

PRODUCTHANDBOEK

ABB i-bus[®] KNX

IPR/S 3.5.1

IP-Router Secure



Inhoud

Pagina

1	Algemeen.....	5
1.1	Het producthandboek gebruiken.....	5
1.1.1	Opmerkingen.....	5
1.2	Cybersecurity (netwerkbeveiliging).....	6
1.3	Toegang tot de verschillende media blokkeren	6
1.4	Twisted-pair kabels.....	6
1.5	IP-kabels in het gebouw	6
1.6	Met internet verbinden.....	7
1.7	KNXnet/IP Security.....	7
1.8	Product- en functieoverzicht	7
1.8.1	Op uitval van de busspanning bewaken	8
1.8.2	Overzicht versies	9
2	Apparaattechniek.....	11
2.1	Technische gegevens.....	11
2.2	Aansluitschema	13
2.3	Afmetingen	14
2.4	Montage en installatie.....	15
2.4.1	Voorwaarde voor ingebruikname.....	15
2.4.2	Toestand bij levering	15
2.4.3	Toekenning van het fysieke adres	16
2.4.4	Downloaden.....	16
2.4.5	Software van apparaat verwijderen en apparaat op fabrieksinstellingen resetten	16
2.4.6	Reinigen	17
2.4.7	Onderhoud.....	17
2.5	Beschrijving van de in- en uitgangen.....	17
2.6	Bedieningselementen	18
2.7	Weergave-elementen	18
3	Ingebruikname	19
3.1	Overzicht	19
3.2	Parameters	19
3.2.1	Parametervenster <i>KNX -> LAN</i>	20
3.2.2	Parametervenster <i>LAN -> KNX</i>	23
3.2.3	Parametervenster <i>IP-instellingen</i>	26
3.3	Communicatieobjecten	30
3.4	De geïntegreerde tunnelingservers gebruiken.....	31
3.4.1	Instellingen in de ETS 5.....	32
3.5	KNX Secure.....	33
4	Ontwerp en toepassing	35
4.1	De IP-router Secure in het netwerk	35
4.1.1	Toekenning van het IP-adres.....	35
4.1.2	KNX-telegrammen in het netwerk.....	36
4.1.3	Een IPR/S 3.5.1 bewaken.....	37
4.1.4	Systeembroadcast.....	37
4.1.5	IGMP	38
4.1.6	IPR/S als zonekoppelaar	38
4.1.7	IPR/S als lijnkoppelaar	39
4.1.8	Gemengde topologie	40
4.2	De i-bus® Tool	41
4.2.1	Discovery.....	41
4.2.2	Firmware-update	42
A	Bijlage	43
A.1	Bestelgegevens	43
A.2	Opensourcecomponenten	43

ABB i-bus® KNX

Inhoud

1 Algemeen

De ABB i-bus® IP-router Secure IPR/S 3.5.1 verbindt de KNX-bus met een ethernetnetwerk. Via het netwerk kunnen KNX-telegrammen aan andere apparaten worden verzonden of van andere apparaten worden ontvangen.

Het apparaat ondersteunt het KNX Secure-protocol (KNXnet/IP Security).

1.1 Het producthandboek gebruiken

In dit handboek vindt u gedetailleerde technische informatie over de werking, montage en programmering van het ABB i-bus® KNX-apparaat. Het gebruik wordt aan de hand van voorbeelden uitgelegd.

Het handboek bevat de volgende hoofdstukken:

Hoofdstuk 1	Algemeen
Hoofdstuk 2	Apparaattechniek
Hoofdstuk 3	Ingebruikname
Hoofdstuk 4	Ontwerp en toepassing
Hoofdstuk A	Bijlage

1.1.1 Opmerkingen

In dit handboek worden opmerkingen en veiligheidswaarschuwingen als volgt weergegeven:

Opmerking
Vereenvoudigingen en tips voor de bediening

Voorbeelden
Voorbeelden van toepassing, montage en programmering

Belangrijk
Deze veiligheidswaarschuwing wordt gebruikt als er kans is op een functiestoring zonder risico van schade of letsel.

Let op
Deze veiligheidswaarschuwing wordt gebruikt als er kans is op een functiestoring zonder risico van schade of letsel.

 Gevaar
Deze veiligheidswaarschuwing wordt gebruikt als er door onjuist gebruik of bediening gevaar voor lijf en leven ontstaat.

 Gevaar
Deze veiligheidswaarschuwing wordt gebruikt als er door onjuist gebruik of bediening acuut levensgevaar ontstaat.

1.2 Cybersecurity (netwerkbeveiliging)

Onze branche wordt steeds vaker met online veiligheidsrisico's geconfronteerd. Voor stabielere, veiligere en robuustere oplossingen heeft ABB in het kader van het productontwikkelingsproces officieel robuustheidscontroles voor online beveiliging ingevoerd.

De volgende aanwijzingen dienen als extra richtlijn en verwijzen naar mechanismen die gebruikt kunnen worden om de beveiliging van KNX-installaties te verbeteren.

1.3 Toegang tot de verschillende media blokkeren

Aan de basis van elk beschermingsconcept ligt de zorgvuldige afscherming van het systeem tegen ongeoorloofde toegang. Bij een KNX-installatie geldt dat alleen geautoriseerde personen (installateur, huismeester, gebruiker) fysieke toegang tot de KNX-installatie mogen hebben. Bij de planning en installatie moeten voor elk KNX-medium de kritieke punten zo goed mogelijk worden beveiligd.

In principe geldt dat toepassingen en apparaten vast moeten worden gezet, zodat ze niet makkelijk kunnen worden verwijderd, waardoor onbevoegde personen toegang tot de KNX-installatie hebben. Subsystemen met KNX-apparaten moeten zijn afgesloten of zich in een ruimte bevinden waartoe alleen bevoegde personen toegang hebben.

