/NACK mit erweiterten Statusinformationen, wenn anwendbar). Wenn die Anforderung vom Server angenommen wurde, enthält der CONNECT_RESPONSE-Frame zusätzlich eine Kennung sowie die HPAI des Datenendpunktes, die der Server nun für diesen Kommunikationskanal[3)] vorbereitet hat.

Nach dem Senden der Verbindungsanforderung muss der KNXnet/IP-Client während der vom Host-Protokoll abhängigen CONNECT_REQUEST_TIMEOUT-Zeit (= 10 s) auf den Antwort-Frame vom KNXnet/IP-Server warten. Nach dieser Zeitdauer muss jeder empfangene Antwort-Frame von diesem Client ignoriert werden, bis dieser eine neue Verbindungsanforderung startet.

Die aktuelle Protokoll-Spezifikation setzt voraus, dass eine Verbindung nicht von mehreren Clients gemeinsam genutzt werden darf. Ein KNXnet/IP-Server darf daher nicht mehrere Verbindungsanforderungen derselben Art, z. B. auf derselben physikalischen KNX-Verbindung, annehmen, obwohl er durchaus mehrere physikalische Verbindungen implementieren kann, die logisch jeweils als unabhängiger KNXnet/IP-Server dargestellt werden, wenn dies von dem verwendeten Host-Protokoll unterstützt wird. Die Client-Implementierung kann auf dieser Beschränkung aufbauen und muss ein derartiges Szenario einer gemeinsam genutzten Verbindung nicht unterstützen. Durch bestimmte Dienstfamilien bedingte Ausnahmen zu dieser allgemeinen Regel sind in dem KNXnet/IP-Kapitel der entsprechenden Dienstfamilie beschrieben.

---

2) Die Liste der unterstützten Schichten und Dienste sollte in zukünftigen Überarbeitungen erweitert werden.

3) Es sollte beachtet werden, dass eine KNXnet/IP-Verbindung aus technischen Gründen aus mehreren logischen Verbindungen in der Host-Protokoll-Schicht bestehen kann.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

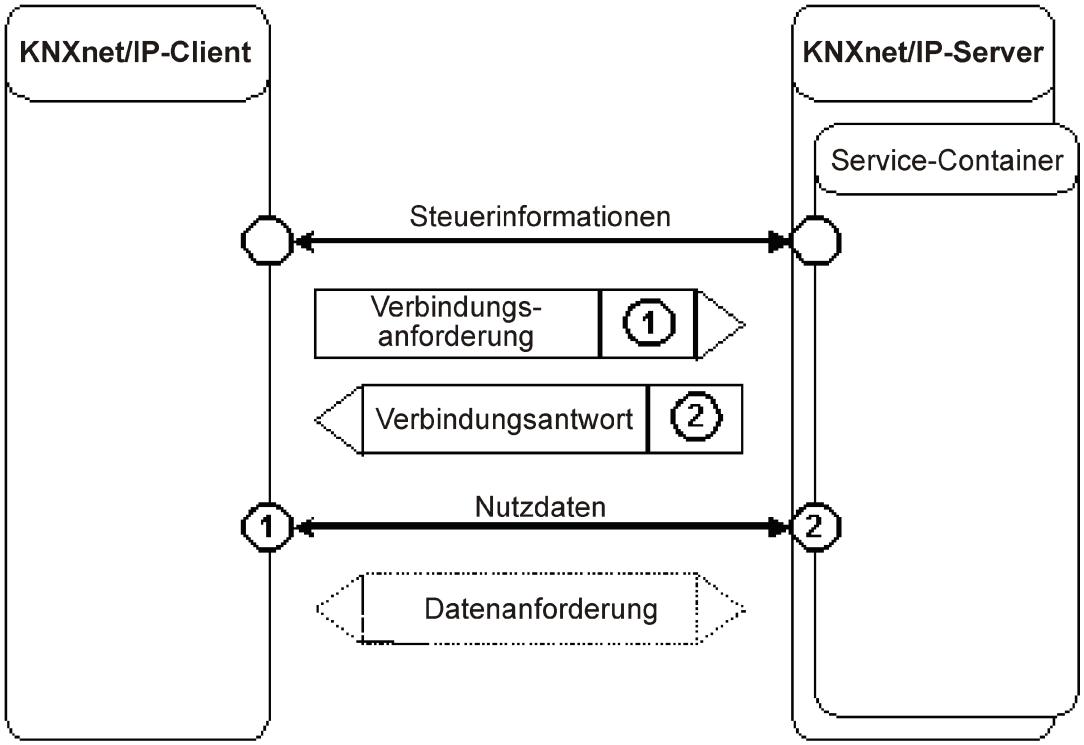


Bild 7 — Aufbau einer Datenverbindung

5.2.5.3 Connection-Header

5.2.5.3.1 Beschreibung

Der Body eines jeden KNXnet/IP-Frames, der über einen aufgebauten Kommunikationskanal gesendet wird, beginnt mit Datenfeldern, die zusätzliche allgemeine Informationen zur Datenverbindung enthalten. Die Menge dieser Daten und die Art der eingeschlossenen Informationen wird durch verschiedene Optionen während der Verbindungsphase eines Kommunikationskanals bestimmt. Die Gesamtheit dieser Datenfelder wird als „Connection-Header“ bezeichnet und sein Aufbau unterscheidet sich stark in Abhängigkeit von den bereits erwähnten Verbindungsoptionen. Nur die Reihenfolge, in der die verschiedenen Datenfelder im Connection-Header gespeichert werden, ist festgelegt.

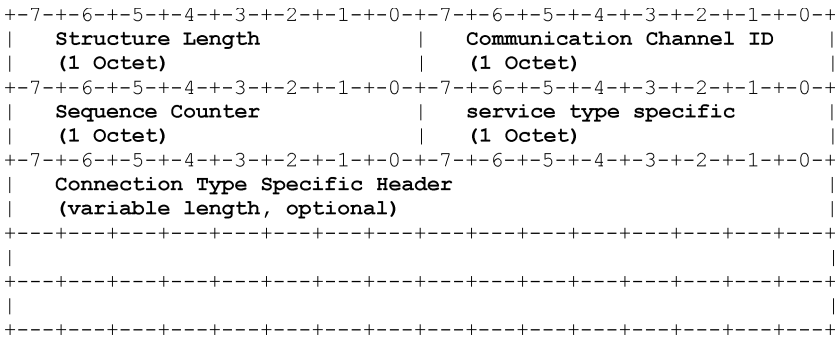


Bild 8 — Üblicher Connection-Header

5.2.5.3.2 Strukturlänge

Die Strukturlänge bezeichnet die Gesamtlänge des Connection-Headers.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5.2.5.3.3 Kommunikationskanal-ID

Der KNXnet/IP-Server weist jedem aufgebauten Kommunikationskanal eine Kommunikationskanal-ID zu.

5.2.5.3.4 Folgezähler

Der Folgezähler wird für jeden Kommunikationskanal verwaltet. Er muss sich für jeden Kommunikationskanal einzeln bei jedem KNXnet/IP-Frame, der über die Datenverbindung gesendet wird, um eins erhöhen. Beide KNXnet/IP-Geräte, die den Kommunikationskanal aufrechterhalten, verfügen über unabhängige Folgezähler.

Jedes Mal, wenn eine Verbindung aufgebaut wird, muss der Zähler für diese Verbindung auf 0 gesetzt werden, sodass der erste KNXnet/IP-Frame, der über einen aufgebauten Kommunikationskanal gesendet wird, einen Folgezähler von 0 aufweist.

Bei Verbindungen innerhalb einer TCP-Verbindung darf der Folgezähler nicht vom Empfänger ausgewertet werden. Der Sender darf den Folgezähler auf null setzen.

5.2.5.3.5 Verbindungsartspezifische Header-Elemente

Die verbindungsartspezifischen Header-Elemente sind optional und in ihrer Länge in Abhängigkeit von der Art der Verbindung variabel.

5.2.5.4 Heartbeat-Überwachung

Host-Protokolle, die keine Mechanismen zur Prüfung der Lebensdauer wie UDP/IP bereitstellen, benötigen eine Vorgehensweise, um Kommunikationsausfälle im KNX- oder Tunnelling-Netzwerk zu ermitteln. Um derartige Situationen aufzudecken, wurde die Heartbeat-Überwachung entwickelt und muss sowohl von KNXnet/IP-Clients als auch KNXnet/IP-Servern implementiert werden.

Der Client muss regelmäßig, d. h. alle 60 s, einen CONNECTIONSTATE_REQUEST-Frame an den Kontrollendpunkt des Servers senden, der unverzüglich mit einem CONNECTIONSTATE_RESPONSE-Frame antworten muss (dies zählt als Heartbeat-Antwort).

Wenn der KNXnet/IP-Client die Heartbeat-Antwort nicht innerhalb der CONNECTIONSTATE_REQUEST_TIMEOUT (= 10 s) empfängt oder der Status der empfangenen Heartbeat-Antwort irgendeinen Fehlerzustand meldet, muss der Client den CONNECTIONSTATE_REQUEST dreimal wiederholen und dann die Verbindung beenden, indem er einen DISCONNECT_REQUEST an den Kontrollendpunkt des Servers sendet.

Wenn der KNXnet/IP-Server eine Heartbeat-Anforderung nicht innerhalb von 120 s des letzten korrekt empfangenen Nachrichten-Frames empfängt, muss der Server die Verbindung beenden, indem er einen DISCONNECT_REQUEST an den Kontrollendpunkt des Clients sendet. Der Server darf die Zeitüberschreitung nicht erneut auslösen, nachdem Nachrichten mit einer unerwarteten Folgenummer empfangen wurden.

5.2.5.5 Verbindung trennen

Normalerweise beendet der Client die Verbindung. Während des normalen Betriebs muss der Client einen DISCONNECT_REQUEST an den Kontrollendpunkt des Servers senden, um die Beendigung der Datenkanalverbindung anzufordern.

