PRODUKTHANDBUCH

ABB i-bus® KNX

IPR/S 3.5.1

IP-Router Secure

Inhalt

Seite

ABB i-bus® KNX
Inhalt

1 Allgemein

Der ABB i-bus® IP-Router Secure IPR/S 3.5.1 verbindet den KNX-Bus mit einem Ethernet-Netzwerk. Über das Netzwerk können KNX-Telegramme an andere Geräte gesendet oder von diesen empfangen werden.

Das Gerät unterstützt das KNX Secure Protokoll (KNXnet/IP Security).

1.1 Nutzung des Produkthandbuchs

Das vorliegende Handbuch gibt Ihnen detaillierte technische Informationen über Funktion, Montage und Programmierung des ABB i-bus® KNX-Geräts. Anhand von Beispielen wird der Einsatz erläutert.

Das Handbuch ist in folgende Kapitel unterteilt:

Kapitel 1	Allgemein
Kapitel 2	Gerätetechnik
Kapitel 3	Inbetriebnahme
Kapitel 4	Planung und Anwendung
Kapitel A	Anhang

1.1.1 Hinweise

In diesem Handbuch werden Hinweise und Sicherheitshinweise folgendermaßen dargestellt:

Hinweis
Bedienungserleichterungen, Bedienungstipps

Beispiele
Anwendungsbeispiele, Einbaubeispiele, Programmierbeispiele

Wichtig
Dieser Sicherheitshinweis wird verwendet, sobald die Gefahr einer Funktionsstörung besteht, ohne Schadens- oder Verletzungsrisiko.

Achtung
Dieser Sicherheitshinweis wird verwendet, sobald die Gefahr einer Funktionsstörung besteht, ohne Schadens- oder Verletzungsrisiko.

Gefahr
Dieser Sicherheitshinweis wird verwendet, sobald bei unsachgemäßer Handhabung Gefahr für Leib und Leben besteht.

Gefahr
Dieser Sicherheitshinweis wird verwendet, sobald bei unsachgemäßer Handhabung akute Lebensgefahr besteht.

1.2 Cyber Security (Netzwerksicherheit)

Die Branche ist verstärkt mit Internetsicherheitsrisiken konfrontiert. Um Stabilität, Sicherheit und Robustheit seiner Lösungen zu erhöhen, hat ABB im Rahmen des Produktentwicklungsprozesses offiziell Robustheitsprüfungen zur Internetsicherheit eingeführt.

Die folgenden Hinweise dienen darüber hinaus als Leitfaden und beschreiben Mechanismen, die verwendet werden können um die Sicherheit von KNX Anlagen zu verbessern.

1.3 Verhindern des Zugangs zu den unterschiedlichen Medien

Die Basis jedes Schutz-Konzeptes bildet die sorgfältige Abschottung des Systems gegen unberechtigten Zugriff. Im Falle einer KNX Anlage gilt, dass nur befugte Personen (Installateur, Hausmeister, Nutzer) physischen Zugang zur KNX Anlage haben dürfen. Bei der Planung und Installation müssen für jedes KNX Medium die kritischen Punkte bestmöglich geschützt werden.

Allgemein gilt, dass Anwendungen und Geräte fest installiert werden sollten, um zu verhindern, dass diese leicht entfernt werden und dadurch unbefugte Personen Zugang zur KNX Anlage haben. Unterverteilungen mit KNX Geräten sollten verschlossen sein, oder sich in Räumen befinden, zu denen nur befugte Personen Zugang haben.

1.4 Twisted Pair Verkabelung

- ► Die Leitungsenden des KNX Twisted Pair-Kabels sollten nicht sichtbar sein oder aus der Wand herausstehen, weder im noch außerhalb des Gebäudes.
- ► Wenn verfügbar, sollten die Diebstahlschutzeinrichtungen der Applikationsmodule verwendet werden.
- ► Busleitungen im Außenbereich stellen ein erhöhtes Risiko dar. Der physische Zugang zum KNX Twisted Pair-Kabel sollte hier besonders erschwert werden.
- ► Geräte, die in begrenzt geschützten Bereichen verbaut sind (Außenbereich, Tiefgarage, WC, etc.), können als zusätzlicher Schutz als eigene Linie ausgeführt werden. Durch Aktivierung der Filtertabellen im Linienkoppler (nur KNX) wird verhindert, dass ein Angreifer Zugriff auf die gesamte Anlage erlangen kann.

1.5 IP-Verkabelung innerhalb des Gebäudes

Für die Gebäudeautomation sollte ein getrenntes LAN- oder WLAN-Netzwerk mit eigener Hardware (Router, Switches etc.) verwendet werden.

Unabhängig von der KNX Anlage sind unbedingt die üblichen Sicherheitsmechanismen für IP-Netzwerke anzuwenden. Diese sind beispielsweise:

- MAC-Filter
- Verschlüsselung von Drahtlosnetzwerken
- Verwendung starker Passwörter und Schutz dieser vor unbefugten Personen

Hinweis
Während eines IP-, TCP- oder UDP-Flooding (Zugriff aus dem Internet) ist das Gerät nicht erreichbar. Um diese Reaktion zu vermeiden, ist eine Datenratenlimitierung auf Netzwerkebene einzustellen. Bitte sprechen Sie dazu mit dem Netzwerkadministrator.

1.6 Anbindung an das Internet

Das Gerät ist nicht zur Verwendung im öffentlichen Internet vorgesehen. Aus diesem Grund dürfen keine Ports von Routern Richtung Internet geöffnet werden; dies verhindert, dass die KNX Kommunikation im Internet sichtbar wird.

Ein Zugriff auf eine Anlage aus dem Internet kann auf folgende Weise ermöglicht werden:

- Zugang zu KNX Installationen über VPN Verbindungen: dies setzt jedoch einen Router mit VPN Server-Funktionalität voraus.
- Verwendung von herstellerspezifischen Lösungen oder Visualisierungen, z.B. mit Zugang über https.

1.7 KNXnet/IP Security

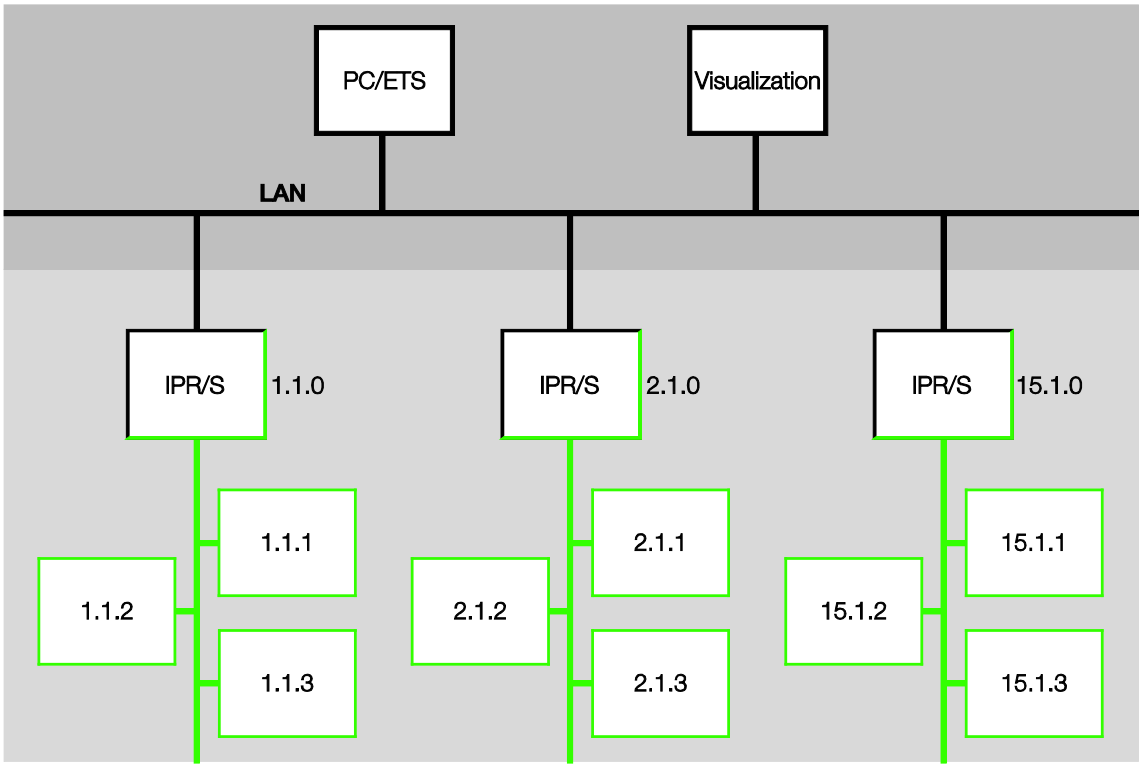
Das Gerät sollte immer im KNX Secure-Modus betrieben werden. So ist sichergestellt, dass die Laufzeitkommunikation auf dem IP-Backbone, die Tunneling Server und die Inbetriebnahme des Gerätes selbst sicher sind.

Siehe auch Kapitel 3.5, KNX Secure.

1.8 Produkt- und Funktionsübersicht

Der ABB i-bus® IP-Router Secure IPR/S 3.5.1 verbindet den KNX-Bus mit einem Ethernet-Netzwerk. Über das Netzwerk können KNX-Telegramme an andere Geräte gesendet oder von diesen empfangen werden.

Das Gerät verwendet zur Kommunikation das KNXnet/IP Protokoll sowie das KNXnet/IP Security Protokoll der KNX Association (Routing und Tunneling).



Der Router verfügt über fünf Tunneling Server, siehe Kapitel 3.4, Verwendung der integrierten Tunneling Server. Diese unterstützen sowohl den Busmonitor- als auch den Gruppenmonitorbetrieb.

Die Tunneling Server können im KNX Secure-Modus betrieben werden.

Alternativ zur KNX-Standardkommunikation (Multicast) können bis zu zehn ABB IP-Router IPR/S 3.x.1 auch über das Unicast-Protokoll miteinander kommunizieren, siehe Kapitel 4.1.2, KNX-Telegramme im Netzwerk. Der KNX Secure-Modus ist in dem Fall nicht verfügbar.

Die Spannungsversorgung kann über PoE (Power over Ethernet) nach IEEE 802.3af Class 1 erfolgen oder über eine Versorgungsspannung.

Für die IP-Router Secure steht das ABB i-bus® Tool zur Verfügung, mit dem die Router im Netzwerk gefunden werden können (IP Discovery) und die Einstellungen für die Unicast-Kommunikation vorgenommen werden können. (Siehe Kapitel 4.2, Das i-bus® Tool.)

Für das Firmware Update steht eine ETS App (ABB KNX Bus Update) zur Verfügung. Sofern der KNX Secure-Modus bei den Geräten nicht aktiviert ist, kann ein Firmware Update auch mit dem i-bus® Tool erfolgen.

Während des Updatevorgangs muss zusätzlich zum IP-Netzwerk (LAN) auch der KNX-Bus (TP) angeschlossen sein, damit die KNX-Parameter korrekt wiederhergestellt werden können. Andernfalls schlägt der Updatevorgang fehl.

Es muss sichergestellt werden, dass während des Updatevorgangs kein Spannungsausfall (KNX oder IP) auftritt, da ansonsten das Gerät zerstört werden kann.

Das Gerät unterstützt die KNX-Standardfunktion "Überwachung auf Busspannungsausfall". Dies ist eine Netzwerk-Management-Funktion, die z.B. von Visualisierungen verwendet wird (siehe Kapitel 1.8.1, Überwachung auf Busspannungsausfall).

1.8.1 Überwachung auf Busspannungsausfall

Der IP-Router Secure überwacht den KNX TP-Bus auf Spannungsausfall. Bei einer Zustandsänderung der Busspannung wird ein Broadcastbefehl vom Typ "NetworkParameterWrite" auf das IP-Netzwerk gesendet.

Folgende Werte werden gesendet:

- Busspannungsausfall: "00063301" (hex)
- Busspannungswiederkehr: "00063300" (hex)

Diese Telegramme können z.B. von einer Visualisierung ausgewertet werden.