1.4 Twisted-pair kabels

- ▶ De uiteinden van de twisted-pair KNX-kabels mogen niet zichtbaar zijn of uit de muur steken, noch aan de binnenkant van het gebouw, noch aan de buitenkant.
- ▶ Indien beschikbaar moeten de anti-diefstalbeschermingen van de applicatiemodule worden gebruikt.
- ▶ Bus-kabels aan de buitenkant vormen een verhoogd risico. De fysieke toegang tot de twisted-pair KNX-kabels moet hiervoor bijzonder moeilijk worden gemaakt.
- ▶ Apparaten die in beperkt beveiligde ruimtes zijn ingebouwd (buiten, parkeergarage, WC, etc.) kunnen als extra beveiliging als eigen lijn worden uitgevoerd. Door de filtertabellen in de lijnkoppelaar (alleen KNX) te activeren, wordt voorkomen dat een aanvaller toegang tot de hele installatie heeft.

1.5 IP-kabels in het gebouw

Voor de gebouwautomatisering moet een apart LAN- of wifi-netwerk met eigen hardware (router, switches, etc.) worden gebruikt.

Onafhankelijk van de KNX-installatie moeten per se de gewoonlijke beveiligingsmechanismen voor IP-netwerken worden gebruikt. Dit zijn bijvoorbeeld:

- MAC-filter
- versleuteling van draadloze netwerken
- gebruik van sterke wachtwoorden en bescherming hiervan tegen onbevoegde personen

Opmerking

Tijdens IP-, TCP- of UDP-flooding (toegang via internet) is het apparaat niet bereikbaar. Om deze reactie te vermijden, moet een limiet voor de gegevenssnelheid op netwerkniveau worden ingesteld. Neem hiervoor contact op met de netwerkbeheerder.

1.6 Met internet verbinden

Het apparaat is niet bedoeld voor gebruik in het openbare internet. Daarom poorten van routers niet richting internet worden geopend. Op deze manier wordt voorkomen dat de KNX-communicatie op internet zichtbaar is.

Toegang vanuit internet tot een installatie is op de volgende manieren mogelijk:

- Toegang tot KNX-installaties via VPN-verbindingen; hiervoor is echter een router met VPN-serverfunctionaliteit nodig.
- Gebruik van fabrikantspecifieke oplossingen of visualisaties, bijv. met toegang via https.

1.7 KNXnet/IP Security

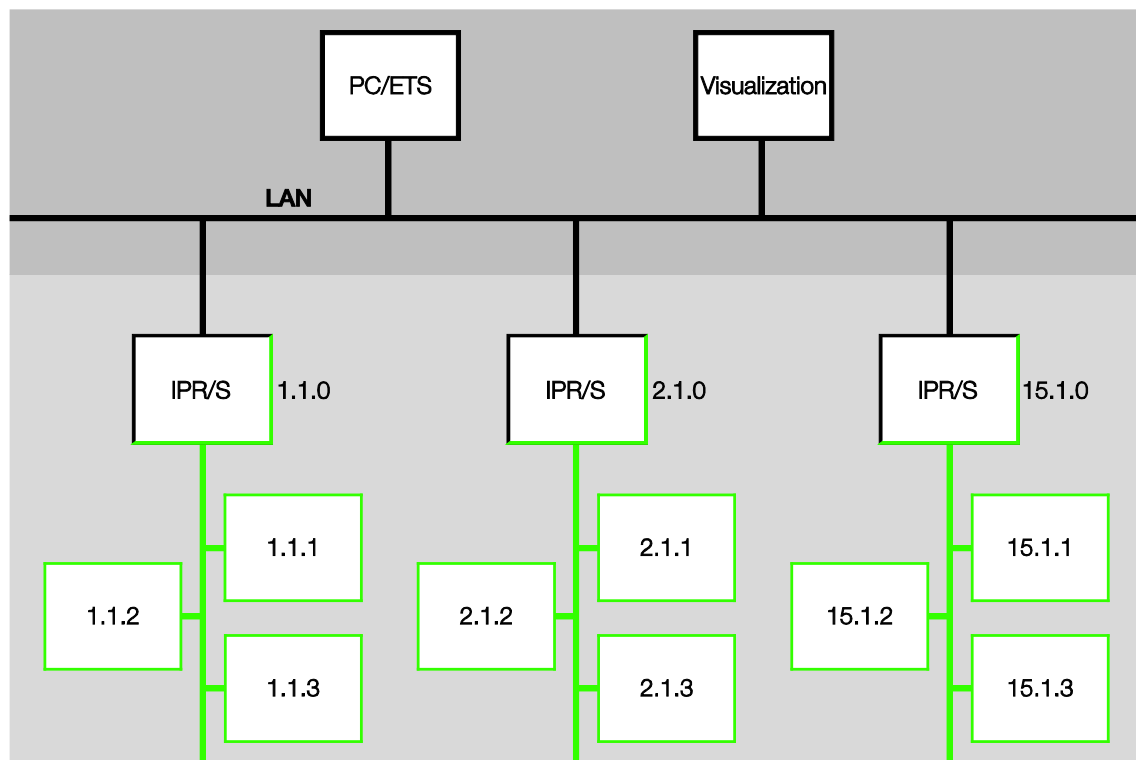
Het apparaat moet altijd in de KNX Secure-modus staan. Op die manier zijn de looptijdcommunicatie op de IP-backbone, de tunnelingserver en de ingebruikname van het apparaat zeker gesteld.

Zie ook hoofdstuk 3.5, [KNX Secure](#).

1.8 Product- en functieoverzicht

De ABB i-bus® IP-router Secure IPR/S 3.5.1 verbindt de KNX-bus met een ethernetnetwerk. Via het netwerk kunnen KNX-telegrammen aan andere apparaten worden verzonden of van andere apparaten worden ontvangen.

De communicatie van het apparaat verloopt via het KNXnet/IP-protocol en het KNXnet/IP Security-protocol van de KNX Association (routing en tunneling).



De router beschikt over vijf tunnelingservers; zie hoofdstuk 3.4, [De geïntegreerde tunnelingserver gebruiken](#). Deze ondersteunen zowel de werking van de busmonitor als van de groepsmonitor.

De tunnelingservers kunnen ook in de KNX Secure-modus worden gebruikt.