Der Client sollte, wenn möglich, versuchen, die Verbindung nicht abrupt zu beenden, auch bei Fehlerbedingungen. Der Server kann die Verbindung mit dem Client im Fall von internen Problemen oder wenn er ungültige Datenpakete empfängt trennen, indem er einen DISCONNECT_REQUEST sendet; es wird jedoch empfohlen, den Client die Verbindung beenden zu lassen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

Das KNXnet/IP-Gerät, das den DISCONNECT_REQUEST vom Kommunikationspartner empfängt, muss die Operation mit einem DISCONNECT_RESPONSE-Frame bestätigen. Dieses Datenpaket meldet die endgültige Beendigung des zuvor aufgebauten Kommunikationskanals.

5.2.6 Allgemeine Implementierungsrichtlinien

5.2.6.1 Einleitung

Dieser Abschnitt legt die Programmierungsrichtlinien fest, die bei der Implementierung von KNXnet/IP-Servern bzw. KNXnet/IP-Clients beachtet werden müssen.

5.2.6.2 KNXnet/IP-Server

— Wenn ein Server ein Datenpaket mit einem nicht unterstützten Versionsfeld empfängt, muss er mit einer NACK-Nachricht antworten, die im Statusfeld „E_VERSION_NOT_SUPPORTED“ angibt.

— Wenn ein ungültiges Datenpaket empfangen wird, muss die Implementierung das Datenpaket ignorieren, ohne eine weitere Aktion auszuführen.

— Wenn eine Verbindung aufgebaut wird, müssen alle Datenpakete mit derselben Protokollversion gesendet werden.

— Wenn eine Verbindung aufgebaut wird und sich die Protokollversion innerhalb der empfangenen Datenpakete ändert, muss der Server die Verbindung beenden.

5.2.6.3 KNXnet/IP-Clients

— Wenn ein Client ein Datenpaket mit einem nicht unterstützten Versionsfeld empfängt, muss er mit einer NACK-Nachricht antworten, die im Statusfeld „E_VERSION_NOT_SUPPORTED“ angibt. Wenn eine Verbindung mit diesem Server, der Datenpakete mit einer nicht unterstützten Protokollversion sendet, aufgebaut wird, muss der Client die Verbindung trennen. Der Client kann anschließend versuchen, erneut eine Verbindung mit dem Server aufzubauen.

— Wenn ein ungültiges Datenpaket empfangen wird, muss die Implementierung das Datenpaket ignorieren, ohne eine weitere Aktion auszuführen.

— Wenn eine Verbindung aufgebaut wird, müssen alle Datenpakete mit derselben Protokollversion gesendet werden.

— Wenn eine Verbindung aufgebaut wird und sich die Protokollversion innerhalb der empfangenen Datenpakete ändert, muss der Client die Verbindung zum Server trennen. Der Client kann anschließend versuchen, erneut eine Verbindung mit dem Server aufzubauen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.2.6.4 Einstellungen für KNXnet/IP-Router

5.2.6.4.1 Werksseitige Standardeinstellungen für KNXnet/IP-Router

Eine wichtige Funktion von KNXnet/IP-Routern ist die Bereitstellung eines ordnungsgemäßen KNXnet/IP-Routings ohne Benutzereingriff. Dieses sofort betriebsbereite Routing-Verhalten („Plug and Play“) setzt eine standardisierte Werkskonfiguration voraus.

— Router müssen mit der individuellen Standardadresse FF00h ausgeliefert werden.

— Die Routing-Multicast-Adresse entspricht der Multicast-Adresse der Systemkonfiguration.

— KNXnet/IP-Broadcast-Telegramme müssen von einem KNX-Subnetz zu einem anderen geleitet werden, auch wenn die KNXnet/IP-Routing-Geräte nach wie vor mit ihrer Standard-Werkskonfiguration verwendet werden.

— Das KNXnet/IP-Routing muss bereits funktionieren, auch wenn noch keine gültige Unicast-IP-Adresse vom KNXnet/IP-Routing-Gerät bezogen oder diesem zugewiesen wurde.

— Wenn einem KNXnet/IP-Router eine individuelle Adresse über das KNX-Subnetz zugewiesen wurde, muss das Routing bereits funktionieren und das Tunnelling muss für die (weitere) Konfiguration des KNXnet/IP-Routers verfügbar sein.

5.2.6.4.2 Zuweisung einer IP-Adresse zu einem KNXnet/IP-Router

KNXnet/IP-Router müssen ein sofort betriebsbereites KNXnet/IP-Routing („Plug and Play“) unterstützen, auch wenn noch keine gültige Unicast-IP-Adresse von einem DHCP-Server durch manuelle Eingabe oder durch Konfiguration über ETS bezogen wurde. Dies kann erfordern, dass der IP-Protokollstapel Multicast-IP-Nachrichten senden und empfangen können muss, obwohl noch keine gültige Unicast-IP-Adresse bezogen wurde.

Wenn ein IP-Protokollstapel Multicasting nicht ohne eine zugewiesene Unicast-IP-Adresse unterstützt, muss der KNXnet/IP-Router eine Unicast-IP-Adresse über AutoIP beziehen oder sich die standardmäßige Unicast-IP-Addresse für KNXnet/IP-Quellen 0.0.0.0 selbst zuweisen.

Wenn keine gültige Unicast-IP-Adresse bezogen wurde, muss der KNXnet/IP-Router für das Routing die standardmäßige Unicast-IP-Addresse für KNXnet/IP-Quellen 0.0.0.0 verwenden, darf jedoch kein KNXnet/IP-Tunnelling unterstützen.

5.2.6.5 Ersteinrichtungsmaßnahmen für KNXnet/IP-Server

5.2.6.5.1 Allgemeines

KNXnet/IP-Geräte müssen in derselben Art und Weise wie herkömmliche KNX-Geräte konfigurierbar sein. In unkonfiguriertem Zustand müssen KNXnet/IP-Router mit Default-Werten arbeiten, damit KNX-Telegramme von einem KNX-Subnetz zu einem anderen gelangen können; dadurch können KNX-Router (Linien- und Bereichskoppler) nahtlos durch KNXnet/IP-Router ersetzt werden.

Diese Anforderung setzt voraus, dass individuelle KNX-Adressen über das gesamte IP-Netzwerk hinweg eindeutig sind. Wenn KNXnet/IP-Geräte zweier unabhängiger Installationen mit demselben IP-Netzwerk verbunden werden oder wenn ein KNX-Projekt aus mehreren Installationen besteht, kann die Verwendung einer werksseitigen Default-Routing-Konfiguration nicht gewährleisten, dass KNX-Telegramme an ihr beabsichtigtes Ziel übertragen werden, da dieselbe KNX-Adresse (individuelle oder Gruppenadresse) in den verschiedenen Installationen vorhanden sein könnte.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

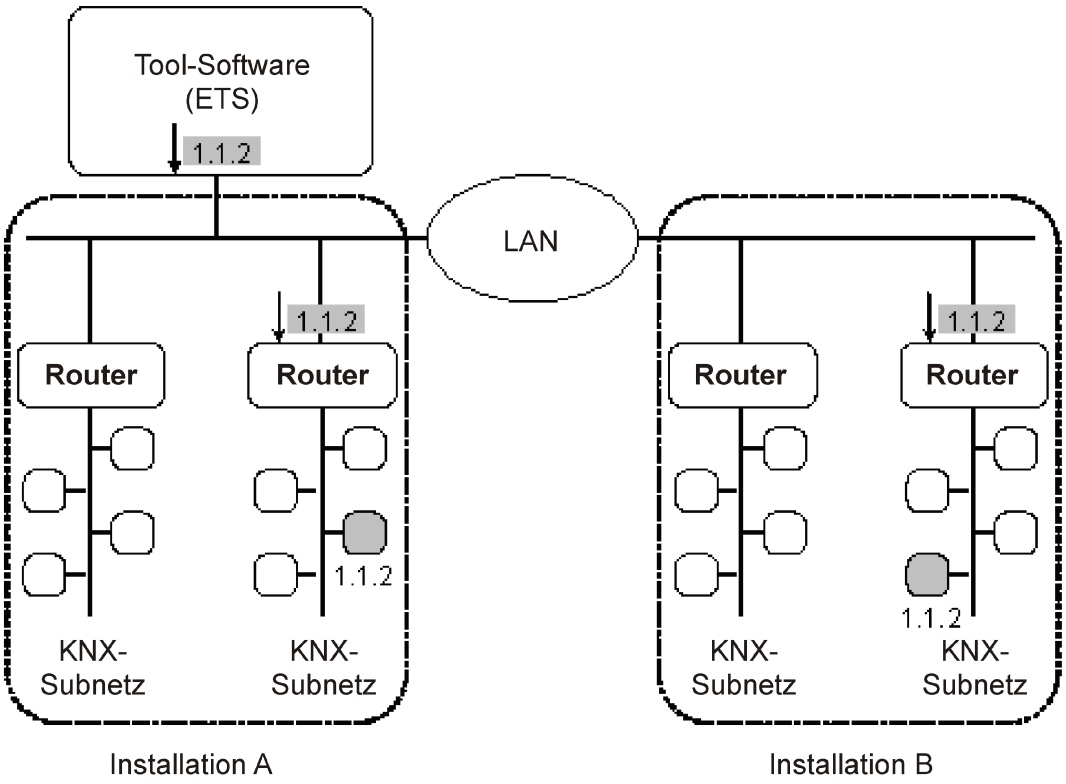


Bild 9 — KNX-Projekt mit mehreren Installationen

Unter der Voraussetzung, dass nur eine Installation mit dem IP-Netzwerk verbunden ist, gelten folgende Regeln:

1) Nach dem Einschalten durchläuft das KNXnet/IP-Gerät die im Kapitel „KNXnet/IP Core“ unter 5.2.8.5 „IP-Adresszuweisung“ beschriebene Prozedur, um eine individuelle IP-Adresse zu beziehen.