Typ	Info	Bedeutung
NetworkParameterWrite	00 06 33 01	Busspannungsausfall TP1
NetworkParameterWrite	00 06 33 00	Busspannungswiederkehr TP1

1.8.2 Übersicht Versionen

Gerät	IPR/S 3.1.1	IPR/S 3.5.1
Applikation	**IP-Router /2.0**	**IP-Router Secure/1.0**
ETS	**ETS 4/5**	**ETS 5**
Eigenschaften *IP-Router*		
Anzahl Tunneling Server	5	5
Anzahl Unicast-Verbindungen	10	10
Überwachung auf Busspannungsausfall (siehe Kapitel 1.8.1, Überwachung auf Busspannungsausfall)	■	■
Filterung Gruppentelegramme Hauptgruppe 0…31	■	■
IP-Discovery (i-bus® Tool)	■	■
Firmware Update mit i-bus® Tool	■	■*
Firmware Update mit KNX Bus Update App	-	■
Parametrierung Unicast (i-bus® Tool)	■	■*
Power over Ethernet	■	■
KNX Secure	-	■

* Nur, wenn Gerät nicht im KNX Secure-Modus betrieben wird

2 Gerätetechnik

2CDC071007F0017

IPR/S 3.5.1

Der IP-Router Secure 3.5.1 bildet die Schnittstelle zwischen KNX-Installationen und IP-Netzwerken. Er kann als Linien- oder Bereichskoppler eingesetzt werden und dabei das lokale Netzwerk (LAN) für den Austausch von Telegrammen zwischen den Linien/Bereichen nutzen.

Mit der ETS können KNX-Geräte über das LAN programmiert werden (es stehen 5 Tunneling Server zur Verfügung). Das Gerät verwendet das KNXnet/IP-Protokoll bzw. das KNXnet/IP Security Protokoll der KNX-Association (Routing und Tunneling).

Alternativ kann das Gerät über Unicast kommunizieren.

Die Stromversorgung erfolgt über 12 bis 30 V DC oder PoE (Power over Ethernet) nach IEEE 802.3af Class 1.

2.1 Technische Daten

Versorgung	Versorgungsspannung U_s	12…30 V DC (+10 % / -15 %) oder PoE (IEEE 802.3af Class 1)
	Verlustleistung	Maximal 1,8 W
	Stromaufnahme Versorgungsspannung	Maximal 120 mA bei 12 V
	Nennspannung U_n	12 V DC
	Stromaufnahme KNX	< 10 mA
Anschlüsse	KNX	Busanschlussklemme
	Betriebsspannung	Steckklemme
	LAN	RJ45-Buchse für 10/100BaseT, IEEE 802.3 Netzwerke, AutoSensing
Bedien- und Anzeigeelemente	LED rot und Taste	Vergabe der physikalischen Adresse
	LED grün "On"	Anzeige Betriebsbereitschaft
	LED gelb "LAN/Link"	Anzeige Netzwerkverbindung
	LED gelb "Telegram"	Anzeige KNX-Telegrammverkehr
Schutzart	IP 20	Nach DIN EN 60 529
Schutzklasse	II	Nach DIN EN 61 140
Isolationskategorie	Überspannungskategorie	III nach DIN EN 60 664-1
	Verschmutzungsgrad	2 nach DIN EN 60 664-1

KNX-Sicherheitskleinspannung	SELV 30 V DC	
Temperaturbereich	Betrieb	-5 °C…+45 °C
	Lagerung	-25 °C…+55 °C
	Transport	-25 °C…+70 °C
Umgebungsbedingung	maximale Luftfeuchte	95 %, keine Betauung zulässig
	Luftdruck	Atmosphäre bis 2.000 m
Design	Reiheneinbaugerät (REG)	Modulares Installationsgerät, pro *M*
	Abmessungen	90 x 36 x 63,5 mm (H x B x T)
	Einbaubreite	2 Module à 18 mm
Montage	Auf Tragschiene 35 mm	Nach DIN EN 60 715
Einbaulage	Beliebig	
Gewicht	0,1 kg	
Gehäuse, Farbe	Kunststoff, halogenfrei, grau	
Approbation	KNX nach DIN EN 50491 und EN 60 669-2-5	
CE-Zeichen	gemäß EMV- und Niederspannungsrichtlinien	

Gerätetyp	Applikation	maximale Anzahl Kommunikationsobjekte	maximale Anzahl Gruppenadressen	maximale Anzahl Zuordnungen
IPR/S 3.5.1	IP-Router Secure/…*	0	0	0

* … = aktuelle Versionsnummer der Applikation. Bitte beachten Sie hierzu die Softwareinformationen auf unserer Homepage.

Hinweis

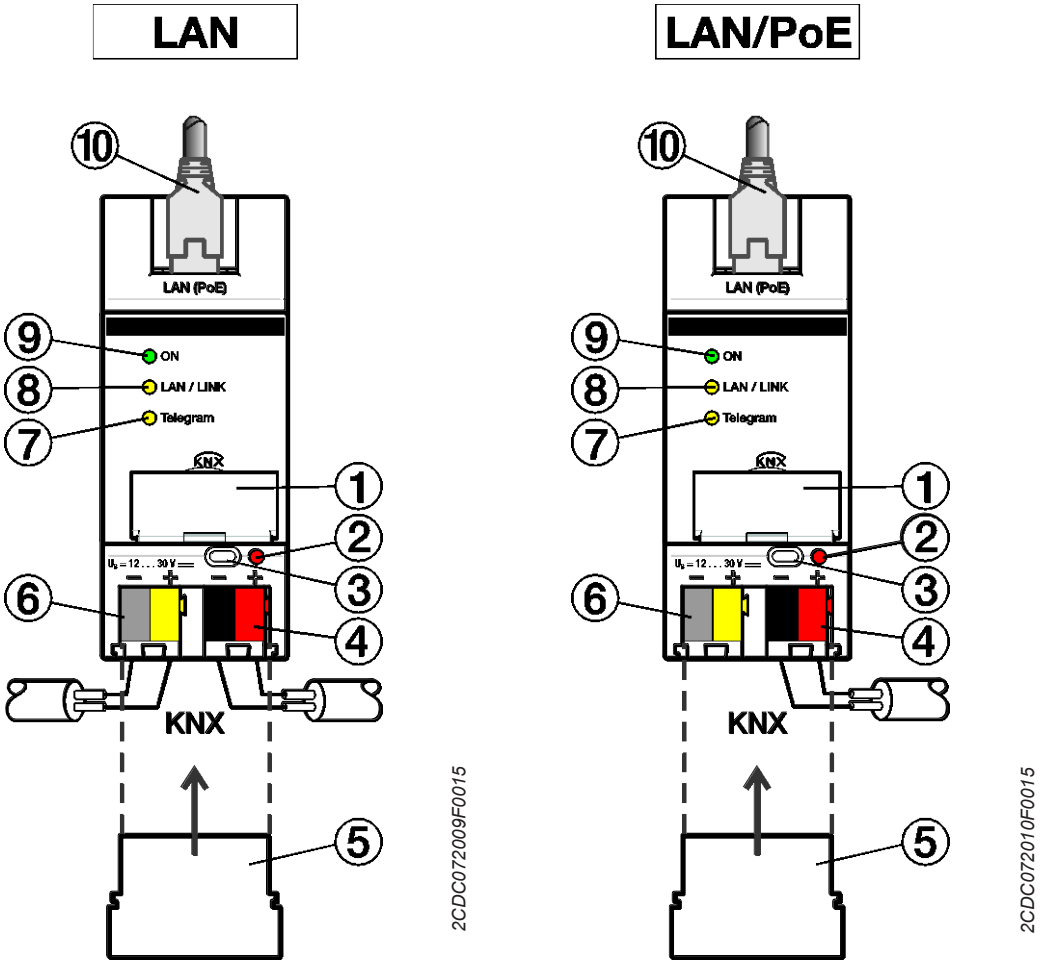
Für die Programmierung sind die ETS 5 und die aktuelle Applikation des Gerätes erforderlich.

Soll das Gerät im KNX Secure-Modus betrieben werden, ist zusätzlich der seitlich auf dem Gerät aufgebrachte Inbetriebnahmeschlüssel (FDSK, Siehe Kapitel 3.5, KNX Secure) erforderlich.

Die aktuelle Applikation finden Sie mit der entsprechenden Softwareinformation zum Download im Internet unter *www.abb.com/knx.* Nach dem Import in die ETS liegt die Applikation im Fenster *Kataloge unter Hersteller/ABB/Systemgeräte/Koppler* ab.

Das Gerät unterstützt nicht die Verschließfunktion eines KNX-Geräts in der ETS. Falls Sie den Zugriff auf alle Geräte des Projekts durch einen *BCU-Schlüssel* sperren, hat es auf dieses Gerät keine Auswirkung. Es kann weiterhin ausgelesen und programmiert werden.
Ausnahme: Wenn der KNX Secure-Modus aktiviert ist, kann das Gerät nicht mehr mit einer anderen ETS programmiert werden.

2.2 Anschlussbild



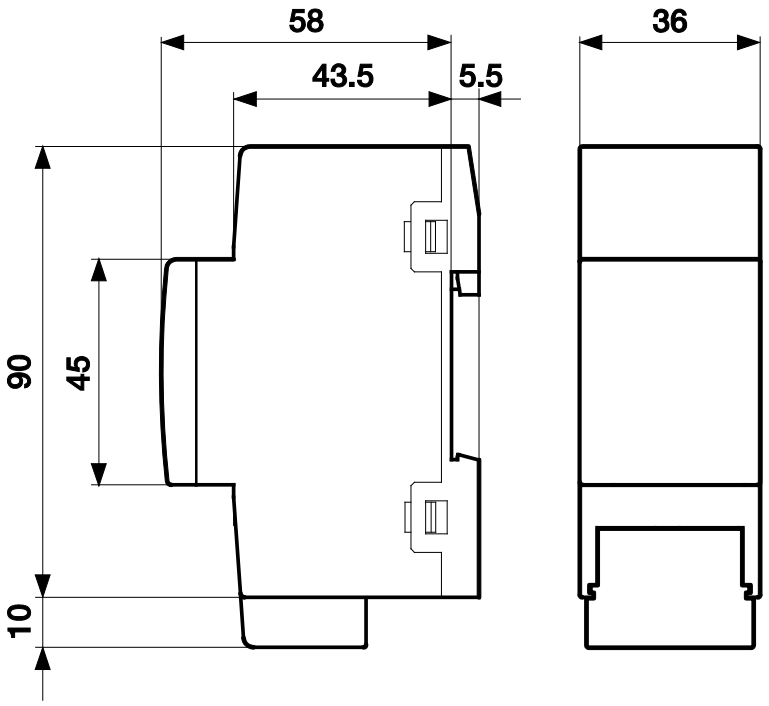
IPR/S 3.5.1

Legende

1	Schildträger	**6**	Anschluss Versorgungsspannung U_S
2	LED *Programmieren*	**7**	LED Telegramm
3	Taste *Programmieren*	**8**	LED LAN/LINK
4	Anschluss KNX	**9**	LED ON
5	Abdeckkappe	**10**	Anschluss LAN bzw. LAN/PoE

Hinweis
Es ist auch möglich, den Router über den unverdrosselten Spannungsausgang einer ABB KNX Spannungsversorgung (Typ SV/S) zu versorgen.

2.3 Maßbild



2CDC072011F0015

IPR/S 3.5.1

2.4 Montage und Installation

Das Gerät ist ein Reiheneinbaugerät zum Einbau in Verteilern zur Schnellbefestigung auf 35-mm-Tragschienen nach DIN EN 60 715.

Das Gerät kann in jeder Einbaulage montiert werden.

Die Verbindung zum Bus erfolgt über die mitgelieferte Busanschlussklemme. Die Klemmenbezeichnung befindet sich auf dem Gehäuse.

Das Gerät ist betriebsbereit, nachdem die Busspannung und die Versorgungsspannung angelegt wurden.

Die Zugänglichkeit des Geräts zum Betreiben, Prüfen, Besichtigen, Warten und Reparieren muss gemäß DIN VDE 0100-520 sichergestellt sein.

2.4.1 Inbetriebnahmevoraussetzung

Um das Gerät in Betrieb zu nehmen, werden ein PC mit der ETS 5 in der aktuellsten Version, sowie eine Versorgungsspannung von 12 bis 30 V DC benötigt. Alternativ kann die Versorgung über PoE (Power over Ethernet) nach IEEE 802.3af Class 1 erfolgen.

Mit dem Anlegen der Busspannung und der Versorgungsspannung ist das Gerät betriebsbereit.