Als alternatief voor de KNX-standaardcommunicatie (multicast) kunnen maximaal 10 ABB IP-routers IPR/S 3.x.1 ook via het unicast-protocol met elkaar communiceren; zie hoofdstuk 4.1.2, [KNX-telegrammen in het netwerk](#). De KNX Secure-modus is in dit geval niet beschikbaar.

De voeding kan via PoE (Power over Ethernet) volgens IEEE 802.3af Klasse 1 gebeuren of via een hulpspanning.

Voor de IP-router Secure kan de ABB i-bus® tool worden gebruikt, waarmee de routers in het netwerk kunnen worden gevonden (IP Discovery) en de instellingen voor de unicast-communicatie kunnen worden gemaakt. (Zie hoofdstuk 4.2, [De i-bus® tool](#).)

Voor de firmware-update is er al een ETS-app (ABB KNX Bus Update) beschikbaar. Als de KNX Secure-modus niet is geactiveerd bij de apparaten, kan een firmware-update ook via de i-bus® Tool worden uitgevoerd.

Tijdens het updaten moet naast het IP-netwerk (LAN) ook de KNX-bus (TP) aangesloten zijn, zodat de KNX-parameters correct opnieuw kunnen worden ingesteld. Anders mislukt het updaten.

Tijdens het update mag de voeding niet wegvallen (KNX of IP), omdat het apparaat dan kan worden vernield.

Het apparaat ondersteunt de KNX-standaardfunctie "Bewaking op uitval van de busspanning". Dit is een netwerkmanagementfunctie die bijvoorbeeld door visualisaties wordt gebruikt (zie hoofdstuk 1.8.1, [Bewaking op uitval van de busspanning](#)).

1.8.1

Op uitval van de busspanning bewaken

De IP-router Secure bewaakt de KNX TP-bus op spanningsuitval. Bij een toestandswijziging van de busspanning wordt een broadcast-commando van het type "NetworkParameterWrite" naar het IP-netwerk gezonden.

De volgende waarden worden verzonden:

- Uitval van de busspanning: "00063301" (hex)
- Terugkeer van de busspanning: "00063300" (hex)

Deze telegrammen kunnen bijvoorbeeld door een visualisering worden geëvalueerd.

Type	Info	Betekenis
NetworkParameterWrite	00 06 33 01	Busspanningsuitval TP1
NetworkParameterWrite	00 06 33 00	Busspanningsterugkeer TP1

1.8.2

Overzicht versies

Apparaat	IPR/S 3.1.1	IPR/S 3.5.1
Applicatie	IP-Router /2.0	IP-Router Secure/1.0
ETS	ETS 4/5	ETS 5
Eigenschappen IP-Router		
Aantal tunnelingservers	5	5
Aantal unicast-verbindingen	10	10
Op busspanningsuitval bewaken (zie hoofdstuk 1.8.1, Op uitval van de busspanning bewaken)	■	■
Filtering groepstelegrammen hoofdgroep 0-31	■	■
IP-Discovery (i-bus® Tool)	■	■
Firmware-update met i-bus® Tool	■	■*
Firmware-update met de app KNX Bus Update	-	■
Parametreering unicast (i-bus® Tool)	■	■*
Power over Ethernet	■	■
KNX Secure	-	■

* Alleen wanneer apparaat niet in de KNX Secure-modus wordt gebruikt.

2 Apparaattechniek



IPR/S 3.5.1

2CDC071007F0017

De IP-router Secure 3.5.1 vormt de interface tussen KNX-installaties en IP-netwerken. Hij kan als lijn- of zonekoppelaar worden ingezet en bovendien het lokale netwerk (LAN) gebruiken voor het uitwisselen van telegrammen tussen de lijnen/bereiken.

Met ETS kunnen KNX-apparaten via het LAN worden geprogrammeerd (er zijn 5 tunnelingsservers beschikbaar). Het apparaat gebruikt het KNXnet/IP-protocol of het KNXnet/IP Security-protocol van de KNX Association (routing en tunneling).

Het apparaat kan ook via unicast communiceren.

De voeding gebeurt met 12 tot 30 V DC of PoE (Power over Ethernet) volgens IEEE 802.3af, klasse 1.

2.1 Technische gegevens

Voeding	Voedingsspanning U_s	12...30 V DC (+10% / -15%) of PoE (IEEE 802.3af, klasse 1)
	Vermogensverlies	Maximaal 1,8 W
	Stroomopname voedingsspanning	Maximaal 120 mA bij 12 V
	Nominale spanning U_n	12 V DC
	Stroomopname KNX	< 10 mA
Aansluitingen	KNX	Bus-aansluitklemmen
	Bedrijfsspanning	Steekklem
	LAN	RJ45-bus voor 10/100BaseT, IEEE 802.3 netwerken, AutoSensing
Bedienings- en weergave-elementen	LED rood en toets	Toekenning van het fysieke adres
	LED groen "On"	Weergave bedrijfsklaar
	LED geel "LAN/link"	Weergave netwerkverbinding
	LED geel "Telegram"	Weergave KNX-telegramverkeer
Beschermingsgraad	IP 20	Conform DIN EN 60 529
Beschermingsklasse	II	Conform DIN EN 61 140
Isolatiecategorie	Overspanningscategorie	III conform DIN EN 60 664-1
	Vervuilingsgraad	2 conform DIN EN 60 664-1