2) Wenn die Tool-Software mit einem seriellen Schnittstellengerät (RS232) oder einer KNX-USB-Schnittstelle verbunden ist, kann sie solange nur auf KNX-Geräte im lokalen KNX-Subnetz (einschließlich des lokalen KNXnet/IP-Routers) zugreifen, bis alle zu einem Projekt gehörenden KNXnet/IP-Router-Geräte erfolgreich konfiguriert wurden.

3) Die Tool-Software sollte stets versuchen, zuerst die KNXnet/IP-Router-Geräte zu konfigurieren, um Zugriff auf KNX-Geräte hinter möglicherweise noch unkonfigurierten KNXnet/IP-Routern zu erhalten.

4) Wenn die Tool-Software direkt mit dem IP-Netzwerk verbunden ist, kann sie auf alle KNXnet/IP-Geräte und über die konfigurierten Router auf die entsprechenden KNX-Subnetze zugreifen.

5) Die Tool-Software sollte das IP-Netzwerk für die Einrichtung von Projekten verwenden, die KNXnet/IP-Geräte enthalten.

6) KNXnet/IP-Geräte können in einer einzigen Konfigurationsprozedur (Zuweisung individueller KNX-Adressen und Parameter-Download) vollständig konfiguriert werden.

7) Zuweisung von individuellen KNX-Adressen: Wenn die Tool-Software über ein serielles KNX-Schnittstellengerät (RS232) oder über eine KNX-USB-Schnittstelle mit dem KNX-Netzwerk verbunden ist, findet die herkömmliche KNX-Management-Prozedur für KNXnet/IP-Geräte sowie für andere KNX-Knoten Anwendung. Geräte hinter unkonfigurierten Routern sind nicht erreichbar. Wenn die Tool-Software mit dem IP-Netzwerk verbunden ist, findet die nachfolgend beschriebene

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Konfigurationsprozedur für KNXnet/IP-Geräte Anwendung. Vor dem Einrichten der KNX-Medien auf der Feldebene muss die Tool-Software zuerst alle KNXnet/IP-Router-Geräte konfigurieren.

8) Parameter-Download: Wenn die Tool-Software über eine serielle Schnittstelle mit dem KNX-Netzwerk verbunden ist, findet die herkömmliche KNX-Management-Prozedur für KNXnet/IP-Geräte sowie für andere KNX-Knoten Anwendung. Wenn die Tool-Software mit dem IP-Netzwerk verbunden ist, wird zu jedem KNXnet/IP-Gerät eine Management-Verbindung aufgebaut, um die Geräteparameter herunterzuladen (siehe Konfigurationsprozedur). Nachdem alle KNXnet/IP-Router-Geräte konfiguriert wurden, kann die Tool-Software für die weitere Einrichtung und den Download über eine KNXnet/IP-Tunnelling-Verbindung auf alle anderen KNX-Knoten des Projekts zugreifen.

9) Wenn aus den SEARCH_RESPONSE-Antworten ersichtlich wird, dass die KNXnet/IP-Geräte unterschiedliche IP-Adressbereiche verwenden, muss die Tool-Software eine Fehlermeldung anzeigen.

10) Wenn aus den SEARCH_RESPONSE-Antworten ersichtlich wird, dass sich die IP-Adresse eines KNXnet/IP-Gerätes von den Netzwerkeinstellungen der Tool-Software unterscheidet und die IP-Adresse des KNXnet/IP-Gerätes eine AutoIP-Adresse ist, muss die Tool-Software eine Fehlermeldung sowie eine Bedienschaltfläche anzeigen, mit der der Benutzer das KNXnet/IP-Gerät über KNXnet/IP-Routing mit dem verbindungslosen KNX-Neustartdienst zurücksetzen kann.

5.2.6.5.2 Konfigurationsprozedur für die Konfiguration über KNXnet/IP-Routing

Die Tool-Software ist über ein serielles KNX-Schnittstellengerät (RS232) oder eine KNX-USB-Schnittstelle mit einem KNX-Subnetz (1.1) verbunden. Ein zweites KNX-Subnetz (1.2) ist mit dem ersten KNX-Subnetz über zwei KNXnet/IP-Router und ein LAN verbunden. Alle Geräte einschließlich der Router sind zunächst nicht konfiguriert.

Die Tool-Software verwendet KNX-Management-Prozeduren und (indirekt) KNXnet/IP-Routing, um die beiden KNXnet/IP-Router zu konfigurieren.

Im Folgenden wird die Konfigurationsprozedur für die Zuweisung der individuellen KNX-Adresse und die Konfiguration der Parameter eines KNXnet/IP-Gerätes beschrieben:

1) Die Tool-Software fordert den Benutzer auf, den Programmiermodus des KNXnet/IP-Gerätes zu aktivieren.

   ANMERKUNG Dies kann durch Drücken der Programmiertaste auf dem KNXnet/IP-Gerät erfolgen.

2) Die Tool-Software sendet eine KNX-Leseanforderung (Broadcast). Der KNXnet/IP-Router in diesem KNX-Subnetz sendet diesen Broadcast an weitere KNXnet/IP-Router, die diesen wiederum an ihre KNX-Subnetze weiterleiten und das Telegramm selbst verarbeiten, sofern der Programmiermodus aktiviert ist.

3) Die Tool-Software muss prüfen, ob mehr als ein Gerät mit „Programmiermodus aktiv“ antwortet, und die Prozedur in einem solchen Fall mit einer beschreibenden Meldung über die Ursache abbrechen. Der KNXnet/IP-Router in diesem KNX-Subnetz leitet die Antwort(en) an das KNX-Subnetz weiter.

4) Die Tool-Software muss eine KNX-Schreibanforderung (Broadcast) senden, um die individuelle KNX-Adresse in das KNXnet/IP-Gerät zu schreiben. Der KNXnet/IP-Router in diesem KNX-Subnetz sendet diesen Broadcast an weitere KNXnet/IP-Router, die diesen wiederum an ihre KNX-Subnetze weiterleiten und das Telegramm selbst verarbeiten, sofern der Programmiermodus aktiviert ist.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5) Die Tool-Software muss eine KNX-Verbindung mit dem KNXnet/IP-Gerät aufbauen, um die Konfigurationsparameter (Eigenschaften) herunterzuladen. Dafür ist es erforderlich, dass der KNXnet/IP-Router, der in demselben KNX-Subnetz wie die Tool-Software vorhanden ist, zuerst konfiguriert wird, bevor weitere KNXnet/IP-Geräte konfiguriert werden können.

6) Nach dem Herunterladen der Parameter muss die Tool-Software das KNXnet/IP-Gerät zurücksetzen, damit die Parameter wirksam werden.

5.2.6.5.3 Konfigurationsprozedur für die Konfiguration über KNXnet/IP Device Management

Die Tool-Software ist direkt mit einem LAN verbunden. Zwei KNX-Subnetze, (1.1) und (1.2), sind mit dem LAN über zwei KNXnet/IP-Router verbunden. Alle Geräte einschließlich der Router sind zunächst nicht konfiguriert.

Die Tool-Software muss KNXnet/IP Device Management verwenden, um die beiden KNXnet/IP-Router zu konfigurieren.

Im Folgenden wird die Konfigurationsprozedur für die Zuweisung der individuellen KNX-Adresse und die Konfiguration der Parameter eines KNXnet/IP-Gerätes beschrieben:

1) Die Tool-Software muss den Benutzer auffordern, den Programmiermodus des KNXnet/IP-Gerätes zu aktivieren.

   ANMERKUNG Dies kann durch Drücken der Programmiertaste auf dem KNXnet/IP-Gerät erfolgen.

2) Die Tool-Software muss einen KNXnet/IP-SEARCH_REQUEST-Frame senden.

3) Die Tool-Software muss prüfen, ob mehr als ein KNXnet/IP-Gerät (Dienst-Container) mit dem Gerätestatus „Programmiermodus aktiv“ antwortet und die Prozedur in einem solchen Fall abbrechen.

4) Die Tool-Software muss die IP-Adresse von dem SEARCH_RESPONSE-Frame des KNXnet/IP-Gerätes verwenden, um eine Device-Management-Verbindung mit dem Gerät aufzubauen.

5) Die Tool-Software muss die individuelle KNX-Adresse, die Projektkennung sowie Subnetzinformationen festlegen, wenn anwendbar.

6) Zu diesem Zeitpunkt kann die Tool-Software zusätzliche Parameter herunterladen, wenn erforderlich.

7) Nach dem erfolgreichen Trennen der Device-Management-Verbindung oder dem Senden eines reset_req-Dienstes an das Gerät, müssen die geänderten Werte in das Gerät geschrieben und das Gerät neu gestartet werden.

5.2.7 Datenpaketstrukturen

5.2.7.1 Einleitung

Alle KNXnet/IP-Frames müssen einen gemeinsamen Header aufweisen, der aus Informationen zur Header-Länge, der Protokollversion, der KNXnet/IP-Dienstartkennung und der Gesamtlänge des KNXnet/IP-Frames besteht.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

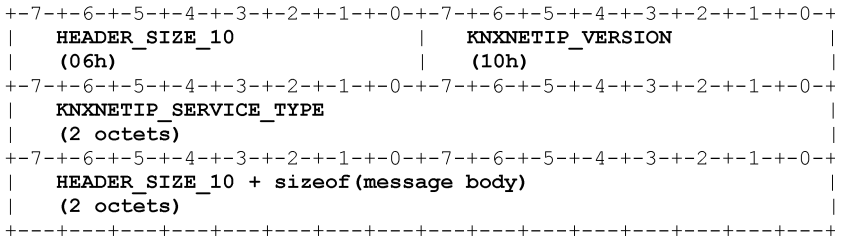


Bild 10 — KNXnet/IP-Nachrichten-Header

Anforderungen, die an verbindungslose KNXnet/IP-Endpunkte gesendet werden, müssen Informationen zur Rückkehradresse enthalten. Diese HPAI für den Empfang der Antwortinformationen stellen stets die ersten Daten des KNXnet/IP-Bodys derartiger Anforderungen dar. Zusätzliche, zum KNXnet/IP-Dienst gehörende Daten können sich anschließen. Antwortpakete enthalten diese Art von Informationen zur Rückkehradresse nicht.