Montage und Inbetriebnahme dürfen nur von Elektrofachkräften ausgeführt werden. Bei der Planung und Errichtung von elektrischen Anlagen, sowie von sicherheitstechnischen Anlagen für Einbruch- und Branderkennung, sind die einschlägigen Normen, Richtlinien, Vorschriften und Bestimmungen des jeweiligen Landes zu beachten.

- Gerät bei Transport, Lagerung und im Betrieb vor Feuchtigkeit, Schmutz und Beschädigung schützen!
- Gerät nur innerhalb der spezifizierten technischen Daten betreiben!
- Gerät nur im geschlossenen Gehäuse (Verteiler) betreiben!
- Vor Montagearbeiten ist das Gerät spannungsfrei zu schalten.

Gefahr

Um gefährliche Berührungsspannung durch Rückspeisung aus unterschiedlichen Außenleitern zu vermeiden, muss bei einer Erweiterung oder Änderung des elektrischen Anschlusses eine allpolige Abschaltung vorgenommen werden.

2.4.2 Auslieferungszustand

Das Gerät wird mit der physikalischen Adresse 15.15.0 ausgeliefert.

Alle physikalischen Adressen der Tunneling-Verbindungen stehen im Auslieferungszustand auf 15.15.100, d.h. nach außen ist nur ein Tunnel sichtbar. Erst nach dem ersten Download werden die in der ETS eingestellen Adressen der Tunneling-Verbindungen übernommen.

Die IP-Adresse ist auf automatische Vergabe (DHCP/AutoIP) eingestellt.

Hinweis

Das Gerät wird ab Werk mit der Option *weiterleiten* ausgeliefert. Das entspricht nicht der Standardeinstellung in der Applikation, erleichtert aber die Inbetriebnahme. Siehe Kapitel 3.2.1, Parameterfenster KNX -> LAN.
Nach dem ersten Download wird dann die parametrierte Einstellung übernommen.

2.4.3 Vergabe der physikalischen Adresse

In der ETS erfolgt die Vergabe und Programmierung der physikalischen Adressen und Parameter.

Das Gerät besitzt zur Vergabe der physikalischen Adresse eine Taste *Programmieren*. Nachdem die Taste betätigt wurde, leuchtet die rote LED *Programmieren* auf. Sie erlischt, sobald die ETS die physikalische Adresse vergeben hat oder die Taste *Programmieren* erneut betätigt wurde.

2.4.4 Downloadverhalten

Das Gerät kann auf unterschiedliche Arten programmiert werden: Über einen der integrierten Tunneling Server, über lokalen Download, über KNXnet/IP Routing oder über eine weitere Programmierschnittstelle (USB oder IP).

Hinweis
Wird für die Programmierung eines KNX Secure Gerätes eine USB Schnittstelle verwendet, muss diese „Long Frames“ unterstützen. Geeignet ist z.B. die USB-Schnittstelle USB/S 1.2 von ABB.

Damit das Gerät programmiert werden kann, muss eine Verbindung zum KNX TP (Twisted Pair) bestehen.

Nach erfolgtem Download startet das Gerät neu und schließt alle offenen Tunneling-Verbindungen. Sofern beim Download die IP-Adresse des Gerätes geändert wurde, müssen die Tunneling-Verbindungen manuell in den Tunneling Clients neu konfiguriert werden. Tunneling Clients stellen die Verbindung zum Server über die IP Adresse her.

Die Übernahme der mit der ETS parametrierten Daten erfolgt ca. 30-60 Sekunden nach dem Download.

2.4.5 Entladen des Gerätes und Rücksetzen auf Werkseinstellungen

Das Gerät kann auf Werkseinstellungen zurückgesetzt werden. Da es sich um ein Secure Gerät handelt, ist folgendes zu beachten:

Im KNX Secure-Modus-Betrieb kann das Gerät über die ETS nur dann zurückgesetzt werden, wenn die ETS das Projekt verwendet, mit dem das Gerät parametriert wurde, bzw. wenn im Projekt der Inbetriebnahmeschlüssel vorhanden ist.

Über einen Rechtsklick auf das Gerät in der ETS kann das Gerät entladen werden.

Option: Applikation entladen

- Die IP-Adresse und IP-Konfiguration bleiben erhalten
- Die Unicast-Konfiguration bleibt erhalten, sofern vorhanden
- Die Passwörter und IP Adressen der Tunnelingserver werden gelöscht
- Der Schlüssel für die Multicastkommunikation („Backbone Key“) bleibt
- Der von der ETS vergebene Tool Key bleibt erhalten, d.h.für die erneute Programmierung ist der FDSK nicht erforderlich.
- Die physikalische Adresse bleibt erhalten

Option: Physikalische Adresse und Applikation entladen

- Das Gerät wird auf Werkszustand zurück gesetzt
- Für die erneute Inbetriebnahme ist der FDSK notwendig, sofern er nicht von der ursprünglichen Inbetriebnahme noch im ETS Projekt vorhanden ist.

Das Zurücksetzen auf Werkseinstellungen kann auch direkt am Gerät vorgenommen werden. Dies stellt kein Sicherheitsrisiko dar, da das Gerät anschließend nicht mehr Teil der Anlage ist.

- Drücken der Programmiertaste bei nicht verbundenem KNX Bus
- Programmiertaste gedrückt halten und Busklemme aufstecken. Die Programmier-LED blinkt (2 Hz).
- Taste mindestens 5s gedrückt halten und dann loslassen. Die Programmier-LED erlischt, das Gerät startet neu mit Werkseinstellungen.

Verbindet sich nach dem Rücksetzen die ETS mit dem Gerät und der FDSK Schlüssel des Gerätes ist der ETS noch bekannt, kann der Router erneut programmiert werden. Die ETS meldet in dem Fall, dass das Gerät zurückgesetzt wurde.

Weitere Hinweise zum FDSK (Factory Default Setup Key) siehe Kapitel 3.5, KNX Secure.

.

2.4.6 Reinigen

Das Gerät ist vor dem Reinigen spannungsfrei zu schalten. Verschmutzte Geräte können mit einem trockenen oder leicht mit Seifenlauge angefeuchteten Tuch gereinigt werden. Auf keinen Fall dürfen ätzende Mittel oder Lösungsmittel verwendet werden.

2.4.7 Wartung

Das Gerät ist wartungsfrei. Bei Schäden, z.B. durch Transport und/oder Lagerung, dürfen keine Reparaturen vorgenommen werden.

2.5 Beschreibung der Ein- und Ausgänge

Versorgungsspannungseingang 12 bis 30 V DC

Am Eingang für die Versorgungsspannung darf nur eine Gleichspannung von 12 bis 30 V angeschlossen werden. Wir empfehlen die Verwendung der Netzteile NT/S aus unserem Sortiment.

Es ist auch möglich, den Router über den unverdrosselten Spannungsausgang einer ABB KNX Spannungsversorgung (Typ SV/S) zu versorgen.

Achtung
Die Versorgungsspannung muss 12 bis 30 V DC betragen, oder das Gerät wird über PoE (Power over Ethernet) nach IEEE 802.3af Class 1 versorgt. Bei Anschluss von 230 V kann das Gerät zerstört werden!

KNX-Anschluss

Zum Anschluss an den KNX-Bus wird die mitgelieferte Busanschlussklemme verwendet.

Hinweis
Zur Programmierung ist die ETS 5 in der aktuellsten Version erforderlich.

LAN-Anschluss

Die Netzwerkanbindung erfolgt über eine Ethernet-RJ45-Schnittstelle für LAN-Netzwerke.
Die Netzwerkschnittstelle kann mit einer Übertragungsgeschwindigkeit von 10/100 MBit/s betrieben werden. Die Netzwerkaktivität wird durch die LED LAN/LINK auf der Gehäusefrontseite angezeigt.

2.6 Bedienelemente

Es befinden sich keine Bedienelemente am IP-Router Secure.

2.7 Anzeigeelemente

Auf der Frontseite des IPR/S befinden sich drei LEDs zur Anzeige:

ON LAN/LINK Telegram

ON

- Die LED leuchtet wenige Sekunden nach Zuschalten der Versorgungsspannung.
- Die LED leuchtet nach dem Zuschalten der Versorgungsspannung zunächst dauerhaft. Nach ca. 40 Sekunden fängt die LED an zu blinken, bis der Startvorgang vollständig abgeschlossen ist und die LED wieder dauerhaft leuchtet. Dies kann je nach Größe der Filtertabelle 5 bis 60 Sekunden dauern.

LAN/LINK

- Die LED leuchtet, wenn die Versorgungsspannung vorhanden ist und der Router an ein Ethernet-Netzwerk angeschlossen ist.
- Die LED blinkt, wenn das Gerät Aktivität auf dem Netzwerk erkennt, z.B. wenn Daten ausgetauscht werden.

Telegram

- Die LED leuchtet, wenn der Router an ein TP-Netzwerk angeschlossen ist und der Startvorgang (siehe LED "On") vollständig abgeschlossen ist.
- Die LED blinkt, wenn das Gerät Aktivität auf der KNX-Sublinie TP1 (Twisted Pair 1) erkennt, z.B. wenn Daten ausgetauscht werden.

3 Inbetriebnahme

Die Parametrierung des IPR/S erfolgt mit der Applikation und der Engineering Tool Software (ETS).

Die Applikation ist unter *Hersteller/ABB/Systemgeräte/Koppler* zu finden.

Für die Parametrierung wird ein PC oder Laptop mit der ETS und eine Anbindung an den KNX Bus benötigt.

3.1 Überblick

Die Parametrierung des IPR/S erfolgt mit der Engineering Tool Software (ETS 5 in der aktuellsten Version).

Einige Funktionen (Unicast) werden über ein separates Tool (i-bus® Tool) parametriert.

3.2 Parameter

Dieses Kapitel beschreibt die Parameter des IP-Router Secure an Hand der Parameterfenster.

Die Parameterfenster sind dynamisch aufgebaut, so dass je nach Parametrierung und Funktion der Ausgänge weitere Parameter oder ganze Parameterfenster freigegeben werden.

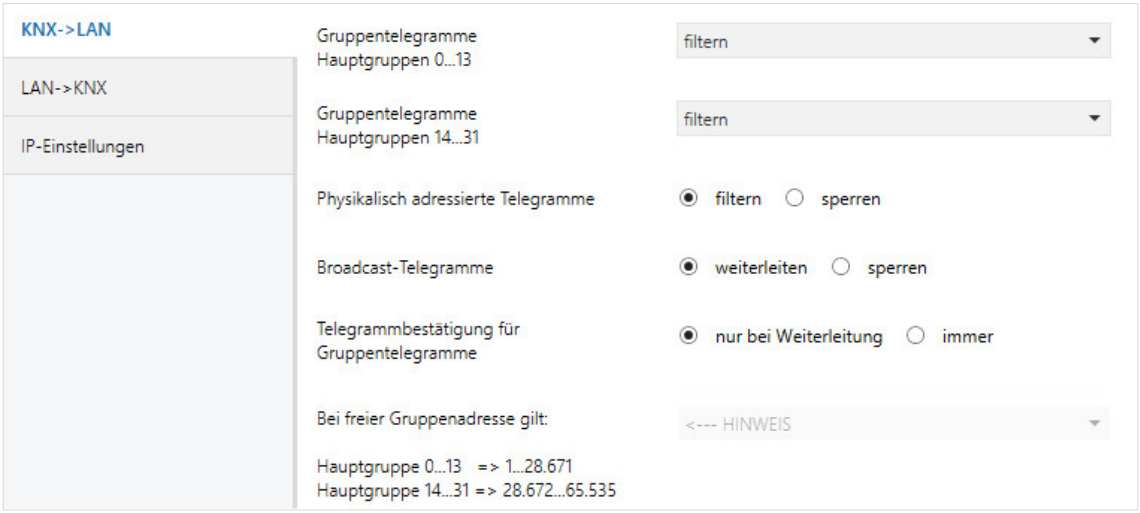
Die Defaultwerte der Parameter sind unterstrichen dargestellt, z.B.:

Optionen: ja
<u>nein</u>

3.2.1 Parameterfenster *KNX -> LAN*

Im Parameterfenster KNX -> LAN kann die Bearbeitung der Telegramme vom KNX-System zum LAN-Netzwerk festgelegt werden.