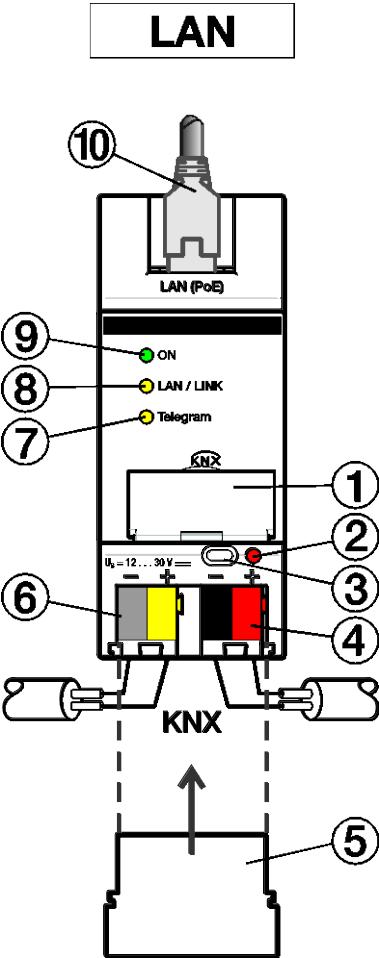
Lage KNX-veiligheidsspanning	SELV 30 V DC	
Temperatuurbereik	In bedrijf	-5 °C tot +45 °C
	Opslag	-25 °C tot +55 °C
	Transport	-25 °C tot +70 °C
Omgevingsvoorwaarde	Maximale luchtvochtigheid	95 %, geen bedauwing toegestaan
	Luchtdruk	atmosfeer tot 2.000 m
Design	DIN-railapparaat	modulair installatieapparaat, pro <i>M</i>
	Afmetingen	90 x 36 x 63,5 mm (h x b x d)
	Inbouwbreedte	2 modules à 18 mm
Montage	Op rail 35 mm	Conform DIN EN 60 715
Inbouwplaats	willekeurig	
Gewicht	0,1 kg	
Behuizing, kleur	Kunststof, halogeenvrij, grijs	
Certificering	KNX conform DIN EN 50491 en EN 60 669-2-5	
CE-markering	Conform EMC- en laagspanningsrichtlijnen	

Apparaattype	Applicatie	Maximaal aantal communicatieobjecten	Maximaal aantal groepsadressen	Maximaal aantal toewijzingen
IPR/S 3.5.1	IP-Router Secure/...*	0	0	0

* ... = Huidig versienummer van de applicatie. Raadpleeg hiervoor de software-informatie op onze homepage.

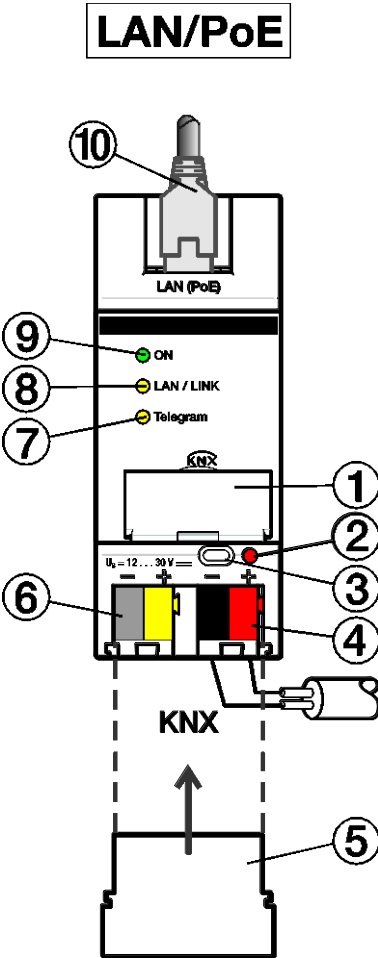
Opmerking
Voor de programmering zijn ETS 5 en het huidige applicatieprogramma van het apparaat vereist. Als het apparaat in de KNX Secure-modus moet worden gebruikt, dan is bovendien de ingebruiknamesleutel op het apparaat (FDSK, zie hoofdstuk 3.5, KNX Secure) vereist. De meest recente applicatie kunt u samen met de betreffende software-informatie van internet downloaden via www.abb.com/knx. Na de import in ETS is de applicatie in het venster Catalogi onder <i>Fabrikanten/ABB/Systeemapparaten/Koppelaars</i> opgeslagen. Het apparaat biedt geen ondersteuning voor de beveiligingsfunctie van een KNX-apparaat in ETS. Als u de toegang tot alle apparaten van het project via een <i>BCU-sleutel</i> blokkeert, is dit niet van invloed op dit apparaat. Het kan nog steeds worden uitgelezen en geprogrammeerd. Uitzondering: Wanneer de KNX Secure-modus is geactiveerd, kan er gaan andere ETS meer in het apparaat worden geprogrammeerd.

2.2 Aansluitschema



IPR/S 3.5.1

2CDC072009F0015



2CDC072010F0015

Legenda

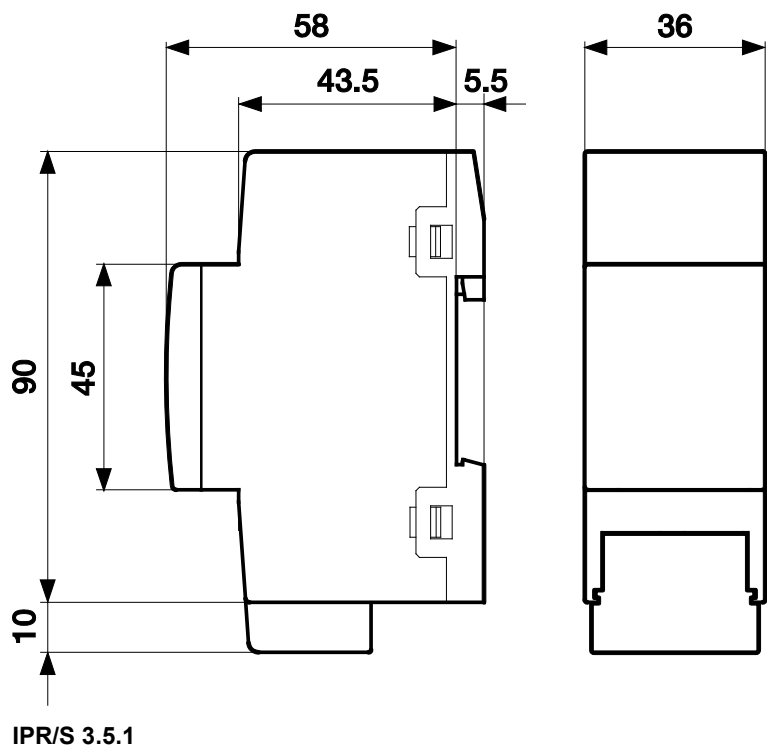
- 1 Labelhouder
- 2 LED *Programmeren*
- 3 Toets *Programmeren*
- 4 Aansluiting KNX
- 5 Deksel

- 6 Aansluiting voedingsspanning U_S
- 7 LED Telegram
- 8 LED LAN/LINK
- 9 LED ON
- 10 Aansluiting LAN of LAN/PoE

Opmerking

De router kan ook via de de-tuned spanningsuitgang van een ABB KNX-voeding (type SV/S) tegen voeding worden gelegd.