5.2.7.2 Übliche Konstanten

5.2.7.2.1 HEADER_SIZE_10

Diese Konstante mit dem Wert 06h kennzeichnet den KNXnet/IP-Header, wie in der Protokollversion 1.0 definiert.

5.2.7.2.2 KNXNETIP_VERSION_10

Diese Konstante mit dem Wert 10h kennzeichnet die KNXnet/IP-Protokollversion 1.0.

5.2.7.3 Übliche Fehlercodes

5.2.7.3.1 E_NO_ERROR

Diese Konstante mit dem Wert 00h kennzeichnet eine erfolgreiche Operation.

5.2.7.3.2 E_HOST_PROTOCOL_TYPE

Diese Konstante mit dem Wert 01h kennzeichnet, dass das angeforderte Host-Protokoll nicht von dem KNXnet/IP-Gerät unterstützt wird.

5.2.7.3.3 E_VERSION_NOT_SUPPORTED

Diese Konstante mit dem Wert 02h kennzeichnet, dass die angeforderte Protokollversion nicht von dem KNXnet/IP-Gerät unterstützt wird.

5.2.7.3.4 E_SEQUENCE_NUMBER

Diese Konstante mit dem Wert 04h kennzeichnet, dass die empfangene Folgenummer fehlerhaft ist.

5.2.7.4 KNXnet/IP-Dienste

5.2.7.4.1 KNXnet/IP-Core-Dienste

5.2.7.4.1.1 SEARCH_REQUEST

Diese Konstante mit dem Wert 0201h kennzeichnet die Art des KNXnet/IP-Dienstes, der von einem KNXnet/IP-Client gesendet wird, um nach verfügbaren KNXnet/IP-Servern zu suchen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5.2.7.4.1.2 SEARCH_RESPONSE

Diese Konstante mit dem Wert 0202h kennzeichnet die Art des KNXnet/IP-Dienstes, der von einem KNXnet/IP-Server gesendet wird, wenn er auf einen KNXnet/IP-SEARCH_REQUEST antwortet.

5.2.7.4.1.3 DESCRIPTION_REQUEST

Diese Konstante mit dem Wert 0203h kennzeichnet die Art des KNXnet/IP-Dienstes, der von einem KNXnet/IP-Client an einen KNXnet/IP-Server gesendet wird, um Informationen zu den Funktionen und unterstützten Diensten abzurufen.

5.2.7.4.1.4 DESCRIPTION_RESPONSE

Diese Konstante mit dem Wert 0204h kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Server als Antwort auf einen DESCRIPTION_REQUEST gesendet wird, um Informationen zur Server-Implementierung bereitzustellen.

5.2.7.4.1.5 CONNECT_REQUEST

Diese Konstante mit dem Wert 0205h kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Client gesendet wird, um einen Kommunikationskanal mit einem KNXnet/IP-Server aufzubauen.

5.2.7.4.1.6 CONNECT_RESPONSE

Diese Konstante mit dem Wert 0206h kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Server als Antwort auf ein CONNECT_REQUEST-Telegramm gesendet wird.

5.2.7.4.1.7 CONNECTIONSTATE_REQUEST

Diese Konstante mit dem Wert 0207h kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Client gesendet wird, um den Verbindungsstatus einer mit einem KNXnet/IP-Server aufgebauten Verbindung anzufordern.

5.2.7.4.1.8 CONNECTIONSTATE_RESPONSE

Diese Konstante mit dem Wert 0208h kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Server gesendet wird, wenn er einen CONNECTIONSTATE_REQUEST für eine aufgebaute Verbindung empfängt.

5.2.7.4.1.9 DISCONNECT_REQUEST

Diese Konstante mit dem Wert 0209h kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Gerät, normalerweise dem Client, gesendet wird, um eine aufgebaute Verbindung zu beenden.

5.2.7.4.1.10 DISCONNECT_RESPONSE

Diese Konstante mit dem Wert 020Ah kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Gerät, normalerweise dem Server, als Antwort auf einen DISCONNECT_REQUEST gesendet wird.

5.2.7.4.1.11 SEARCH_REQUEST_EXTENDED

Diese Konstante mit dem Wert 020Bh kennzeichnet die Art des KNXnet/IP-Dienstes, der von einem KNXnet/IP-Client gesendet wird, um nach verfügbaren KNXnet/IP-Servern zu suchen und erweiterte Informationen zu den verfügbaren KNXnet/IP-Servern zu empfangen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.2.7.4.1.12 SEARCH_RESPONSE_EXTENDED

Diese Konstante mit dem Wert 020Ch kennzeichnet die Art des KNXnet/IP-Dienstes, der vom KNXnet/IP-Server als Antwort auf einen SEARCH_REQUEST-EXTENDED gesendet wird.

5.2.7.5 Platzhalter

5.2.7.5.1 HPAI (Host Protocol Address Information)

Die HPAI-Struktur muss den Adressinformationen entsprechen, die für die eindeutige Identifizierung eines Kommunikationskanals auf dem Host-Protokoll erforderlich sind. Ihre Größe kann bei verschiedenen Host-Protokollen variieren. Für eine spezifische Definition der HPAI siehe die entsprechenden Anhänge der KNXnet/IP-Spezifikation zu den Host-Protokollen.

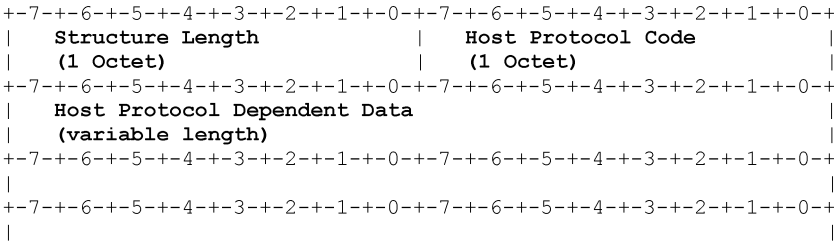


Bild 11 — HPAI-Struktur im Binärformat

5.2.7.5.2 CRI (Connection Request Information)

Die CRI-Struktur muss den zusätzlichen Informationen entsprechen, die für die verschiedenen Arten von Kommunikationskanälen zur Erfüllung einer Verbindungsanforderung notwendig sind. Da diese Struktur zwei Unterstrukturen umfassen muss, die sowohl vom Host-Protokoll unabhängige Daten als auch vom Host-Protokoll abhängige Informationen enthalten, müssen für die spezifische Definition der CRI die Beschreibung der Verbindungsart sowie die entsprechenden Teile der KNXnet/IP-Spezifikation zu den Host-Protokollen konsultiert werden.

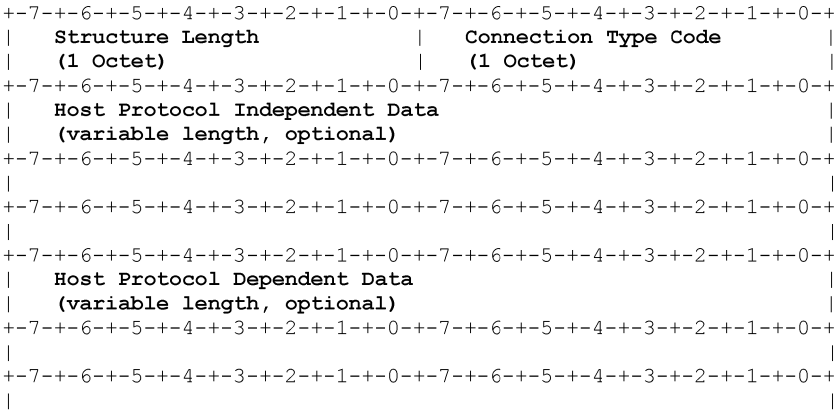


Bild 12 — CRI-Struktur im Binärformat

5.2.7.5.3 CRD (Connection Response Data Block)

Die CRD-Struktur muss dem Datenblock entsprechen, der mit dem CONNECT_RESPONSE-Frame zurückgegeben wird. Da diese Struktur zwei Unterstrukturen umfassen muss, die sowohl vom Host-Protokoll unabhängige Daten als auch vom Host-Protokoll abhängige Informationen enthalten, müssen für die spezifische Definition der CRD die Beschreibung der Verbindungsart sowie die entsprechenden Teile der KNXnet/IP-Spezifikation zu den Host-Protokollen konsultiert werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

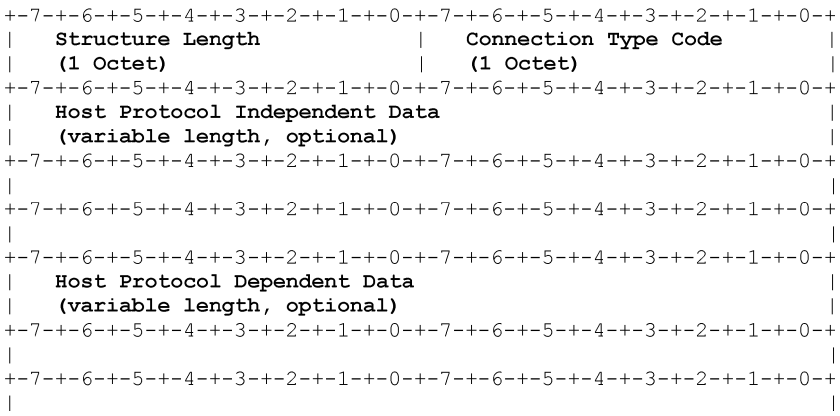


Bild 13 — CRD-Struktur im Binärformat

5.2.7.5.4 DIB (Description Information Block)

5.2.7.5.4.1 Verwendung, Format und allgemeine Anforderungen

Die DIB-Struktur muss von einem KNXnet/IP-Server verwendet werden, um einen spezifischen Block von Geräteinformationen zurückzugeben, wenn er auf einen DESCRIPTION_REQUEST antwortet.