Hinweis
Das Gerät wird ab Werk mit der Option *weiterleiten* ausgeliefert. Das entspricht nicht der Standardeinstellung in der Applikation, erleichtert aber die Inbetriebnahme. Nach dem ersten Download wird dann die parametrierte Einstellung übernommen.



Gruppentelegramme Hauptgruppe 0…13

Optionen: filtern
weiterleiten
sperren

Dieser Parameter legt fest, ob Telegramme mit Gruppenadressen der Hauptgruppen 0 bis 13 gefiltert, weitergeleitet oder gesperrt werden sollen.

- *filtern:* Die Telegramme mit Gruppenadressen der Hauptgruppen 0 bis 13 vom KNX zum LAN werden gemäß der Filtertabelle, welche von der ETS automatisch berechnet wird, gefiltert.
- *weiterleiten:* Alle Gruppentelegramme der Hauptgruppen 0 bis 13 werden weitergeleitet, ohne Berücksichtigung der Filtertabelle.

Wichtig
Diese Einstellung ist nur für die Inbetriebnahme und zur Diagnose sinnvoll. Im Normalbetrieb sollte diese nicht verwendet werden. Da durch diese Einstellung die KNX-Linien überlastet werden können, kann es zu einem Telegrammverlust kommen.

- *sperren:* Alle Gruppentelegramme der Hauptgruppen 0 bis 13 werden gesperrt, ohne Berücksichtigung der Filtertabelle.

Gruppentelegramme Hauptgruppe 14…31

Optionen: filtern
weiterleiten
sperren

Dieser Parameter legt fest, ob Telegramme mit Gruppenadressen der Hauptgruppen 14…31 gefiltert, weitergeleitet oder gesperrt werden sollen.

- *filtern:* Die Telegramme mit Gruppenadressen der Hauptgruppen 14…31 vom KNX zum LAN werden gemäß der Filtertabelle, welche von der ETS automatisch berechnet wird, gefiltert.
- *weiterleiten:* Alle Gruppentelegramme der Hauptgruppen 14…31 werden weitergeleitet, ohne Berücksichtigung der Filtertabelle.

Wichtig
Diese Einstellung ist nur für die Inbetriebnahme und zur Diagnose sinnvoll. Im Normalbetrieb sollte diese nicht verwendet werden. Da durch diese Einstellung die KNX-Linien überlastet werden können, kann es zu einem Telegrammverlust kommen.

- *sperren:* Alle Gruppentelegramme der Hauptgruppen 14…31 werden gesperrt, ohne Berücksichtigung der Filtertabelle.

Physikalisch adressierte Telegramme

Optionen: filtern
sperren

Dieser Parameter legt fest, ob physikalisch adressierte Telegramme gefiltert oder gesperrt werden.

- *filtern:* Es werden nur die Telegramme vom KNX zum LAN übertragen, welche die Linie des IPR/S zum LAN verlassen sollen.
- *sperren:* Physikalisch adressierte Telegramme werden nicht vom IPR/S bearbeitet. Bei dieser Einstellung ist es nicht möglich, aus der Linie unterhalb des IPR/S heraus in eine andere Linie hinein physikalisch adressierte Telegramme zu schicken, z.B. während der Programmierung.

Broadcast-Telegramme

Optionen: weiterleiten
sperren

Dieser Parameter legt fest, ob Broadcast-Telegramme weitergeleitet oder gesperrt werden.

- *weiterleiten:* Broadcast-Telegramme werden weitergeleitet.
- *sperren:* Broadcast-Telegramme werden nicht vom IPR/S bearbeitet. Bei dieser Einstellung ist es nicht möglich, aus der Linie unterhalb des IPR/S heraus in eine andere Linie hinein Broadcast-Telegramme zu schicken, z.B. während der Programmierung.

Der Parameter *Broadcast-Telegramme* gilt auch für „System Broadcast-Telegramme“. Details siehe Kapitel 4.1.4, System Broadcast.

Telegrammbestätigung für Gruppentelegramme

Optionen: nur bei Weiterleitung
immer

Dieser Parameter legt fest, ob der IP-Router Secure Gruppentelegramme mit einem Telegramm bestätigen soll.

- *nur bei Weiterleitung:* Die Gruppentelegramme werden nur bestätigt (ACK senden), wenn sie vom IP-Router Secure auch auf das LAN weitergeleitet werden. Damit werden nur Telegramme bestätigt, die auch in der Filtertabelle des IPR/S eingetragen sind.
- *immer:* Alle Gruppentelegramme auf dem KNX werden durch den IPR/S bestätigt.

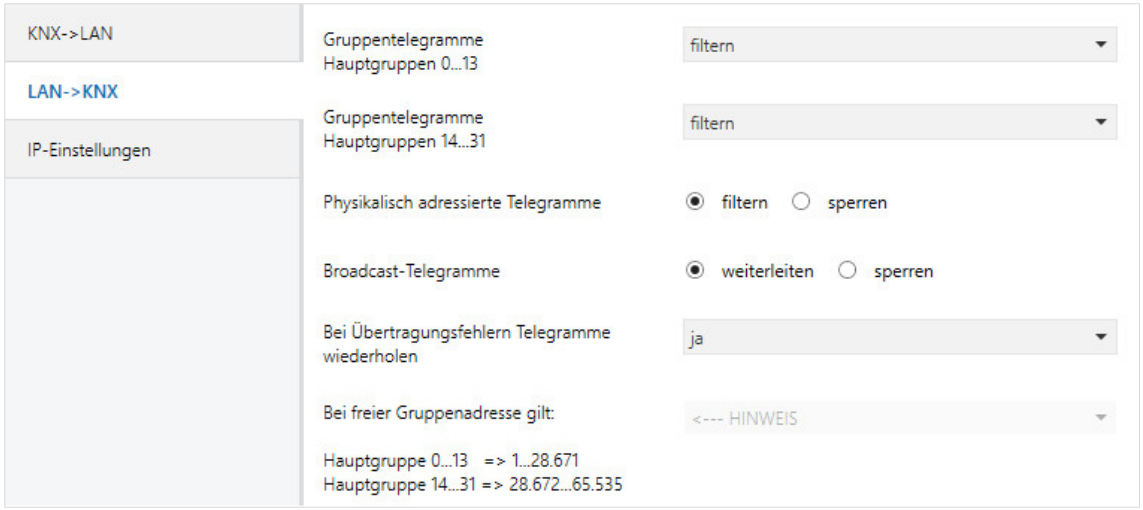
Bei freier Gruppenadresse gilt:

Hauptgruppen 0…13 => 1…28.671
Hauptgruppe 14…31 => 28.672…65.535

Hinweis
In der ETS 5 besteht die Möglichkeit, die Gruppenadressen nicht zwei- oder dreistufig zu vergeben, sondern frei. Wird die freie Gruppenadressansicht gewählt, entspricht Hauptgruppe 0…13 dem Untergruppenbereich 1…28.671 und Hauptgruppe 14…31 dem Untergruppenbereich 28.672…65.535. Details hierzu sind in der Hilfe der ETS nachzulesen.

3.2.2 Parameterfenster *LAN -> KNX*

Im Parameterfenster LAN -> KNX kann die Bearbeitung der Telegramme vom LAN-Netzwerk zum KNX-System festgelegt werden.



Gruppentelegramme Hauptgruppe 0…13

Optionen: filtern
weiterleiten
sperren

Dieser Parameter legt fest, ob Telegramme mit Gruppenadressen der Hauptgruppen 0 bis 13 gefiltert, weitergeleitet oder gesperrt werden sollen.

- *filtern:* Die Telegramme mit Gruppenadressen der Hauptgruppen 0 bis 13 vom KNX zum LAN werden gemäß der Filtertabelle, welche von der ETS automatisch berechnet wird, gefiltert.
- *weiterleiten:* Alle Gruppentelegramme der Hauptgruppen 0 bis 13 werden weitergeleitet, ohne Berücksichtigung der Filtertabelle.

Wichtig
Diese Einstellung ist nur für die Inbetriebnahme und zur Diagnose sinnvoll. Im Normalbetrieb sollte diese nicht verwendet werden. Da durch diese Einstellung die KNX-Linien überlastet werden können, kann es zu einem Telegrammverlust kommen.

- *sperren:* Alle Gruppentelegramme der Hauptgruppen 0 bis 13 werden gesperrt, ohne Berücksichtigung der Filtertabelle.

Gruppentelegramme Hauptgruppe 14…31

Optionen: filtern
weiterleiten
sperren

Dieser Parameter legt fest, ob Telegramme mit Gruppenadressen der Hauptgruppen 14…31 gefiltert, weitergeleitet oder gesperrt werden sollen.

- *filtern:* Die Telegramme mit Gruppenadressen der Hauptgruppen 14…31 vom KNX zum LAN werden gemäß der Filtertabelle, welche von der ETS automatisch berechnet wird, gefiltert.
- *weiterleiten:* Alle Gruppentelegramme der Hauptgruppen 14…31 werden weitergeleitet, ohne Berücksichtigung der Filtertabelle.

Wichtig
Diese Einstellung ist nur für die Inbetriebnahme und zur Diagnose sinnvoll. Im Normalbetrieb sollte diese nicht verwendet werden. Da durch diese Einstellung die KNX-Linien überlastet werden können, kann es zu einem Telegrammverlust kommen.

- *sperren:* Alle Gruppentelegramme der Hauptgruppen 14…31 werden gesperrt, ohne Berücksichtigung der Filtertabelle.

Physikalisch adressierte Telegramme

Optionen: filtern
sperren

Dieser Parameter legt fest, ob physikalisch adressierte Telegramme gefiltert oder gesperrt werden.

- *filtern:* Es werden nur die Telegramme vom KNX zum LAN übertragen, welche die Linie des IPR/S zum LAN verlassen sollen.
- *sperren:* Physikalisch adressierte Telegramme werden nicht vom IPR/S bearbeitet. Bei dieser Einstellung ist es nicht möglich, aus der Linie unterhalb des IPR/S heraus in eine andere Linie hinein physikalisch adressierte Telegramme zu schicken, z.B. während der Programmierung.

Broadcast-Telegramme

Optionen: weiterleiten
sperren

Dieser Parameter legt fest, ob Broadcast-Telegramme weitergeleitet oder gesperrt werden.

- *weiterleiten:* Broadcast-Telegramme werden weitergeleitet.
- *sperren:* Broadcast-Telegramme werden nicht vom IPR/S bearbeitet. Bei dieser Einstellung ist es nicht möglich, aus der Linie unterhalb des IPR/S heraus in eine andere Linie hinein Broadcast-Telegramme zu schicken, z.B. während der Programmierung.

Bei Übertragungsfehlern Telegramme wiederholen

Optionen: ja
nein
benutzerdefiniert

- *ja:* Wird bei der Übertragung eines Telegramms ein Fehler erkannt, wird das Telegramm bis zu drei Mal wiederholt
- *nein:* Die Übertragung wird nicht wiederholt.
- *benutzerdefiniert:* Das Verhalten kann für die unterschiedlichen Telegrammarten individuell eingestellt werden.

Bei Auswahl der Option *benutzerdefiniert* erscheinen folgende abhängigen Parameter:

Gruppenadressierte Telegramme wiederholen

Optionen: ja
nein

- *ja:* Wird bei der Übertragung eines gruppenadressierten Telegramms ein Fehler erkannt, wird das Telegramm bis zu drei Mal wiederholt.
- *nein:* Die Übertragung wird nicht wiederholt.

Physikalisch adressierte Telegramme wiederholen

Optionen: ja
nein

- *ja:* Wird bei der Übertragung eines physikalisch adressierten Telegramms ein Fehler erkannt, wird das Telegramm bis zu drei Mal wiederholt.
- *nein:* Die Übertragung wird nicht wiederholt.

Broadcast-Telegramme wiederholen

Optionen: ja
nein

- *ja:* Wird bei der Übertragung eines Broadcast-Telegramms ein Fehler erkannt, wird das Telegramm bis zu drei Mal wiederholt.
- *nein:* Die Übertragung wird nicht wiederholt.

Bei freier Gruppenadresse gilt:

Hauptgruppen 0…13 => 1…28.671
Hauptgruppe 14…31 => 28.672…65.535

Hinweis
In der ETS 5 besteht die Möglichkeit, die Gruppenadressen nicht zwei- oder dreistufig zu vergeben, sondern frei. Wird die freie Gruppenadressansicht gewählt, entspricht Hauptgruppe 0…13 dem Untergruppenbereich 1…28.671 und Hauptgruppe 14…31 dem Untergruppenbereich 28.672…65.535. Details hierzu sind in der Hilfe der ETS nachzulesen.