2.3 Afmetingen



2CDC072011F0015

2.4 Montage en installatie

Dit DIN-railapparaat is ontworpen voor inbouw in verdeelkasten met snelle bevestiging op 35-mm-rails volgens EN 60 715.

Het apparaat kan op elke inbouwpositie worden gemonteerd.

Voor de verbinding met de bus is een busaansluitklem meegeleverd. Het klemmenschema bevindt zich op de behuizing.

Het apparaat is klaar voor gebruik als de busspanning en de voedingsspanning zijn aangelegd.

Toegang tot het apparaat voor het bedienen, controleren, bekijken, onderhouden en repareren moet gegarandeerd zijn conform DIN VDE 0100-520.

2.4.1 Voorwaarde voor ingebruikname

Om het apparaat in gebruik te nemen, heeft u een pc met ETS 5 met de nieuwste versie en een voedingsspanning van 12 tot 30 V DC nodig. Ook kan de voeding via PoE (Power over Ethernet) volgens IEEE 802.3af klasse 1 verlopen.

Na inschakeling van de busspanning en de voedingsspanning is het apparaat klaar voor gebruik.

Montage en ingebruikname mogen alleen worden uitgevoerd door elektromonteurs. Bij de planning en inrichting van elektrische installaties en veiligheidsvoorzieningen tegen brand en inbraak moeten de relevante normen, richtlijnen, voorschriften en bepalingen van het betreffende land in acht worden genomen.

- Apparaat tijdens transport, opslag en bedrijf beschermen tegen vocht, verontreiniging en beschadiging!
- Apparaat alleen binnen de gespecificeerde technische gegevens gebruiken!
- Apparaat alleen in afgesloten behuizingen (verdeelkasten) gebruiken!
- Vóór montagewerkzaamheden moet het apparaat spanningsvrij worden geschakeld.



Gevaar

Om gevaarlijke elektrische schokken als gevolg van terugvoeding van verschillende fasegeleiders te voorkomen, moeten bij uitbreiding of wijziging van de elektrische aansluiting alle polen worden losgekoppeld.

2.4.2 Toestand bij levering

Het apparaat wordt geleverd met het fysieke adres 15.15.0.

Alle fysieke adressen voor de tunnelingverbindingen staan in de afleverttoestand 15.15.100, d.w.z. naar buiten toe is er slechts één tunnel te zien. Pas na de eerste download worden de adressen van de tunnelingverbindingen in de ETS worden overgenomen.

Het IP-adres is ingesteld op automatische toekenning (DHCP/AutoIP).

Opmerking

Het apparaat wordt af fabriek met de optie *Doorgeven* geleverd. Dat komt niet overeen met de standaardinstelling in de applicatie, maar maakt de ingebruikname wel gemakkelijker. Zie hoofdstuk 3.2.1, [Parametervenster KNX -> LAN](#).

Na de eerste download wordt dan de ingestelde instelling overgenomen.

2.4.3 Toekenning van het fysieke adres

Fysieke adressen en parameters worden toegekend en geprogrammeerd in ETS.

Voor de toekenning van het fysieke adres wordt de toets *Programmeren* gebruikt. Als deze toets wordt ingedrukt, gaat de rode LED *Programmeren* branden. De LED dooft zodra ETS het fysieke adres heeft toegekend of de toets *Programmeren* opnieuw wordt ingedrukt.

2.4.4 Downloaden

Het apparaat kan op verschillende manieren worden geprogrammeerd: via een van de geïntegreerde tunnelingsservers, via een lokale download, via KNXnet/IP-routing of via een extra programmeerinterface (USB of IP).

Opmerking

Als de programmering van een KNX Secure-apparaat via een USB-interface wordt gebruikt, moet deze "long frames" ondersteunen. Hiervoor is bijvoorbeeld de USB-interface USB/S 1.2 van ABB geschikt.

Om ervoor te zorgen dat het apparaat geprogrammeerd kan worden, moet een verbinding met KNX TP (Twisted Pair) bestaan.

Na een geslaagde download start het apparaat opnieuw op en worden alle open tunnelingverbindingen gesloten. Als bij het downloaden het IP-adres van het apparaat gewijzigd is, moeten de tunnelingverbindingen handmatig opnieuw worden geconfigureerd in de tunnelingclients. Tunnelingclients maken de verbinding van de server via het IP-adres mogelijk.

Het overnemen van de met ETS ingestelde gegevens gebeurt ca. 30-60 seconden na het downloaden.

2.4.5 Software van apparaat verwijderen en apparaat op fabrieksinstellingen resetten

Het apparaat kan op de fabrieksinstellingen worden gereset. Het gaat om een Secure-apparaat en daarom moet op het volgende worden gelet:

In de KNX Secure-modus kan het apparaat alleen via de ETS worden gereset, wanneer de ETS het project gebruikt waarmee de parametrisering van het apparaat werd uitgevoerd, of wanneer het project in de ingebruiknamesleutel is opgenomen.

De software kan van het apparaat worden verwijderd met een rechtsklik op het apparaat in de ETS.

Optie: Applicatie verwijderen

- Het IP-adres en de IP-configuratie blijven behouden.
- De unicast-configuratie blijft behouden, indien aanwezig.
- De wachtwoorden en IP-adressen van de tunnelingserver worden gewist.
- De sleutel voor de multicastcommunicatie ("Backbone Key") blijft behouden.
- De tool-sleutel die de ETS heeft uitgegeven blijft behouden, d.w.z. de FDSK is niet nodig voor de programmering.
- Het fysieke adres blijft behouden.