Es müssen mindestens zwei DIB-Strukturen mit Informationen zu den Gerätefunktionen in Bezug auf (1) die Geräte-Hardware und (2) die unterstützten Dienstfamilien zurückgegeben werden.

Es können mehr als zwei DIB-Strukturen in einem einzigen DESCRIPTION_RESPONSE-Frame zurückgegeben werden.

Das erste Oktett jedes DIB muss die Länge der DIB-Struktur enthalten. Das zweite Oktett muss den Typ der DIB-Struktur angeben. Anschließend werden die eigentlichen Daten des DIB angehängt. Die Struktur muss stets eine gerade Anzahl von Oktetten aufweisen, die gegebenenfalls dadurch erreicht wird, dass das letzte Oktett der DIB-Struktur mit 00h aufgefüllt wird.

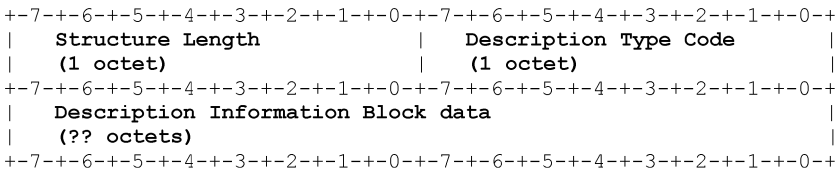


Bild 14 — DIB-Struktur im Binärformat

In Tabelle 4 sind die gültigen Codes für Beschreibungstypen aufgeführt.

Tabelle 3 — Codes für Beschreibungstypen

Beschreibungstyp	Wert	Beschreibung
DEVICE_INFO	01h	Geräteinformationen, z. B. KNX-Medium
SUPP_SVC_FAMILIES	02h	Vom Gerät unterstützte Dienstfamilien
IP_CONFIG	03h	IP-Konfiguration des Gerätes
IP_CUR_CONFIG	04h	Aktuelle IP-Konfiguration des Gerätes
KNX_ADDRESSES	05h	Vom Gerät verwendete/dem Gerät zugewiesene KNX-Adressen

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Beschreibungstyp	Wert	Beschreibung
SECURED_SERVICES	06h	Gesicherte Dienste
TUNNELLING_INFO	07h	Tunnelling-Informationen
EXTENDED_DEVICE_INFO	08h	Erweiterte Geräteinformationen
Reserved	09h-FDh	Für zukünftige Verwendung reserviert
MFR_DATA	FEh	DIB-Struktur für weitere vom Gerätehersteller festgelegte Daten
not used	FFh	nicht verwendet

5.2.7.5.4.2 DIB für Geräteinformationen

Der DIB für Geräteinformationen muss die folgende Struktur aufweisen.

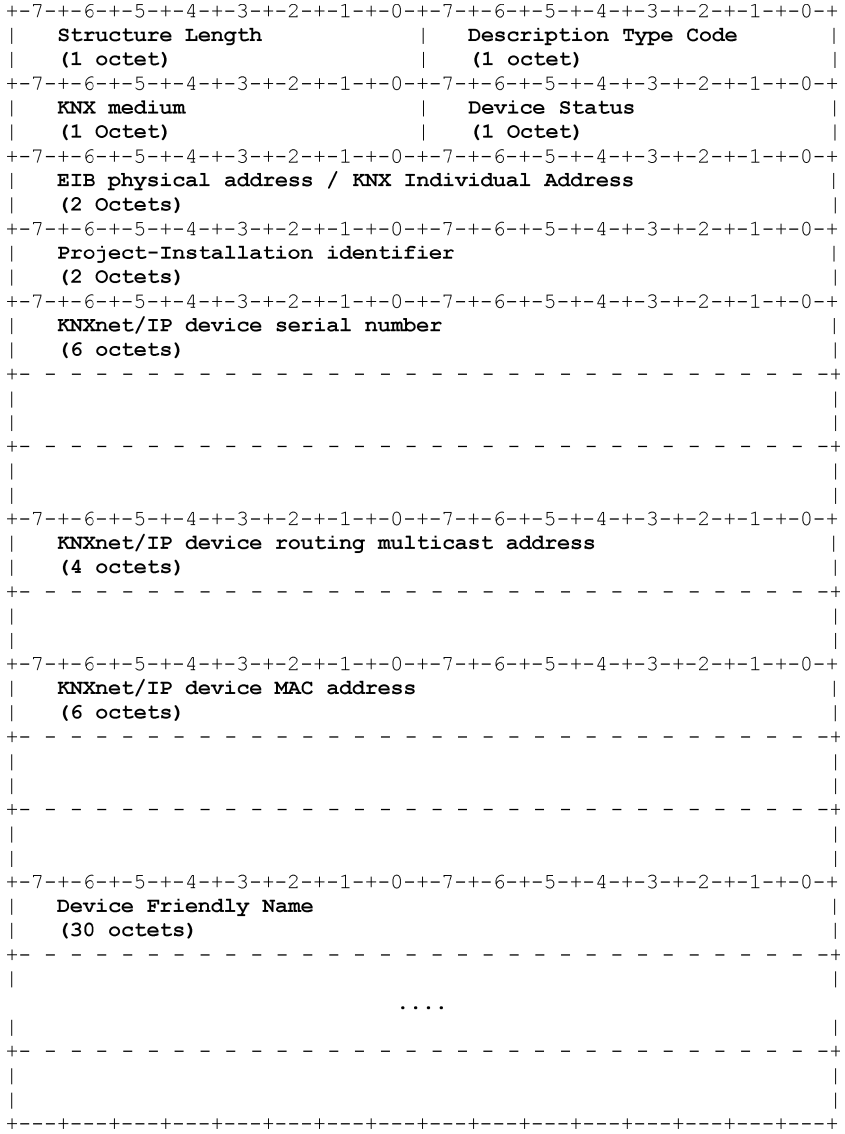


Bild 15 — DIB-Struktur für Geräteinformationen

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

— **KNX-Medium**

Die Codes für das KNX-Medium sind in Tabelle 5 angegeben.

Tabelle 4 — Codes für KNX-Medium

Code für KNX-Medium	KNX-Medium
01h	reserviert
02h	TP1
04h	PL110
08h	reserviert
10h	RF
20h	KNX IP

Es muss genau ein einziges Bit gesetzt werden.

— **Gerätestatus**

Das Gerätestatus-Oktett muss folgendermaßen angegeben werden:

Tabelle 5

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
reserviert	reserviert	reserviert	reserviert	reserviert	reserviert	reserviert	Programmier-modus

— **Projektinstallationskennung**

Die Projektinstallationskennung muss folgendermaßen festgelegt werden:

Tabelle 6

Bit 15-4	Bit 3-0
Projektnummer	Installationsnummer

Die Projektinstallationskennung darf ausschließlich von der ETS zugewiesen werden und muss verwendet werden, um KNXnet/IP-Geräte in einem Projekt mit mehreren KNX-Installationen, d. h. mit mehr als 15 Bereichen mit 12 Linien, oder in einer Umgebung mit mehreren KNX-Projekten eindeutig identifizieren zu können.

— **KNX-Seriennummer des KNXnet/IP-Gerätes**

Die Seriennummer des KNXnet/IP-Gerätes muss der KNX-Seriennummer des KNXnet/IP-Gerätes entsprechen. Diese Information kann zur Identifizierung des Gerätes oder zur Festlegung der individuellen Adresse verwendet werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

— **Routing-Multicast-Adresse des KNXnet/IP-Gerätes**

Die Routing-Multicast-Adresse des KNXnet/IP-Gerätes muss die Multicast-Adresse sein, die von einem KNXnet/IP-Router für KNXnet/IP-Routing verwendet wird. Bei KNXnet/IP-Geräten, die kein KNXnet/IP-Routing implementiert haben, muss dieser Wert auf 0.0.0.0 festgelegt werden. Diese Information kann verwendet werden, wenn KNXnet/IP-Routing-Nachrichten an KNXnet/IP-Router gesendet werden müssen, die nicht die standardmäßige KNXnet/IP-Routing-Multicast-Adresse verwenden, die der Multicast-Adresse der KNXnet/IP-Systemkonfiguration entsprechen muss.

— **MAC-Adresse des KNXnet/IP-Gerätes**

Die MAC-Adresse des KNXnet/IP-Gerätes ist die Ethernet-MAC-Adresse des KNXnet/IP-Gerätes. Diese Information kann zur Identifizierung des Gerätes auf Ethernet gegenüber einem Server verwendet werden, der Netzwerkressourcen, im Speziellen die Unicast-IP-Adresse für das KNXnet/IP-Gerät, zuweist.

— **Anzeigename des Gerätes**

Der Anzeigename des Gerätes kann eine beliebige Zeichenfolge nach ISO/IEC 8859-1 sein, die mit null (00h) endet; sie darf maximal 30 Oktette lang sein. Dieser Name kann zur Identifizierung des Gerätes durch einen Benutzer dienen. Nicht verwendete Oktette werden mit dem Null-Zeichen (00h) aufgefüllt.

5.2.7.5.4.3 DIB für erweiterte Geräteinformationen

Der DIB für erweiterte Geräteinformationen muss die folgende Struktur aufweisen.

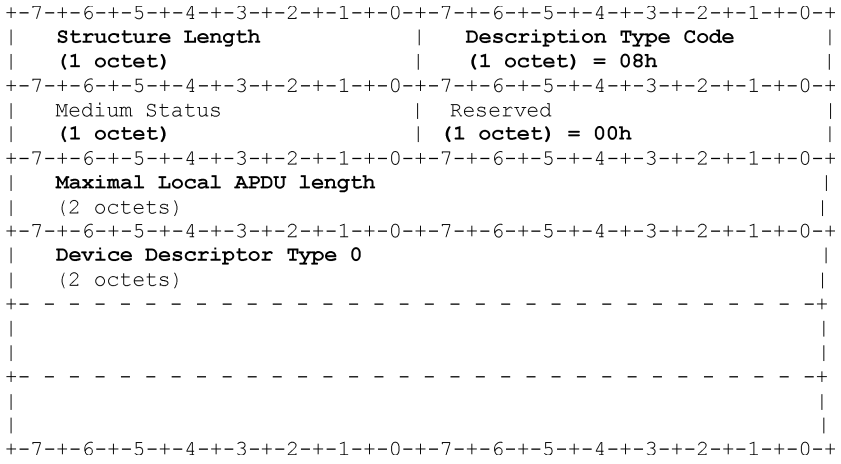


Bild 16 — DIB für erweiterte Geräteinformationen

— **Medienstatus**

Der Inhalt dieses Felds muss dem Inhalt der Eigenschaft PID_MEDIUM_STATUS (PID: 51) im Router-Objekt entsprechen.