3.2.3 Parameterfenster *IP-Einstellungen*

Im Parameterfenster IP-Einstellungen wird eingestellt, wie der IP-Router Secure über IP kommuniziert.

IP-Kommunikationsart

Optionen: Multicast
Unicast

Die IP-Kommunikationsart legt fest, welche Art von Telegrammen der IP-Router Secure auf das IP-Netzwerk sendet.

- *Multicast:* Dies ist die für KNXnet/IP von der KNX Association festgelegte Kommunikationsart für KNX-IP-Geräte. Diese Einstellung sollte so beibehalten werden und nur geändert werden, wenn durch das vorhandene Netzwerk die Notwendwendigkeit besteht, Telegramme als Unicast zu senden.
  Zur Einstellung der Routing Multicast Adresse siehe Routing Multicast Adresse.
- *Unicast:* Das Routing für dieses Gerät wird abgeschaltet.

  Diese spezielle Kommunikation ist nicht gemäß KNXnet/IP Spezifikation. Zur Konfiguration wird das ABB i-bus® Tool benötigt.

  Die Kommunikationsart *Unicast* kann nicht verwendet werden, wenn das Gerät im KNX Secure-Modus betrieben wird. Wird bei aktiviertem KNX Secure-Modus *Unicast* ausgewählt, schaltet die ETS auf *Multicast* um. Die Parametrierung *Unicast* in der Applikation wird dann ignoriert.

  Um die Kommunikationsart *Unicast* zu verwenden, muss der KNX Secure-Modus in der ETS abgeschaltet werden.

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

Sowohl bei Auswahl *Multicast*, als auch bei Auswahl *Unicast* erscheint folgender Hinweis:

**Die Einstellung von Gerätename,
IP-Adresse und Tunneling Servern
erfolgt im Eigenschaftsfenster der ETS.**

Bei Auswahl *Unicast* erscheint zusätzlich folgender Hinweis:

Achtung! Diese Einstellung schaltet das Routing für dieses Gerät ab. Die IP-Telegramme werden nun als Unicast an bis zu 9 Zieladressen gesendet.

Die Unicast-Konfiguration erfolgt mit dem ABB i-bus® Tool.

Siehe Beschreibung *Kommunikation Unicast*, Kapitel 4.1.2, KNX-Telegramme im Netzwerk.

Das i-bus® Tool kann kostenlos von unserer Homepage (www.abb.com/knx) geladen werden.

Für das i-bus® Tool ist keine ETS und auch keine Installation des Falcon erforderlich.

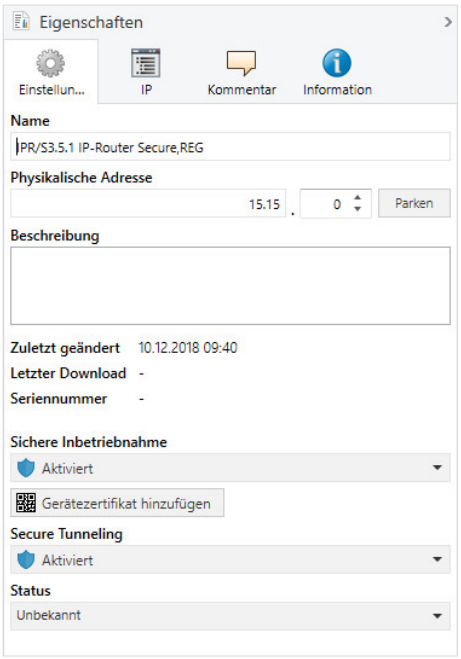
Die Systemanforderungen sind ein Windows-System ab Betriebssystemversion Windows 7 (Service Pack 3) und das .NET Framework ab Version 4.7.2.

Der integrierte Falcon 5.0 unterstützt nur USB- und IP Schnittstellen (kein RS232).

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

Wichtig
Es ist nicht möglich, die Unicast-Kommunikation bei aktiviertem KNX Secure-Modus zu nutzen. Ist der KNX Secure-Modus aktiviert und der Parameter *IP-Kommunikationsart* auf *Unicast* gesetzt, wird dennoch die Multicast-Kommunikation aktiviert. Bei der Parametrierung der Unicast Adressen über das i-bus® Tool wird ein entsprechender Hinweis angezeigt.

Die weitere Konfiguration der IP-Parameter (Gerätename, Zuweisung der IP-Adresse per DHCP oder fest) erfolgt im Eigenschaftenfenster der ETS.



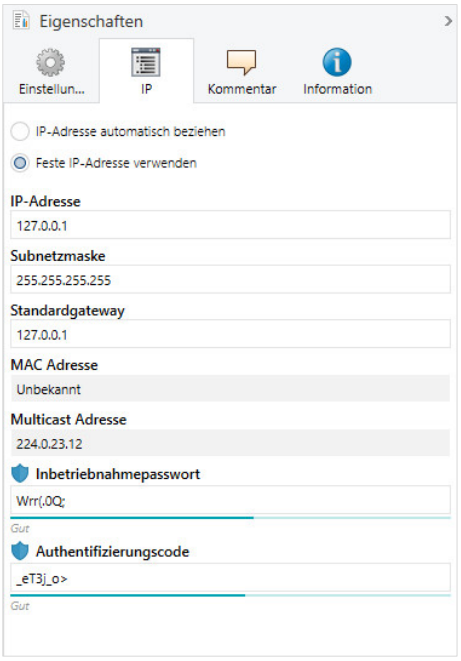
Im Eigenschaftsfenster *Einstellungen* kann der Gerätename eingetragen werden. Im Feld *Name* kann der Gerätename, der ins Gerät geladen wird, geändert werden.

Der Gerätename dient der Identifizierung des Geräts im LAN. Bei einer Suchanfrage, z.B. durch die ETS, meldet jedes KNXnet/IP-Gerät seinen Namen und kann darüber zugeordnet werden. So kann z.B. durch den Namen IPR/S, EG, UV7 auch der Einbauort des Geräts mitgeteilt werden.

Hinweis
Bei Auslieferung lautet der Gerätename standardmäßig "IP Router Secure". Nach dem ersten Download wird der Gerätename, der im Eigenschaftsfenster der ETS eingetragen wird, ins Gerät geladen.

Achtung
Es werden nur die ersten 30 Zeichen des Gerätenamens ins Gerät geladen, der Rest wird abgeschnitten.

Im Eigenschaftsfenster *IP* kann die IP-Adresse definiert werden.



Für die Einstellung der IP-Adresse stehen folgende Optionen zur Verfügung:

Optionen: IP-Adresse automatisch beziehen
Feste IP-Adresse verwenden

- *IP-Adresse automatisch beziehen:* In der Standardeinstellung erwartet der IP-Router Secure die Zuweisung einer IP-Adresse durch einen DHCP-Server (dynamic host configuration protocol). Dieser Server vergibt auf Anfrage eine freie IP-Adresse an das Gerät. Ist kein DHCP-Server im Netzwerk verfügbar, so startet das Gerät eine Auto-IP-Prozedur. Es vergibt sich selbst eine Adresse aus dem reservierten Bereich für Auto-IP-Adressen (169.254.1.0 bis 196.254.254.255).

  Zu DHCP siehe Kapitel 4.1.1., Vergabe der IP-Adresse.

- *Feste IP-Adresse verwenden:* Ist kein DHCP-Server im Netzwerk installiert oder soll die IP-Adresse immer gleich sein, so kann sie auch fest vergeben werden.
  Bei der Vergabe von festen IP-Adressen ist darauf zu achten, dass jedes Gerät eine unterschiedliche IP-Adresse erhält.

Hinweis
Die Routing Multicast Adresse wird hier nur angezeigt. Zur Einstellung der Routing Multicast Adresse siehe Routing Multicast Adresse.

Hinweis
Die MAC-Adresse wird nach einem Download aus dem Gerät ausgelesen. Zusätzlich ist die MAC-Adresse auf dem Gerät aufgebracht und kann alternativ über das i-bus® Tool ermittelt werden.

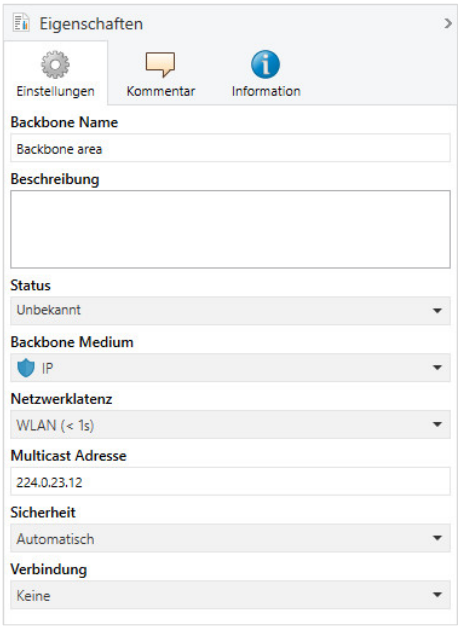
Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

Routing Multicast Adresse
(Standard = 224.0.23.12)

Optionen: 224.0.23.12

Die Routing Multicast Adresse legt die Zieladresse der IP-Telegramme des IPR/S fest. Die voreingestellte Adresse 224.0.23.12 ist die für KNXnet/IP von der KNX Association zusammen mit der IANA festgelegte Adresse für KNX-IP-Geräte. Diese Adresse sollte so beibehalten werden und nur geändert werden, wenn durch das vorhandene Netzwerk die Notwendwendigkeit besteht, eine andere Adresse aus dem Bereich 224.0.0.0 bis 239.255.255.255 (reservierter Bereich für Multicast-Adressen) zu verwenden.

Die Einstellung der Routing Multicast Adresse erfolgt in der ETS in der Ansicht *Topologie* (Auswahl der Topologie, dann kann im Eigenschaftenfenster auf dem Reiter *Einstellungen* die Routing Multicast Adresse eingestellt werden):



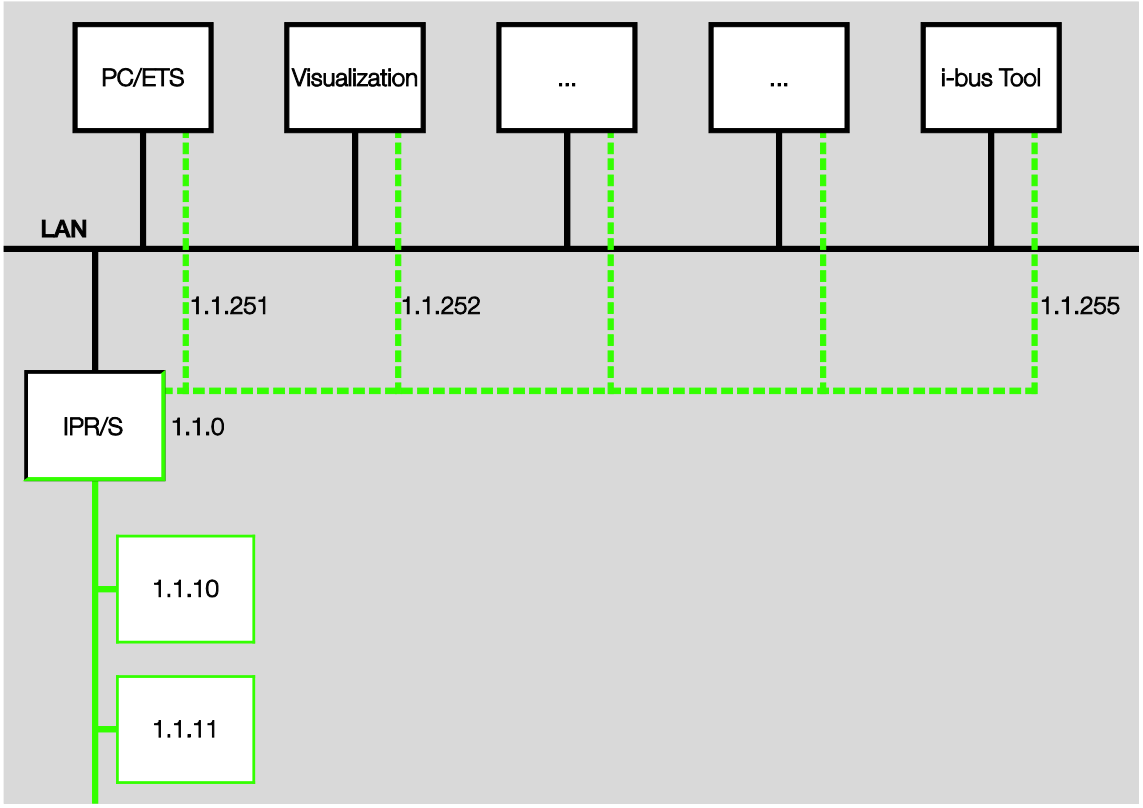
Wichtig
Alle IP-Router Secure oder andere KNXnet/IP-Geräte, die Telegramme am IP-Netzwerk austauschen sollen, müssen die gleiche Routing Multicast Adresse verwenden.