Optie: Fysiek adres en applicatie verwijderen

- Het apparaat wordt op de fabrieksinstellingen gereset.
- Voor een hernieuwde ingebruiknaam is de FDSK nodig, mits deze niet nog van de oorspronkelijke ingebruiknaam nog in het ETS-project is opgenomen.

De fabrieksinstellingen kunnen ook direct bij het apparaat worden gereset. Dit is geen veiligheidsrisico, omdat het apparaat aansluitend geen deel meer van de installatie uitmaakt.

- De programmeertoets indrukken bij een niet-verbonden KNX-bus
- Houd de programmeertoets ingedrukt en steek de busklem vast. De programmeer-led knippert (2 Hz).
- Druk de toets ten minste 5 s in en laat hem weer los. De programmeer-led dooft en het apparaat start op met de fabrieksinstellingen.

Als de ETS na het resetten verbinding met het apparaat maakt en de FDSK-sleutel van het apparaat is nog bekend in de ETS, dan kan de router opnieuw worden geprogrammeerd. De ETS geeft in dit geval aan dat het apparaat is gereset.

Zie hoofdstuk 3.5, [KNX Secure](#) voor meer aanwijzingen voor de FDSK (Factory Default Setup Key).

2.4.6 Reinigen

Vóór het reinigen moet het apparaat spanningsvrij worden geschakeld. Vervuilde apparaten kunnen worden schoongemaakt met een droge doek of een iets vochtige doek met wat zeepsop. Er mogen in geen geval bijtende middelen of oplosmiddelen worden gebruikt.

2.4.7 Onderhoud

Het apparaat is onderhoudsvrij. Bij schade, bijv. als gevolg van transport of opslag, mogen geen reparaties worden uitgevoerd.

2.5 Beschrijving van de in- en uitgangen

Ingang voedingsspanning 12 tot 30 V DC

Op de ingang voor de voedingsspanning mag uitsluitend een gelijkspanning van 12 tot 30 V worden aangesloten. Wij raden u aan de voedingseenheden NT/S uit ons assortiment te gebruiken.

De router kan ook via de de-tuned spanningsuitgang van een ABB KNX-voeding (type SV/S) tegen voeding worden gelegd.

Let op

De voedingsspanning moet 12 tot 30 V DC bedragen, of het apparaat moet worden gevoed via PoE (Power over Ethernet) volgens IEEE 802.3af Klasse 1.
Aansluiting op 230 V kan het apparaat beschadigen!

KNX-aansluiting

Voor aansluiting op de KNX-bus wordt de meegeleverde busaansluitklem gebruikt.

Opmerking

Voor de programmering is de nieuwste versie van de ETS 5 nodig.

LAN-aansluiting

De aansluiting op het netwerk gebeurt via een ethernet-RJ45-interface voor LAN-netwerken. De netwerkinterface kan met een overdrachtssnelheid van 10/100 Mbit/s worden uitgevoerd. De netwerkactiviteit wordt door de LED LAN/LINK op de voorkant van de behuizing aangegeven.

2.6 Bedieningselementen

Er bevinden zich geen bedieningselementen op de IP-router Secure.

2.7 Weergave-elementen

Aan de voorzijde van de IPR/S bevinden zich drie led's die het volgende aangeven:



AAN



LAN/LINK



Telegram

AAN

- De led brandt enkele seconden na het inschakelen van de voedingsspanning.
- De led brandt na het inschakelen van de voedingsspanning in eerste instantie permanent. Na circa 40 seconden gaat de led knipperen tot de opstartprocedure volledig is afgerond, waarna de led weer permanent brandt. Dit kan afhankelijk van de grootte van de filtertabel 5 tot 60 seconden duren.

LAN/LINK

- De led licht op als de voedingsspanning is ingeschakeld en de router op een ethernetnetwerk is aangesloten.
- De led knippert als het apparaat activiteit op het netwerk registreert, bijv. als er gegevens worden uitgewisseld.

Telegram

- De led brandt als de router op een TP-netwerk is aangesloten en het opstartproces (zie led "On") volledig is voltooid.
- De led knippert als het apparaat activiteit registreert op de KNX-sublijn TP1 (Twisted Pair 1), bijv. als er gegevens worden uitgewisseld.

3 Ingebruikname

De parameters van de IPR/S worden ingesteld via de applicatie en de Engineering Tool Software (ETS).

De applicatie is onder *Fabrikanten/ABB/Systeemapparaten/Koppelaars* te vinden.

Voor het instellen van parameters heeft u een pc of laptop met ETS nodig en een verbinding met de KNX-bus.

3.1 Overzicht

De parametreering van het IPR/S wordt uitgevoerd met de Engineering Tool Software (ETS 5 in de nieuwste versie).

Sommige functies (unicast) worden via een aparte tool (i-bus® Tool) ingesteld.

3.2 Parameters

In dit hoofdstuk worden de parameters van de IP-router Secure aan de hand van de parameterventers beschreven.

De parameterventers zijn dynamisch van opbouw, zodat afhankelijk van de parameterinstellingen en de functie van de uitgangen extra parameters of volledige parameterventers worden vrijgegeven.

De standaardwaarden van de parameters worden onderstreept weergegeven. Voorbeeld:

Opties: Ja
 Nee

3.2.1 Parametervenster *KNX -> LAN*

In het parametervenster *KNX -> LAN* kan de bewerking van telegrammen van het KNX-systeem naar het LAN-netwerk worden vastgelegd.

Opmerking

Het apparaat wordt af fabriek met de optie *Doorgeven* geleverd. Dat komt niet overeen met de standaardinstelling in de applicatie, maar maakt de ingebruikname wel gemakkelijker.

Na de eerste download wordt dan de ingestelde instelling overgenomen.