— Bei einem IP/TP1-KNXnet/IP-Router (Maske 091Ah) ist dies der Verbindungsstatus der TP1-Verbindung auf der sekundären Seite.

— Bei einem KNXnet/IP-Tunnelling-Server auf TP1 entspricht dies dem Verbindungsstatus der TP1-Verbindung.

— Bei allen anderen KNXnet/IP-Geräten muss das Feld COMMUNICATION_IMPOSSIBLE den Wert FALSE aufweisen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

— **Maximale Länge der lokalen APDU**

Dies ist die maximale APDU-Länge, die von dem KNXnet/IP-Gerät unterstützt wird.

Der Inhalt dieses Felds muss dem Inhalt der Eigenschaft PID_MAX_LOCAL_APDU_LENGTH (PID: 69) im cEMI-Serverobjekt entsprechen.

ANMERKUNG Dieses Feld darf nicht mit PID_MAX_APDU_LENGTH (PID: 58) im Router-Objekt verwechselt werden, das im KNXnet/IP-Router verfügbar ist.

— **Gerätebeschreibungstyp 0**

Dies entspricht dem Gerätebeschreibungstyp 0 (Maskenversion) des KNXnet/IP-Gerätes.

Der Inhalt dieses Feldes muss dem Inhalt der Eigenschaft PID_DEVICE_DESCRIPTOR (PID: 83) im Geräteobjekt entsprechen.

5.2.7.5.4.4 DIB für unterstützte Dienstfamilien

Der DIB für unterstützte Dienstfamilien muss die folgende Struktur aufweisen.

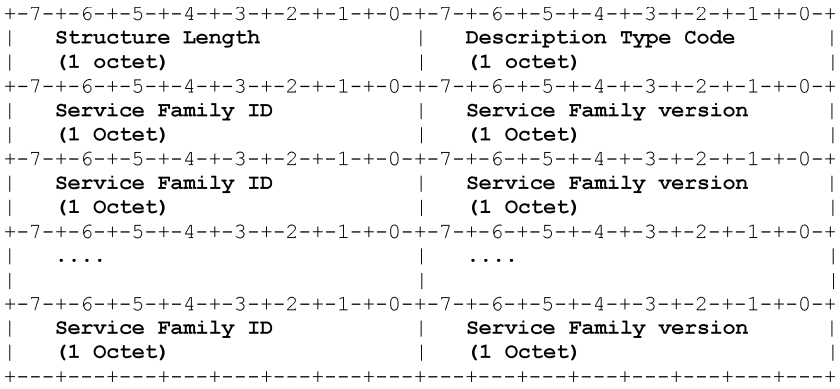


Bild 17 — DIB für unterstützte Dienstfamilien

Die Dienstfamilien-IDs müssen durch das hohe Oktett der Dienstart-ID repräsentiert werden. Eine Liste der Dienstart-IDs ist in Anhang A, Tabelle A.2, enthalten.

Die Version einer Dienstfamilie muss sich auf die Version des entsprechenden KNXnet/IP-Kapiteldokuments beziehen. Diese Version wird nur aktualisiert, wenn das Dokument selbst aktualisiert wird. Jede Version einer Dienstfamilie muss rückwärts kompatibel mit den vorhergehenden Versionen sein, d. h. alle Dienste müssen implementiert und unterstützt werden. Die Dienstfamilienversion entspricht einer ganzen Zahl. Sie stellt nicht die Implementierungsversion des Herstellers dar.

Die *Dienstfamilienversion* muss sich auf die implementierte Version der KNXnet/IP-Dienstfamilie beziehen. Die Versionen der Dienstfamilien sind ausdrücklich in den Spezifikationsdokumenten der Dienste definiert oder werden durch die Definition von Profilen festgelegt.

BEISPIEL Wenn Core v2 unterstützt wird, muss die DIB für unterstützte Dienstfamilien 02h für die Core-Dienstfamilie (02h) einschließen.

Bei Verwendung innerhalb eines SEARCH_RESPONSE- oder DESCRIPTION_RESPONSE-Frames dürfen nur die in Tabelle 7 angegebenen unterstützten Dienstfamilien eingeschlossen werden. Bei Verwendung innerhalb eines SEARCH_RESPONSE_EXTENDED-Frames müssen alle unterstützten Dienstfamilien eingeschlossen werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

Tabelle 7 — Zulässige unterstützte Dienstfamilien

Unterstützte Familie	Code	Zulässig in SEARCH_RESPONSE/ DESCRIPTION_RESPONSE	Zulässig in SEARCH_RESPONSE_EXTENDED
Core	02h	Ja	Ja
Device Management	03h	Ja	Ja
Tunnelling	04h	Ja	Ja
Routing	05h	Ja	Ja
Fernprotokollierung	06h	Ja	Ja
Ferndiagnose und Konfiguration	07h	Ja	Ja
Object-Server	08h	Ja	Ja
Sicherheit	09h	Nein	Ja
Sonstige[4)]		Nein	Ja

5.2.7.5.4.5 DIB für Herstellerdaten

Der DIB für Herstellerdaten weist die folgende Struktur auf.

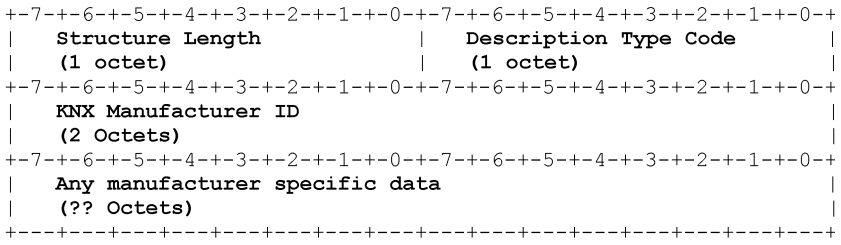


Bild 18 — DIB für Herstellerdaten

Die KNX-Hersteller-ID muss zur eindeutigen Identifizierung des Herstellers hinzugefügt werden. Diese Information ist nicht unbedingt innerhalb der KNXnet/IP-Seriennummer (6 Oktette) verschlüsselt.

Der DIB für Herstellerdaten kann beliebige herstellerspezifische Daten enthalten.

5.2.7.6 Erkennung

5.2.7.6.1 SEARCH_REQUEST

Der SEARCH_REQUEST-Frame muss von einem KNXnet/IP-Client über Multicast an die Erkennungsendpunkte eines empfangenden KNXnet/IP-Servers gesendet werden. Die Kommunikation zu und von dem Erkennungsendpunkt von KNXnet/IP-Geräten ist nur mithilfe von UDP-Datagrammen erlaubt. Da die Kommunikation mit dem Erkennungsendpunkt verbindungs- und zustandslos sein muss, müssen die Adressinformationen des Erkennungsendpunktes des Clients in den KNXnet/IP-Body eingeschlossen werden. Enthält diese Information eine TCP-Adresse, muss der SEARCH_REQUEST-Frame verworfen werden.

4) Platzhalter für mögliche zukünftige Erweiterungen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

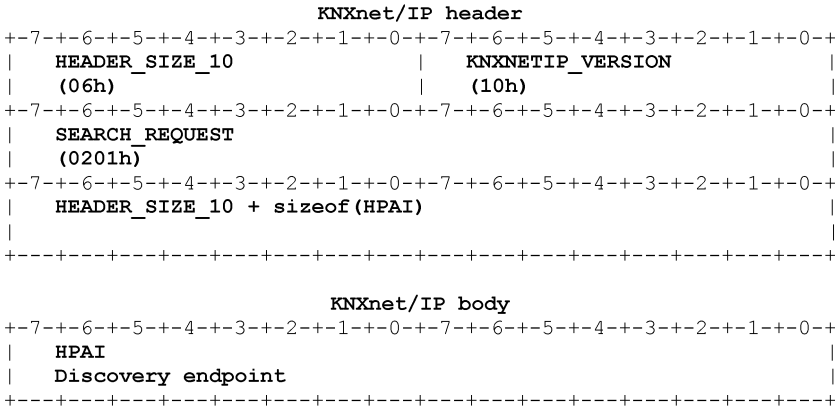


Bild 19 — SEARCH_REQUEST-Frame im Binärformat

5.2.7.6.2 SEARCH_RESPONSE

Der SEARCH_RESPONSE-Frame muss vom KNXnet/IP-Server als Antwort auf einen empfangenen SEARCH_REQUEST-Frame gesendet werden. Er muss an den Erkennungsendpunkt des Clients unter Verwendung der in dem empfangenen Frame enthaltenen HPAI adressiert werden.

Die HPAI des eigenen Kontrollendpunktes des Servers muss zusammen mit der Beschreibung der Geräte-Hardware und der DIB für unterstützte Dienstfamilien, welche die eigentliche Dienstfamilienversion einschließt und nicht auf 01h begrenzt ist, im KNXnet/IP-Body des SEARCH_RESPONSE-Frames übertragen werden.

BEISPIEL Wird Tunnelling v2 unterstützt, muss die Dienstfamilienversion für Tunnelling 02h sein.

Wenn der KNXnet/IP-Server mehrere KNX-Verbindungen unterstützt, muss der Server jeden der eigenen Kontrollendpunkte in einem einzelnen SEARCH_RESPONSE-Frame melden.