3.3 Kommunikationsobjekte

Der IP-Router Secure IPR/S hat keine KNX-Kommunikationsobjekte.

3.4 Verwendung der integrierten Tunneling-Server

Der IP-Router Secure bietet fünf zusätzliche physikalische Adressen, die für eine Tunneling-Verbindung verwendet werden können. Diese sogenannten Tunneling Server können mit der ETS als Programmierschnittstelle oder mit einem anderen Client, z.B. einer Visualisierung, verwendet werden.



Bei Tunneling verbindet sich ein Client mit einer Buslinie. Das Tunneling-Verfahren verwendet UDP, beinhaltet aber eine Sicherungsschicht, so dass im Fehlerfall Telegramme wiederholt werden.

Ab ETS 5 wird Tunneling V2 unterstützt. Hier wird anstatt UDP TCP verwendet und die Sicherungsschicht des TCP für die Übertragung verwendet.

Hinweis
Die physikalische Adresse für die Tunneling-Verbindung muss in die Topologie passen. Daher müssen die Adressen aus dem Adressbereich der untergeordneten Linie gewählt werden. Bei Auslieferung haben alle Tunneling Server die Adresse 15.15.100. In der ETS 5 werden die ersten fünf freien Adressen in der Linie automatisch vergeben, nachdem der Router in eine Linie eingefügt wurde.

Die Tunneling Server können auch mit KNX Secure verschlüsselt werden. Ist der KNX Secure-Modus aktiviert, benötigt ein Client das in der ETS vergebene Passwort.

Details siehe Kapitel 3.5, KNX Secure.

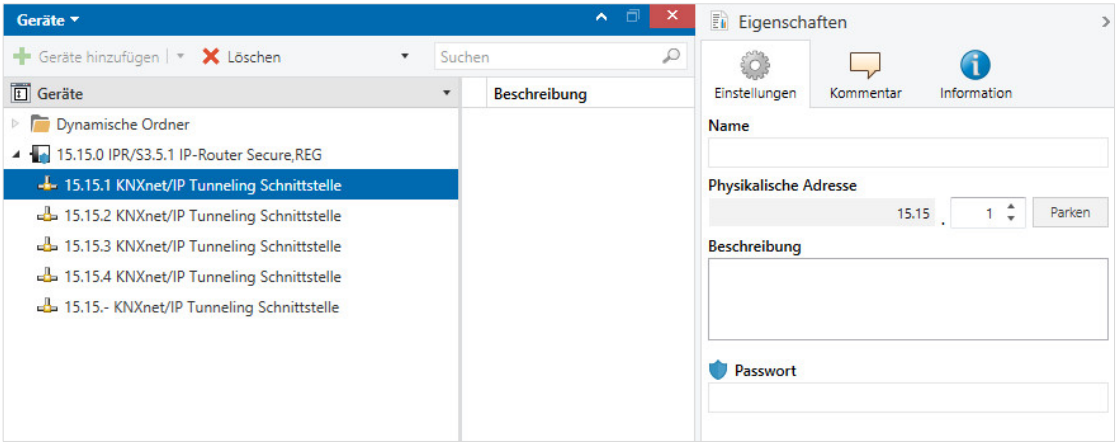
3.4.1 Einstellungen in ETS 5

In der ETS steht für die Einstellung der zusätzlichen physikalischen Adressen ein zusätzliches Eigenschaftenfenster zur Verfügung.

Die ETS reserviert automatisch nach Einfügen des Routers in die Linie die ersten fünf freien Adressen dieser Linie für die Tunneling Server des Routers. Dies ist eine Eigenschaft der ETS und kann nicht geändert werden.

Nach dem ersten Download stehen die Adressen im Gerät zur Verfügung.

Ist dies nicht erwünscht, kann die Einstellung manuell im Eigenschaftenfenster geändert werden:



Zum Ändern der Adresse die aktuelle Geräteadresse bzw. zusätzliche Adresse markieren und mit den Pfeiltasten nach oben oder unten die gewünschte Ziffer auswählen. Durch Markieren einer anderen Adresse wird die geänderte Adresse gespeichert.

Die geänderten Adressen werden erst nach einem Download vom Gerät übernommen.

Parken

Ist für einen Tunnel die Option *Parken* aktiviert, so erhält dieser Tunnel die Adresse 15.15.255.

Sofern bei allen Tunneling Servern die Option *Parken* gewählt wird, erhalten alle Tunneling Server die Adresse 15.15.255. Damit ist nur ein Tunneling Server verfügbar.

3.5 KNX Secure

Der ABB IP-Router Secure ist ein KNX Gerät nach dem KNX Secure Standard. D.h. das Gerät kann sicher in Betrieb genommen werden, die Kommunikation auf dem IP Backbone ist sicher (alle KNX IP Geräte müssen dazu das KNXnet/IP Security Protokoll unterstützen) und die Tunnelingverbindungen sind verschlüsselt.

Bei der Inbetriebnahme des Geräts sind daher folgende Dinge zu berücksichtigen.

- Sobald ein KNX Secure Gerät in ein Projekt importiert wird, muss zwingend ein Projektpasswort vergeben werden. Das Projekt ist damit gegen unbefugten Zugriff geschützt.
  Das Passwort muss sicher aufbewahrt werden – ohne dieses Passwort ist ein Zugriff auf das Projekt nicht möglich (auch nicht durch die KNX Association oder durch ABB)!
- Bei der Inbetriebnahme eines KNX Secure Gerätes (erster Download) ist ein Inbetriebnahmeschlüssel erforderlich. Dieser Schlüssel (FDSK = Factory Default Setup Key) ist auf einem Aufkleber seitlich auf dem Gerät aufgebracht und muss vor dem ersten Download in die ETS importiert werden.
  - Beim ersten Download des Gerätes öffnet sich in der ETS ein Fenster, die zur Eingabe des Schlüssels auffordert. Das Zertifikat kann alternativ auch mit einem QR Scanner eingelesen werden (empfohlen).
  - Alternativ können auch die Zertifikate aller Secure Geräte vorab in die ETS eingegeben werden. Dies erfolgt auf der Projektübersichtsseite auf dem Reiter „Sicherheit“.
  - Der FDSK Aufkleber ist doppelt auf dem Gerät aufgebracht. Ein Teil kann für die Projektdokumentation verwendet werden, der andere kann auf dem Gerät verbleiben.
    Ohne den FDSK kann das Gerät nach einem Reset nicht mehr im KNX Secure-Modus betrieben werden!

Der FDSK wird nur für die Erstinbetriebnahme benötigt. Danach vergibt die ETS neue Schlüssel.
Der FDSK wird erst wieder benötigt, wenn das Gerät auf Werkseinstellungen zurückgesetzt wurde (z.B. wenn das Gerät in einer anderen Anlage mit einem anderen ETS Projekt verwendet werden soll).

Die ETS vergibt an alle KNX IP Secure Geräte im Projekt den „Backbone“ Schlüssel und erzeugt auch für jeden Tunneling Server separate Passwörter. Die Passwörter können bei Bedarf geändert werden.
Die Schlüssel werden von der ETS erzeugt und verwaltet. Bei Bedarf können Schlüssel und Passwörter exportiert werden (z.B. falls ein Client auf einen der Tunnel zugreifen möchte).

Sofern erforderlich, kann der Router auf Werkseinstellungen zurückgesetzt werden, Siehe Kapitel 2.4.5 Entladen des Gerätes und Rücksetzen auf Werkseinstellungen.

4 Planung und Anwendung

4.1 Der IP-Router Secure im Netzwerk

Der IP-Router Secure ist für den Einsatz in 10/100-BaseT-Netzwerken nach IEEE 802.3 ausgelegt. Das Gerät besitzt eine AutoSensing-Funktion und stellt die Übertragungsgeschwindigkeit (10 oder 100 MBit) automatisch ein.

4.1.1 Vergabe der IP-Adresse

DHCP/AutoIP

Die IP-Adresse des Geräts kann von einem DHCP-Server bezogen werden. Dazu ist die Einstellung einer automatischen Vergabe der IP-Adresse in der ETS nötig, siehe Parameterfenster IP-Einstellungen. Wird bei dieser Einstellung kein DHCP-Server gefunden, startet das Gerät eine AutoIP-Prozedur und vergibt sich selbständig eine IP-Adresse aus dem Bereich 169.254.xxx.yyy.

Die IP-Adresse, die das Gerät beim Starten erhält (per DHCP oder AutoIP), wird beibehalten bis

- zum nächsten Neustart (Aus-/Einschalten oder Neuprogrammierung)
- ein DHCP-Server verfügbar ist
- zum Ablauf des des DHCP Lease

Beim Starten ist kein DHPC Server vorhanden

Sollte beim Starten des IP-Router Secures kein DHCP Server vorhanden sein, vergibt sich das Gerät selbst eine AutoIP Adresse. Der Router sucht dann zyklisch (drei Telegramme im Abstand von 3 Sekunden, anschließend 20 Sekunden Pause) nach einem DHCP Server. Sobald wieder ein Server vorhanden ist, wird die vom DHCP-Server zugeteilte Adresse verwendet.

DHCP-Server fällt aus (Gerät hat IP-Adresse bereits von DHCP bezogen)

Bis zum Ende der Lease-Zeit (Gültigkeitsdauer der IP-Adresse, wird bei der Vergabe der IP-Adresse vom DHCP-Server festgelegt) laufen die Anfragen zur Verlängerung der Nutzungsrechte dieser IP-Adresse ins Leere. Die IP-Adresse wird weiter verwendet.
Am Ende der Lease-Zeit oder nach einem Download sucht sich das Gerät eine AutoIP-Adresse.

Feste IP-Adresse

Soll die IP-Adresse des IPR/S fest zugeordnet sein, so kann in der ETS eine feste IP-Adresse (sowie Subnet-Maske und Standard Gateway) eingestellt werden, siehe Parameterfenster IP-Einstellungen.

4.1.2 KNX-Telegramme im Netzwerk

Hinweis
Bei der Auslegung des KNX-Systems ist zu beachten, dass die Anzahl der übertragenen Telegramme auch beim Einsatz des IP-Router Secures begrenzt ist. Durch die hohe Übertragungsrate auf IP-Seite (10/100 MBit/s) können bei hohem Datenaufkommen systembedingt in der TP1-Linie (9,6kBit/s) Telegramme verloren gehen.

Multicast

Multicast bezeichnet die Kommunikation eines Senders mit einer Gruppe von Empfängern.
Der IP-Router Secure sendet die KNX-Telegramme verpackt als UDP/IP-Telegramme auf das IP-Netzwerk und alle IP-Router Secure, bei denen die gleiche Multicast-Adresse parametriert ist, empfangen dieses Telegramm und werten es aus. Sofern ein Telegramm für die entsprechende Sublinie bestimmt ist, routet der IP-Router Secure das Telegramm in die Linie, ansonsten wird es verworfen.

Der IP-Router Secure sendet Telegramme von KNX auf das IP-Netzwerk gemäß KNXnet/IP-Protokollspezifikation. Diese Telegramme werden in der Standardeinstellung als Multicast-Telegramme auf die Multicast-IP-Adresse 224.0.23.12 Port 3671 gesendet. Diese Multicast-IP-Adresse ist die für KNXnet/IP von der KNX Association zusammen mit der IANA festgelegte Adresse für KNX IP-Geräte. Diese Adresse sollte so beibehalten und nur geändert werden, wenn durch das vorhandene Netzwerk die Notwendwendigkeit besteht, eine andere Adresse zu verwenden.