KNX->LAN	Groepstelegrammen hoofdgroepen 0...13	Filteren
LAN->KNX	Groepstelegrammen hoofdgroepen 14...31	Filteren
IP-instellingen	Fysiek geadresseerde telegrammen	☒ Filteren ☐ Blokkeren
	Broadcast-telegrammen	☒ Doorgeven ☐ Blokkeren
	Telegrambevestiging voor groepstelegrammen	☒ Alleen bij doorgeven ☐ Altijd
	Bij vrij groepsadres geldt:	
	hoofdgroep 0...13 => 1...28.671	
	hoofdgroep 14...31 => 28.672...65.535	
		<--- OPMERKING

Groepstelegrammen hoofdgroepen 0...13

Opties: Filteren
Doorgeven
Blokkeren

Deze parameter bepaalt of telegrammen met groepsadressen van de hoofdgroepen 0 t/m 13 moeten worden gefilterd, doorgegeven of geblokkeerd.

- *Filteren*: de telegrammen met groepsadressen van de hoofdgroepen 0 t/m 13 van KNX naar LAN worden gefilterd volgens de filtertabel, die automatisch wordt door de ETS wordt berekend.
- *Doorgeven*: alle groepstelegrammen van de hoofdgroepen 0 t/m 13 worden doorgegeven, zonder rekening te houden met de filtertabel.

Belangrijk

Deze instelling is alleen nuttig voor ingebruikname en diagnose. Bij normaal bedrijf moet hij niet worden gebruikt.
Omdat door deze instelling de KNX-lijnen overbelast kunnen raken, kan dit leiden tot telegramverlies.

- *Blokkeren*: alle groepstelegrammen van de hoofdgroepen 0 t/m 13 worden geblokkeerd, zonder rekening te houden met de filtertabel.

Groepstelegrammen hoofdgroepen 14...31

Opties: [Filteren](#)
Doorgeven
Blokkeren

Deze parameter bepaalt of telegrammen met groepsadressen van de hoofdgroepen 14 t/m 31 moeten worden gefilterd of geblokkeerd.

- *Filteren:* de telegrammen met groepsadressen van de hoofdgroepen 14 t/m 31 van KNX naar LAN worden gefilterd volgens de filtertabel, die automatisch wordt door de ETS wordt berekend.
- *Doorgeven:* alle groepstelegrammen van de hoofdgroepen 14 t/m 31 worden doorgegeven, zonder rekening te houden met de filtertabel.

Belangrijk
Deze instelling is alleen nuttig voor ingebruikname en diagnose. Bij normaal bedrijf moet hij niet worden gebruikt. Omdat door deze instelling de KNX-lijnen overbelast kunnen raken, kan dit leiden tot telegramverlies.

- *Blokkeren:* alle groepstelegrammen van de hoofdgroepen 14 t/m 31 worden geblokkeerd, zonder rekening te houden met de filtertabel.

Fysiek geadresseerde telegrammen

Opties: [Filteren](#)
Blokkeren

Deze parameter bepaalt of fysiek geadresseerde telegrammen moeten worden gefilterd of geblokkeerd.

- *Filteren:* er worden alleen telegrammen van KNX naar LAN overgebracht die de lijn van IPR/S naar LAN moeten verlaten.
- *Blokkeren:* fysiek geadresseerde telegrammen worden niet door de IPR/S bewerkt. Bij deze instelling is het niet mogelijk om fysiek geadresseerde telegrammen vanuit de lijn onder de IPR/S naar een andere lijn te verzenden, bijvoorbeeld tijdens het programmeren.

Broadcast-telegrammen

Opties: [Doorgeven](#)
Blokkeren

Deze parameter bepaalt of broadcast-telegrammen worden doorgegeven of geblokkeerd.

- *Doorgeven:* broadcast-telegrammen worden doorgegeven.
- *Blokkeren:* broadcast-telegrammen worden niet door de IPR/S bewerkt. Bij deze instelling is het niet mogelijk om broadcast-telegrammen vanuit de lijn onder de IPR/S naar een andere lijn te verzenden, bijvoorbeeld tijdens het programmeren.

De parameter *Broadcast-telegrammen* geldt ook voor "systeembroadcast-telegrammen". Voor details zie hoofdstuk 4.1.4, [Systeembroadcast](#).

Telegrambevestiging voor groepstelegrammen

Opties: Alleen bij doorgeven
Altijd

Deze parameter bepaalt of de IP-router Secure groepstelegrammen met een telegram moet bevestigen.

- *Alleen bij doorgeven*: de groepstelegrammen worden alleen bevestigd (ACK versturen) als ze door de IP-router Secure ook aan het LAN worden doorgegeven. Daardoor worden alleen telegrammen bevestigd die ook in de filtertabel van de IPR/S zijn ingevoerd.
- *Altijd*: alle groepstelegrammen op de KNX worden door de IPR/S bevestigd.

Bij vrij groepsadres geldt:

hoofdgroep 0...13 => 1...28.671

hoofdgroep 14...31 => 28.672...65.535

Opmerking
In de ETS 5 bestaat de mogelijkheid de groepsadressen niet in twee of drie fasen toe te kennen, maar vrij. Als de weergave Vrij groepsadres wordt gekozen, dan komt hoofdgroep 0-13 overeen met subgroepbereik 1-28.671 en hoofdgroep 14-31 met subgroepbereik 28.672-65.535. Details hierover kunt u nalezen in de Help van de ETS.

3.2.2

Parametervenster LAN -> KNX

In het parametervenster LAN -> KNX kan de bewerking van telegrammen van het LAN-netwerk naar het KNX-systeem worden vastgelegd.

KNX->LAN	Groepstelegrammen hoofdgroepen 0...13	Filteren
LAN->KNX	Groepstelegrammen hoofdgroepen 14...31	Filteren
IP-instellingen	Fysiek geadresseerde telegrammen	☒ Filteren ☐ Blokkeren
	Broadcast-telegrammen	☒ Doorgeven ☐ Blokkeren
	Bij overdrachtsfouten telegrammen herhalen	Ja
	Bij vrij groepsadres geldt:	
	hoofdgroep 0...13 => 1...28.671	
	hoofdgroep 14...31 => 28.672...65.535	

Groepstelegrammen hoofdgroepen 0...13

Opties: ☒ Filteren
☐ Doorgeven
☐ Blokkeren

Deze parameter bepaalt of telegrammen met groepsadressen van de hoofdgroepen 0 t/m 13 moeten worden gefilterd, doorgegeven of geblokkeerd.