KNXnet/IP-Server, die TCP unterstützen, dürfen nur die UDP-Adresse ihres Kontrollendpunkts im SEARCH_RESPONSE-Frame angeben.

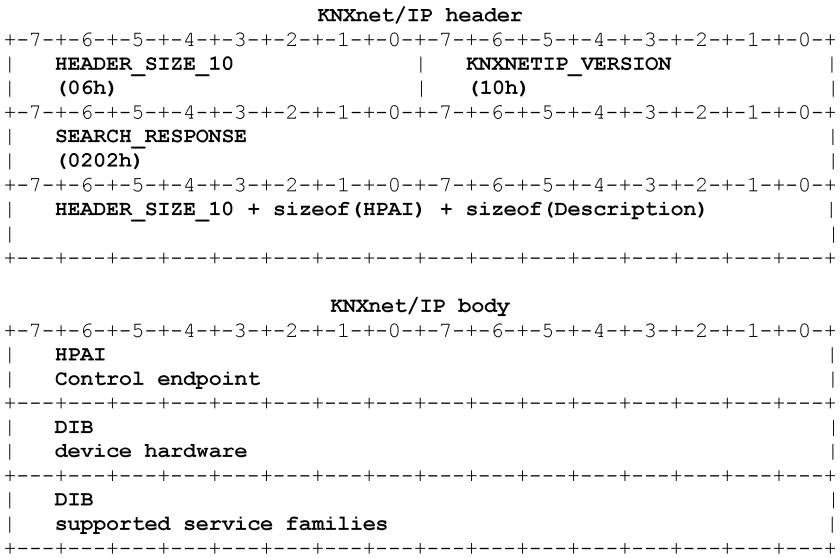


Bild 20 — SEARCH_RESPONSE-Frame im Binärformat

Documents
Document Sharing Hub

Full document details: E DIN EN ISO 22510:2018-06

5.2.7.6.3 SEARCH_REQUEST_EXTENDED

5.2.7.6.3.1 Definition

Der SEARCH_REQUEST_EXTENDED-Frame muss von einem KNXnet/IP-Client entweder an die Erkennungsendpunkte beliebiger empfangender KNXnet/IP-Server oder an den Kontrollendpunkt eines bestimmten KNXnet/IP-Servers übertragen werden.

Die Kommunikation zu und von dem Erkennungsendpunkt von KNXnet/IP-Geräten ist nur mithilfe von UDP-Datagrammen erlaubt. Da die Kommunikation mit dem Erkennungsendpunkt verbindungs- und zustandslos sein muss, müssen die Adressinformationen des Erkennungsendpunktes des KNXnet/IP-Clients in den KNXnet/IP-Body eingeschlossen werden. Enthält diese Information eine TCP-Adresse, muss der SEARCH_REQUEST_EXTENDED-Frame verworfen werden.

Die Kommunikation zu und von dem Kontrollendpunkt von KNXnet/IP-Geräten ist über UDP oder TCP erlaubt.

5.2.7.6.3.2 Binärformat

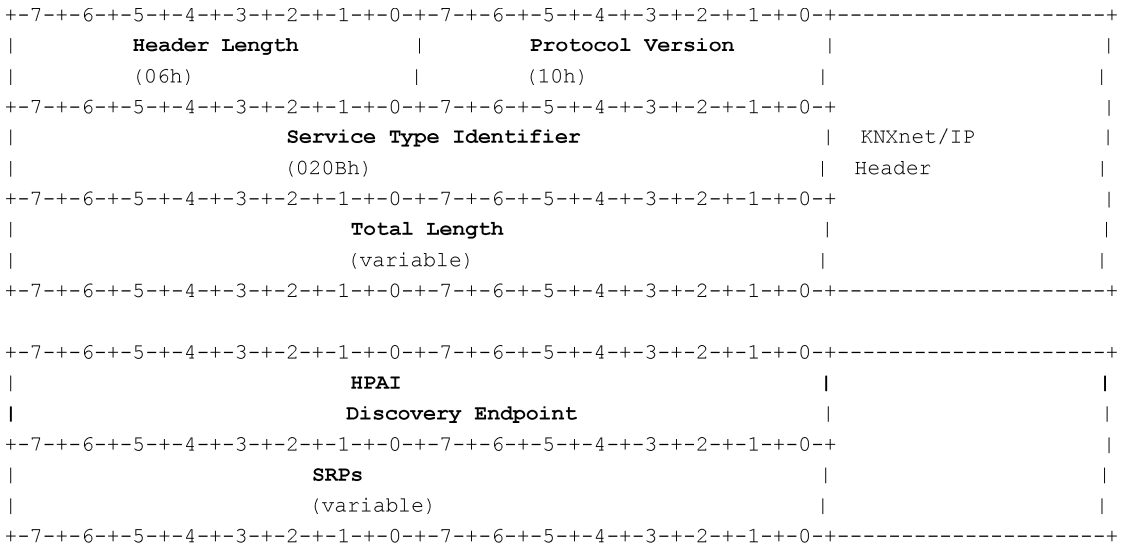


Bild 21 — Binärformat des SEARCH_REQUEST_EXTENDED-Frames

5.2.7.6.3.3 Suchanforderungsparameter (SRP)

5.2.7.6.3.4 Definition

Der KNXnet/IP-Client kann null oder mehr Suchanforderungsparameter-Blöcke (SRP) zur Übertragung zusätzlicher Informationen zur Suche einschließen.

ANMERKUNG Diese Informationen können beispielsweise dazu verwendet werden, die Gruppe der Geräte zu begrenzen, von denen eine Antwort erwartet wird, oder die Art der DIBs zu beeinflussen, an denen der Client interessiert ist.

Ein SRP-Block weist das folgende allgemeine Format auf:

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

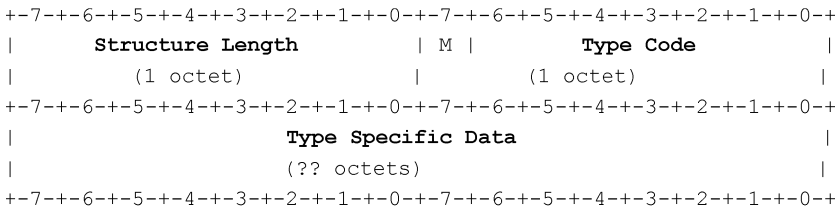


Bild 22 — Binärformat eines Suchanforderungsparameter-Blocks

Der KNXnet/IP-Server muss die SRPs folgendermaßen interpretieren:

— Wenn der KNXnet/IP-Server den SRP unterstützt, muss er die für den jeweiligen SRP-Typ festgelegten Auswahlkriterien anwenden.

— Andernfalls:

  — Wenn das M-Bit (obligatorisch) gesetzt ist, darf der Server auf die Suchanforderung nicht antworten.

  — Wenn das M-Bit (obligatorisch) nicht gesetzt ist, muss der Server diesen SRP ignorieren und so reagieren, als ob dieser SRP nicht vorhanden wäre.

Sind mehrere SRPs vorhanden, ist das erwartete Ergebnis ihrer Kombination in den einzelnen SRP-Typen angegeben. Führt die Bewertung einer der SRPs zu der Entscheidung, nicht auf die Suchanforderung zu antworten, dürfen die folgenden SRPs diese Entscheidung nicht beeinflussen und können daher übersprungen werden.

5.2.7.6.3.5 Überblick über die SRP-Typen

Tabelle 8 — Überblick über die SRP-Typen

SRP-Typ	Code	M/O
Ungültig	00h	Siehe unten
Auswahl nach Programmiermodus	01h	M
Auswahl nach MAC-Adresse	02h	M
Auswahl nach Dienst	03h	M
Anfordern der DIBs	04h	M
Reserviert	05h bis 7Fh	n/a

Der KNXnet/IP-Client darf niemals den ungültigen Code 00h verwenden. Der KNXnet/IP-Server muss einen SRP mit dem ungültigen Code 00h wie jeden anderen unbekannten SRP-Code behandeln, d. h. der Server darf nicht antworten, wenn das M-Bit gesetzt ist, oder der SRP muss ignoriert werden, wenn das M-Bit nicht gesetzt ist.

ANMERKUNG Der ungültige Code 00h wird verwendet, um das Verhalten des Servers bei unbekannten SRPs zu testen.

ANMERKUNG Die Codes 01h und 02h entsprechen der SELECTOR-Codierung im Bereich der Ferndiagnose und Konfiguration von KNXnet/IP. Das bedeutet jedoch nicht, dass diese beiden Codierungen für zusätzliche Selektoren/SRP-Typen identisch sein müssen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5.2.7.6.3.6 SRP-Typ „Auswahl nach Programmiermodus“

Der Client muss diesen SRP einschließen, um anzuzeigen, dass er nur an einer Antwort von KNXnet/IP-Servern interessiert ist, in denen aktuell der Programmiermodus aktiviert ist.

KNXnet/IP-Server, in denen der Programmiermodus nicht aktiviert ist, dürfen nicht auf diese Suchanforderung antworten.

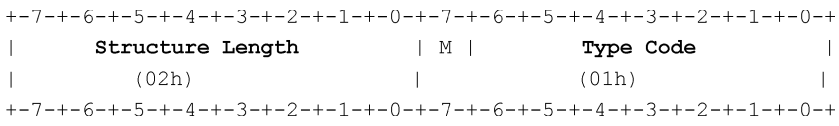


Bild 23 — Binärformat des SRP „Auswahl nach Programmiermodus“

5.2.7.6.3.7 SRP-Typ „Auswahl nach MAC-Adresse“

Der Client muss diesen SRP einschließen, um anzuzeigen, dass er nur an einer Antwort des KNXnet/IP-Servers mit der angegebenen MAC-Adresse interessiert ist.

KNXnet/IP-Server mit anderen MAC-Adressen als der geforderten MAC-Adresse dürfen nicht auf diese Suchanforderung antworten.