Damit mehrere IP-Router Secure im Netzwerk miteinander kommunizieren können, muss zwischen den Geräten eine Multicast-Kommunikation möglich sein. Je nach Art des Netzwerks und der Einstellung der verwendeten Netzwerkkomponenten, z.B. Router, Switch oder Firewall, muss die Multicast-IP-Adresse 224.0.23.12 eventuell erst noch explizit freigeschaltet werden. Bitte sprechen Sie dazu mit dem Netzwerkadministrator.

Weitere Informationen siehe Kapitel 3.2.3, Parameterfenster IP-Einstellungen.

Unicast

Unicast bezeichnet allgemein die Kommunikation zwischen einem Sender und einem Empfänger.
Der Router stellt also zu jedem IP-Router innerhalb der Unicast-Gruppe eine Kommunikationsverbindung her.

Falls in einem Netzwerk keine Multicast-Kommunikation möglich ist, können die ABB IP-Router auch über Unicast miteinander kommunizieren. Bis zu zehn ABB IP-Router können zu einer Unicast-Gruppe zusammengefasst werden. Die Unicast-Gruppe kann aus IPR/S 3.1.1 und/oder IPR/S 3.5.1 bestehen, auch gemischt. Jedem Router werden dann neun IP-Adressen zugewiesen, an die er seine Telegramme versendet.

Die Konfiguration dieser Unicast-Gruppe erfolgt einfach und automatisch mit dem ABB i-bus® Tool.

Es ist auch möglich, einen Client (z.B. eine Visualisierung) mit dieser Unicast-Gruppe zu verknüpfen.
In diesem Fall ist eine der zehn Unicast-Adressen vom Client belegt, und es können noch neun IP-Router Secure verknüpft werden.

Die genaue Beschreibung, wie die Konfiguration mit dem i-bus® Tool funktioniert, ist in der Hilfe des i-bus® Tools zu finden (siehe Kapitel 4.2, Das i-bus® Tool).

Hinweis
Sobald in der ETS unter IP-Kommunikationsart der Parameter auf *Unicast* umgestellt wird, ist die Funktion *Multicast* deaktiviert. Die Geräte können dann nicht mehr über Multicast Routing, sondern nur noch über einen der integrierten Tunneling Server oder eine separate Programmierschnittstelle programmiert werden. Allerdings wird die Kommunikationsart erst umgestellt, wenn die Parametrierung mit dem i-bus® Tool erfolgt ist. Bis dahin steht der Router intern noch auf Multicast. Dies hat den Vorteil, dass der Router über Multicast programmiert werden kann.

Weitere Informationen siehe Parameterfenster IP-Einstellungen.

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

Hinweis
• Bei der Verwendung der Kommunikationsart Unicast muss sicher gestellt sein, dass sich die IP-Adresse des Routers im laufenden Betrieb nicht ändert. Dazu sollte entweder eine feste IP-Adresse vergeben werden, oder eine entsprechende Einstellung beim DHCP Server erfolgen. • Durch die ETS werden bei Änderung der physikalischen Adresse alle IP-Parameter ebenfalls aktualisiert. D.h. auch wenn nur die Option *Programmieren physikalische Adresse* in der ETS ausgewählt wird, werden der Gerätename, die Multicast-Adresse, IP-Kommunikationsart (DHCP, AutoIP, fest), IP-Adresse, Subnetzmaske, Standard-Gateway und alle Tunneling-Adressen neu geladen. Sofern sich die IP-Adresse dabei ändert, muss die Unicast-Konfiguration mit dem i-bus® Tool erneut durchgeführt werden.

Die Kommunikationsart *Unicast* kann nicht verwendet werden, wenn das Gerät im KNX Secure-Modus betrieben wird. Wird bei aktiviertem KNX Secure-Modus *Unicast* ausgewählt, schaltet die ETS auf *Multicast* um. Die Parametrierung *Unicast* in der Applikation wird dann ignoriert.

Um die Kommunikationsart *Unicast* zu verwenden, muss der KNX Secure-Modus in der ETS abgeschaltet werden.

4.1.3 Überwachung eines IPR/S 3.5.1

Die Überwachung einer Tunnelingverbindung sollte bei einer aktiven Tunneling Verbindung über ein „CONNECTIONSTATE_REQUEST“ erfolgen, ist aber auch per T-Connect möglich.

Die Überwachung eines Gerätes über T-Connect kann Nachteile haben, z.B. bei Überwachungs-, Programmier- oder Scanvorgängen in der Linie.

4.1.4 System Broadcast

In einer KNX Anlage müssen alle IP-Geräte, die miteinander kommunizieren wollen, die gleiche Multicast-Adresse nutzen. Standardmäßig wird die Adresse 224.0.23.12 Port 3671 verwendet, siehe Multicast.

Wird in einer Anlage die Multicastadresse geändert, kann es bei der Inbetriebnahme u.U. zu Problemen kommen. Wird z.B. zuerst die Multicastadresse des nächstgelegenen Routers geändert, schaltet dieser nach der Programmierung auf die neue Mulicast-Adresse um. Der Rest der Anlage ist für ihn dann nicht mehr erreichbar und die übrigen Router in der Anlage können nicht mehr programmiert werden.

Diese Geräte kann die ETS dann über die „System Broadcast Adresse“ erreichen. Über die System Broadcast Adresse kann die Multicast-Adresse aller KNX IP-Geräte und auch der Backbone Schlüssel geändert werden. Dies funktioniert nur, wenn das Gerät entweder nicht im KNX Secure-Modus betrieben wird oder der ETS der Backbone Schlüssel bekannt ist.

Das Weiterleiten von System Broadcast Telegramme kann über den Parameter *Broadcast-Telegramme weiterleiten/sperren* eingestellt werden, d.h. dieser Parameter ist für (Standard) Broadcast-Telegramme und System Broadcast-Telegramme wirksam.

4.1.5 IGMP

Das Gerät unterstützt IGMP snooping in der Version V3.

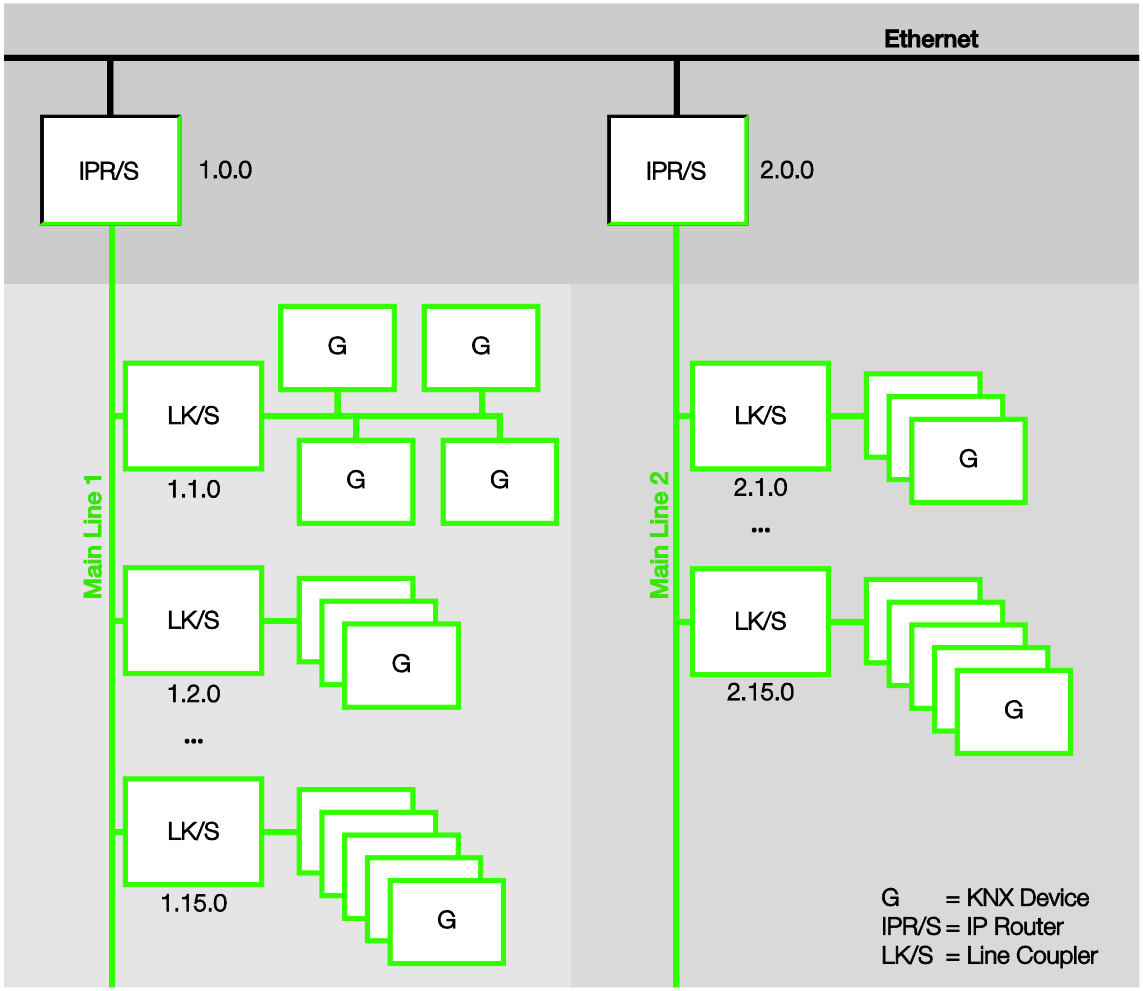
IGMP snooping ist die Fähigkeit Multicast Routing Verkehr nur dorthin weiterzuleiten, wo er auch benötigt wird. Die IT Infrastruktur und das Gerät müssen die gleiche IGMP Version benutzen, sonst funktioniert der IGMP Mechanismus nicht.

Zum Freischalten einer Multicast Adresse meldet sich das Gerät mit einem Membership Report bei dieser Multicast Adresse an.

4.1.6 IPR/S als Bereichskoppler

Der IP-Router Secure kann in KNX-Anlagen die Funktion eines Bereichskopplers übernehmen. Dafür muss er die physikalische Adresse eines Bereichskopplers (1.0.0…15.0.0) erhalten. In einem ETS-Projekt können bis zu 15 Bereiche mit Bereichskopplern angelegt werden.

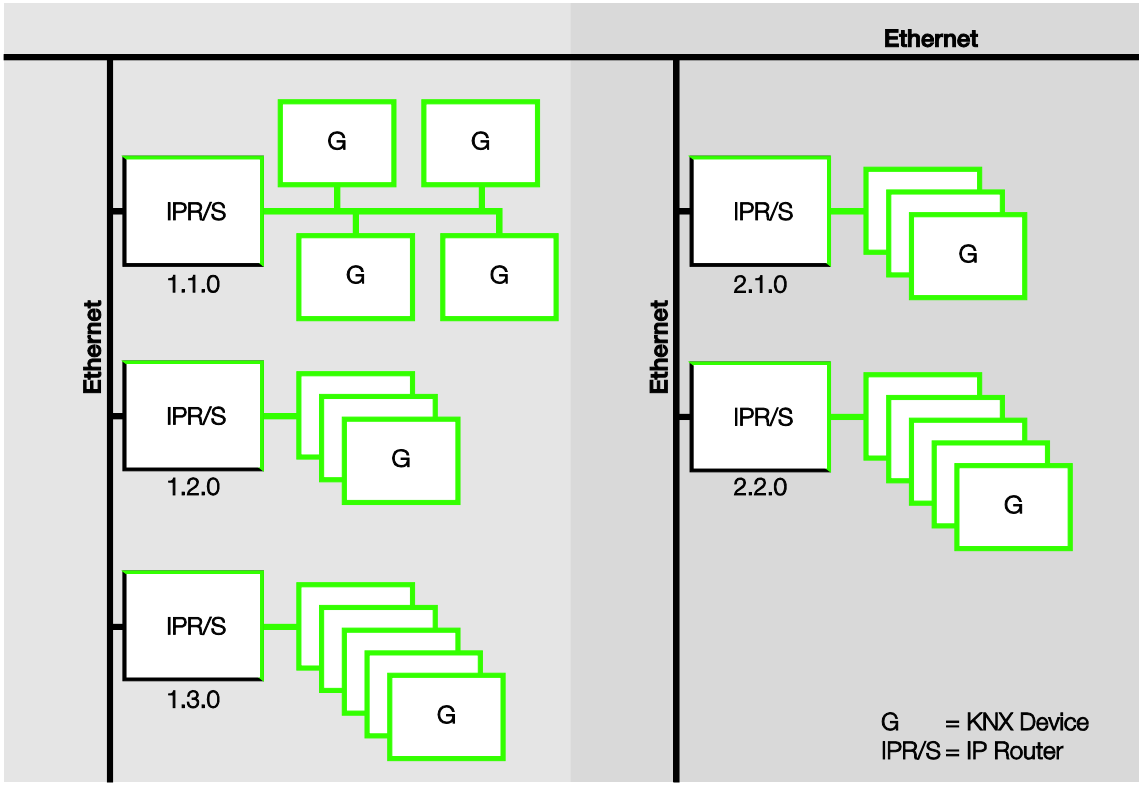
Das folgende Bild zeigt diese Topologie mit IP-Router Secure als Bereichskoppler und KNX-Linienkoppler (LK/S).