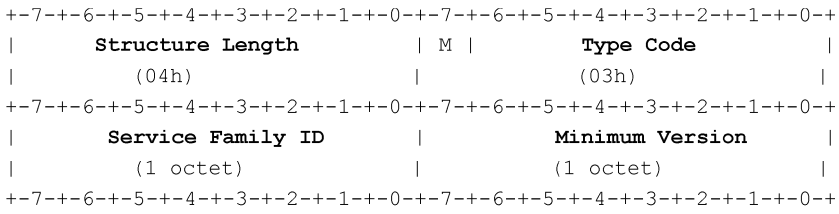


Bild 24 — Binärformat des SRP „Auswahl nach MAC-Adresse“

5.2.7.6.3.8 SRP-Typ „Auswahl nach Dienst“

Der Client muss diesen SRP einschließen, um anzuzeigen, dass er nur an Antworten von KNXnet/IP-Servern interessiert ist, welche die angegebene Dienstfamilie in mindestens der angegebenen Version unterstützen.

KNXnet/IP-Server, welche die angegebene Dienstfamilie nicht oder nur in einer niedrigeren Version unterstützen, dürfen auf diese Suchanforderung nicht antworten.

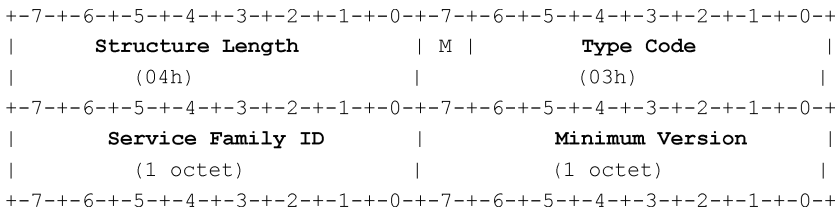


Bild 25 — Binärformat des SRP „Auswahl nach Dienst“

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5.2.7.6.3.9 SRP-Typ „Anfordern der DIBs“

Der Client muss diesen SRP einschließen, um anzuzeigen, dass er an den aufgeführten DIBs interessiert ist. Dieser SRP darf die Entscheidung des KNXnet/IP-Servers, ob er auf die Suchanforderung antwortet oder nicht, nicht beeinflussen.

Ist kein SRP „Anfordern der DIBs“ in der Anforderung vorhanden, muss der KNXnet/IP-Server mindestens den Basissatz der DIBs übermitteln, der aus der DIB für Geräteinformationen, der DIB für erweiterte Geräteinformationen und der DIB für unterstützte Dienste besteht. Der Server darf zusätzlich beliebig viele andere DIBs in die Antwort einschließen.

Ist ein SRP „Anfordern der DIBs“ in der Anforderung vorhanden, muss der KNXnet/IP-Server mindestens den Satz von DIBs übermitteln, die im SRP aufgeführt und vom Server unterstützt werden. Der Server darf zusätzlich beliebig viele andere DIBs in die Antwort einschließen. Der Server muss nicht erkannte oder nicht unterstützte Beschreibungstypen ignorieren.

Dieser SRP hat eine variable Länge. Ist der Client an einer ungeraden Anzahl von DIBs interessiert, muss er einen zusätzlichen Beschreibungstyp 0 hinzufügen, um die Strukturlänge auf einen geraden Wert anzupassen.

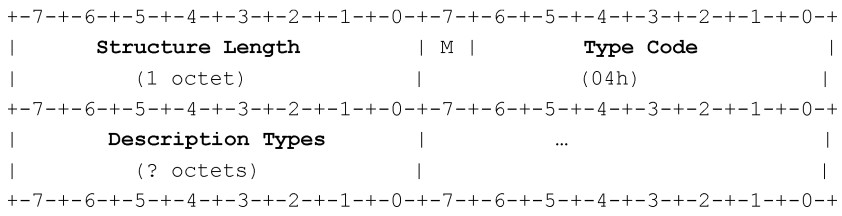


Bild 26 — Binärformat des SRP „Anfordern der DIBs“

5.2.7.6.4 SEARCH_RESPONSE_EXTENDED

5.2.7.6.4.1 Definition

Der KNXnet/IP-Server muss den SEARCH_RESPONSE_EXTENDED-Frame als Antwort auf einen empfangenen SEARCH_REQUEST_EXTENDED-Frame senden. Er muss an den Erkennungsendpunkt des KNXnet/IP-Clients unter Verwendung der in dem empfangenen SEARCH_REQUEST_EXTENDED-Frame enthaltenen HPAI adressiert werden.

Die HPAI des eigenen Kontrollendpunktes des KNXnet/IP-Servers muss zusammen mit der Beschreibung der Geräte-Hardware und der unterstützten Dienstfamilien im KNXnet/IP-Body des SEARCH_RESPONSE_EXTENDED-Frames übertragen werden. Wenn der KNXnet/IP-Server mehrere KNX-Verbindungen unterstützt, muss der KNXnet/IP-Server jeden der eigenen Kontrollendpunkte in einem einzelnen SEARCH_RESPONSE_EXTENDED-Frame melden.

KNXnet/IP-Server, die TCP unterstützen, dürfen nur die UDP-Adresse ihres Kontrollendpunkts im SEARCH_RESPONSE_EXTENDED-Frame angeben.

Der KNXnet/IP-Server kann die DIBs in der Antwort in beliebiger Reihenfolge angeben. Jede DIB darf nur einmal in der Antwort vorhanden sein.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06

5.2.7.6.4.2 Binärformat

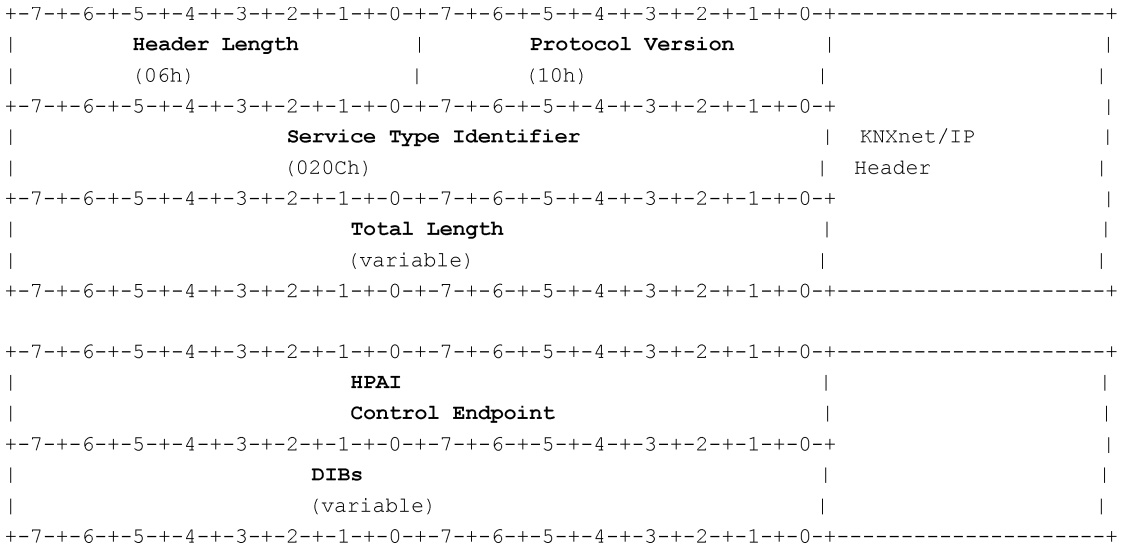


Bild 27 — Binärformat des SEARCH_RESPONSE_EXTENDED-Frames

5.2.7.7 Selbstbeschreibung

5.2.7.7.1 DESCRIPTION_REQUEST

Der DESCRIPTION_REQUEST-Frame muss vom KNXnet/IP-Client an den Kontrollendpunkt des KNXnet/IP-Servers gesendet werden, um eine Selbstbeschreibung des KNXnet/IP-Servergerätes zu erhalten.

Der KNXnet/IP-Body muss Informationen zur Rückkehradresse des Kontrollendpunktes des Clients enthalten.

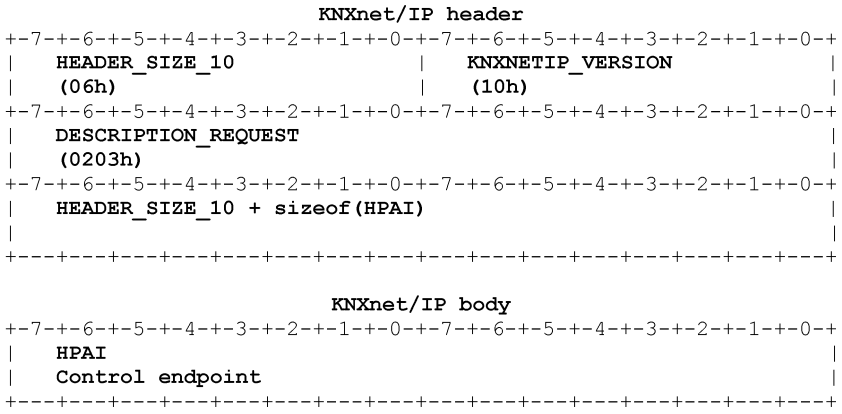


Bild 28 — DESCRIPTION_REQUEST-Frame im Binärformat

5.2.7.7.2 DESCRIPTION_RESPONSE

Der DESCRIPTION_RESPONSE-Frame muss vom KNXnet/IP-Server als Antwort auf einen empfangenen DESCRIPTION_REQUEST-Frame gesendet werden. Er muss an den Kontrollendpunkt des Clients unter Verwendung der in dem empfangenen Frame enthaltenen HPAI adressiert werden.

Die Größe des KNXnet/IP-Bodys variiert in Abhängigkeit von der Anzahl der DIB-Strukturen, die vom Server als Antwort auf den DESCRIPTION_REQUEST des Clients gesendet werden. Die DIB für unterstützte Dienstfamilien muss die eigentliche Dienstfamilienversion einschließen und ist nicht auf 01h begrenzt.

BEISPIEL Wird Tunnelling v2 unterstützt, muss die Dienstfamilienversion für Tunnelling 02h sein.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO 22510:2018-06