4.1.7 IPR/S als Linienkoppler

Der IP-Router Secure kann in KNX-Anlagen die Funktion eines Linienkopplers übernehmen. Dafür muss er die physikalische Adresse eines Linienkopplers (1.1.0…15.15.0) erhalten.

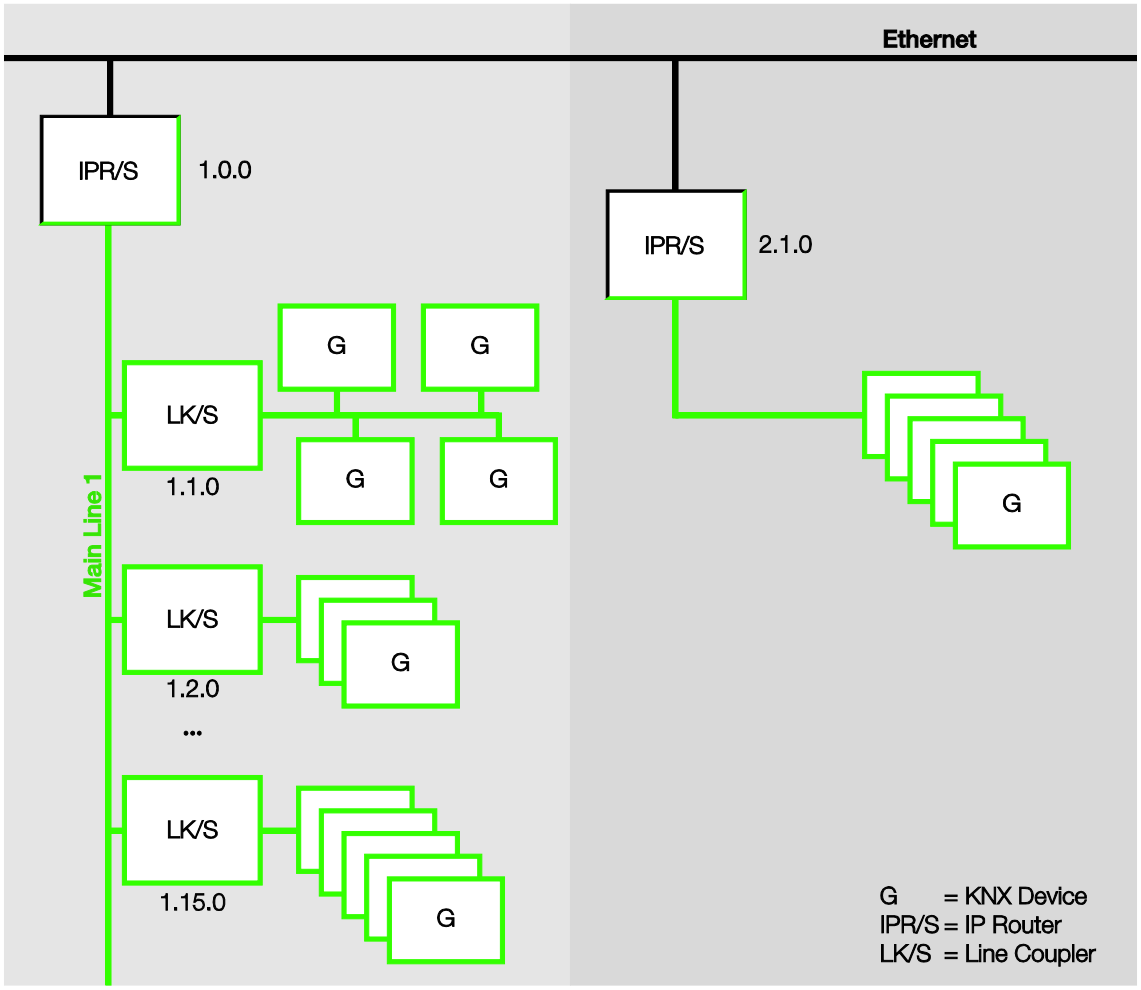
Das folgende Bild zeigt diese Topologie mit IP-Router Secure als Linienkoppler.



4.1.8 Gemischte Topologie

Ist es innerhalb einer KNX-.Anlage nötig, den IP-Router Secure an einer Stelle, z.B. Bürohaus, als Bereichskoppler und an anderer Stelle, z.B. entfernte Tiefgarage, als Linienkoppler einzusetzen, so ist dies möglich.

Dabei muss nur beachtet werden, dass der IP-Router Secure als Linienkoppler die Linienkoppleradresse aus einem freien Bereich verwendet, z.B. hier im Bild 2.1.0.

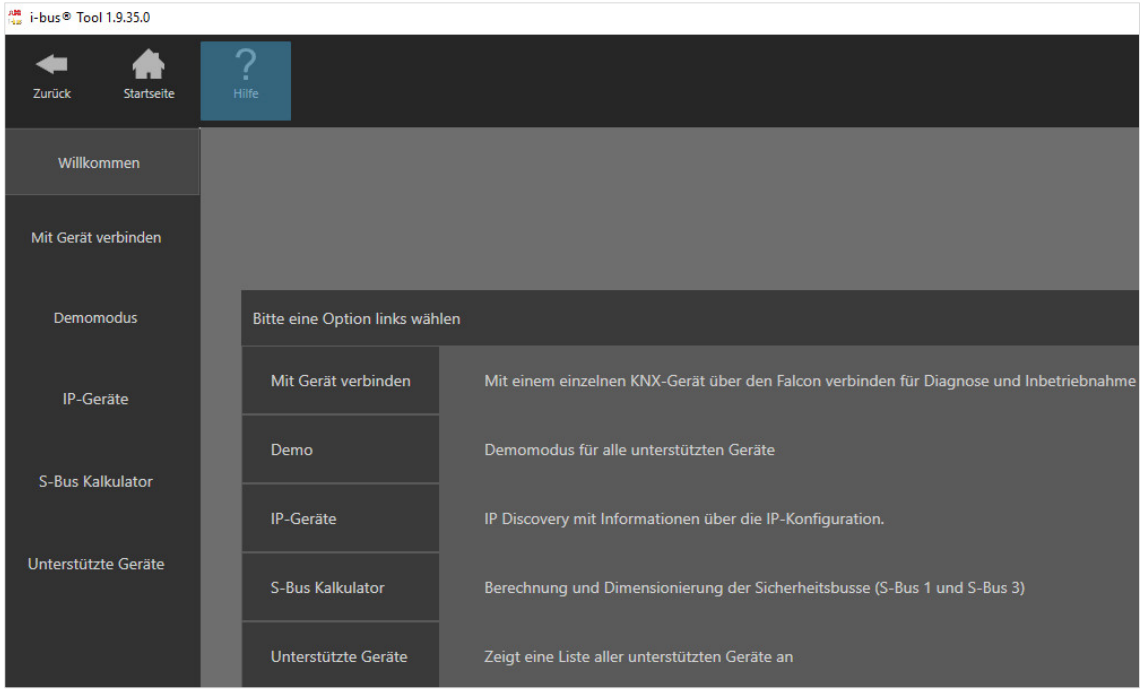


4.2 Das i-bus® Tool

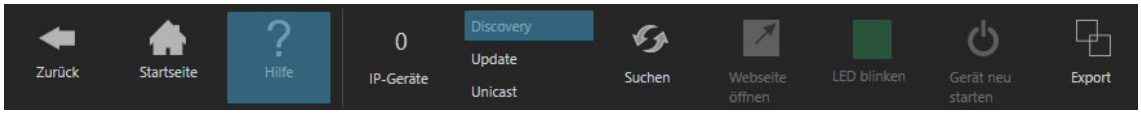
Das ABB i-bus® Tool wird benötigt, um bestimmte Funktionen bei den ABB IP-Geräten einzustellen.

Es erleichtert die Inbetriebnahme auf IP-Seite.

Klicken Sie auf der Startseite des i-bus® Tools auf *Verbinden*, in dem danach erscheinenden Fenster dann auf *IP-Geräte*.



Multifunktionsleiste: Umschalten zwischen Discovery, Firmware Update und Unicast



Klicken Sie auf die entsprechende Schaltfläche, um den Modus *Discovery* oder *Unicast* auszuwählen.

4.2.1 Discovery

Wählen Sie in der Multifunktionsleiste den Modus *Discovery*. Diese Funktion dient zum Auffinden und Anzeigen von ABB IP-Geräten im Netzwerk. Wird der IP-Router im KNX Secure-Modus betrieben, werden nicht alle Informationen angezeigt.

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

4.2.2 Firmware Update

**Im KNX Secure-Modus kann das Gerät nicht mit dem i-bus® Tool aktualisiert werden.
Das Firmwareupdate kann in diesem Fall nur mit der ETS App „ABB KNX Bus Update“ erfolgen, die kostenlos im KNX Online Shop geladen werden kann.**

Wählen Sie in der Multifunktionsleiste den Modus *Update*. Sofern es einmal notwendig sein sollte, kann mit dieser Funktion die Firmware aktualisiert werden.

Wichtig
Die Firmware muss vorab aus dem Internet geladen werden (*www.abb.com/knx)*. Dazu verbindet sich das i-bus® Tool **bei bestehender Internetverbindung** mit einem Server. Für die Aktualisierung der Geräte auf der Anlage ist dann keine Internetverbindung mehr notwendig.

Wichtig
Während des Updatevorgangs muss zusätzlich zum IP-Netzwerk (LAN) auch der KNX-Bus (TP) angeschlossen sein, damit die KNX-Parameter korrekt wiederhergestellt werden können. Andernfalls schlägt der Updatevorgang fehl. Es muss sichergestellt werden, dass während des Updatevorgangs kein Spannungsausfall (KNX oder IP) auftritt, da ansonsten das Gerät zerstört werden kann.

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

Hinweis
Für den Updatevorgang muss das i-bus® Tool mit Administratorrechten ausgeführt werden.

Unicast

Wählen Sie in der Multifunktionsleiste den Modus *Unicast*.

Diese Funktion ist nur verfügbar, wenn vorher in der ETS-Applikation der Parameter *IP-Kommunikationsart* auf *Unicast* umgestellt worden ist.

Hinweis
Eine Beschreibung der Funktionen ist in der Online-Hilfe des i-bus® Tools zu finden.

A Anhang

A.1 Bestellangaben

Gerätetyp	Produktname	Erzeugnis-Nr.	bbn 40 16779 EAN	Gew. 1 St. [kg]	Verp.-einh. [St.]
IPR/S 3.5.1	IP-Router Secure, REG	2CDG110176R0011	**90650 0**	0,1	1

A.2 Open Source Softwarekomponenten

Eine Liste der verwendeten Open Source Komponenten ist im Internet unter folgendem Link zu finden:

http://search.abb.com/library/Download.aspx?DocumentID=9AKK107492A5258&LanguageCode=en&DocumentPartId=&Action=Launch

ABB STOTZ-KONTAKT GmbH
Eppelheimer Straße 82
69123 Heidelberg, Deutschland
Telefon: +49 (0)6221 701 607
Telefax: +49 (0)6221 701 724
E-Mail: knx.marketing@de.abb.com

Weitere Informationen und regionale Ansprechpartner
www.abb.de/knx
www.abb.com/knx

Druckschriftennummer 2CDC502099D0111 Rev. A | 27.06.2019