- **Filteren:** de telegrammen met groepsadressen van de hoofdgroepen 0 t/m 13 van KNX naar LAN worden gefilterd volgens de filtertabel, die automatisch wordt door de ETS wordt berekend.
- **Doorgeven:** alle groepstelegrammen van de hoofdgroepen 0 t/m 13 worden doorgegeven, zonder rekening te houden met de filtertabel.

Belangrijk

Deze instelling is alleen nuttig voor ingebruikname en diagnose. Bij normaal bedrijf moet hij niet worden gebruikt.
Omdat door deze instelling de KNX-lijnen overbelast kunnen raken, kan dit leiden tot telegramverlies.

- **Blokkeren:** alle groepstelegrammen van de hoofdgroepen 0 t/m 13 worden geblokkeerd, zonder rekening te houden met de filtertabel.

Groepstelegrammen hoofdgroepen 14...31

Opties: Filteren
Doorgeven
Blokkeren

Deze parameter bepaalt of telegrammen met groepsadressen van de hoofdgroepen 14 t/m 31 moeten worden gefilterd of geblokkeerd.

- *Filteren*: de telegrammen met groepsadressen van de hoofdgroepen 14 t/m 31 van KNX naar LAN worden gefilterd volgens de filtertabel, die automatisch wordt door de ETS wordt berekend.
- *Doorgeven*: alle groepstelegrammen van de hoofdgroepen 14 t/m 31 worden doorgegeven, zonder rekening te houden met de filtertabel.

Belangrijk
Deze instelling is alleen nuttig voor ingebruikname en diagnose. Bij normaal bedrijf moet hij niet worden gebruikt. Omdat door deze instelling de KNX-lijnen overbelast kunnen raken, kan dit leiden tot telegramverlies.

- *Blokkeren*: alle groepstelegrammen van de hoofdgroepen 14 t/m 31 worden geblokkeerd, zonder rekening te houden met de filtertabel.

Fysiek geadresseerde telegrammen

Opties: Filteren
Blokkeren

Deze parameter bepaalt of fysiek geadresseerde telegrammen moeten worden gefilterd of geblokkeerd.

- *Filteren*: er worden alleen telegrammen van KNX naar LAN overgebracht die de lijn van IPR/S naar LAN moeten verlaten.
- *Blokkeren*: fysiek geadresseerde telegrammen worden niet door de IPR/S bewerkt. Bij deze instelling is het niet mogelijk om fysiek geadresseerde telegrammen vanuit de lijn onder de IPR/S naar een andere lijn te verzenden, bijvoorbeeld tijdens het programmeren.

Broadcast-telegrammen

Opties: Doorgeven
Blokkeren

Deze parameter bepaalt of broadcast-telegrammen worden doorgegeven of geblokkeerd.

- *Doorgeven*: broadcast-telegrammen worden doorgegeven.
- *Blokkeren*: broadcast-telegrammen worden niet door de IPR/S bewerkt. Bij deze instelling is het niet mogelijk om broadcast-telegrammen vanuit de lijn onder de IPR/S naar een andere lijn te verzenden, bijvoorbeeld tijdens het programmeren.

ABB i-bus® KNX

Ingebruikname

Bij overdrachtsfouten telegrammen herhalen

Opties: Ja
Nee
Door gebruiker gedefinieerd

- *Ja*: als bij de overdracht van een telegram een fout wordt vastgesteld, dan wordt het telegram maximaal drie keer herhaald.
- *Nee*: de overdracht wordt niet herhaald.
- *Door gebruiker gedefinieerd*: het gedrag kan voor verschillende soorten telegrammen apart worden ingesteld.

Als de optie *Door de gebruiker gedefinieerd* wordt geselecteerd, verschijnen de volgende parameters die hiervan afhankelijk zijn:

Groepsgeadresseerde telegrammen herhalen

Opties: Ja
Nee

- *Ja*: als bij de overdracht van een groepstelegram een fout wordt vastgesteld, dan wordt het telegram maximaal drie keer herhaald.
- *Nee*: de overdracht wordt niet herhaald.

Fysiek geadresseerde telegrammen herhalen

Opties: Ja
Nee

- *Ja*: als bij de overdracht van een fysiek geadresseerd telegram een fout wordt vastgesteld, dan wordt het telegram maximaal drie keer herhaald.
- *Nee*: de overdracht wordt niet herhaald.

Broadcast-telegrammen herhalen

Opties: Ja
Nee

- *Ja*: als bij de overdracht van een broadcast-telegram een fout wordt vastgesteld, dan wordt het telegram maximaal drie keer herhaald.
- *Nee*: de overdracht wordt niet herhaald.

Bij vrij groepsadres geldt:

hoofdgroep 0...13 => 1...28.671

hoofdgroep 14...31 => 28.672...65.535

Opmerking

In de ETS 5 bestaat de mogelijkheid de groepsadressen niet in twee of drie fasen toe te kennen, maar vrij. Als de weergave Vrij groepsadres wordt gekozen, dan komt hoofdgroep 0-13 overeen met subgroepbereik 1-28.671 en hoofdgroep 14-31 met subgroepbereik 28.672-65.535. Details hierover kunt u nalezen in de Help van de ETS.

3.2.3

Parametervenster *IP-instellingen*

In het parametervenster IP-instellingen wordt ingesteld hoe de IP-router Secure via IP communiceert.

KNX->LAN	IP-communicatiewijze	☒ Multicast ☐ Unicast
LAN->KNX	De instelling van apparaatnaam, IP-adres en tunnelingservers gebeurt in het eigenschappenvenster van ETS.	
IP-instellingen	<--- OPMERKING	

IP-communicatiewijze

Opties: Multicast
Unicast

De IP-communicatiewijze bepaalt welke soort telegrammen de IP-router naar het IP-netwerk verstuurt.

- *Multicast*: dit is de voor KNXnet/IP door de KNX Association vastgelegde communicatiewijze voor KNX-IP-apparaten. Deze instelling moet zo worden gehouden en mag alleen worden gewijzigd als door het beschikbare netwerk de noodzaak bestaat telegrammen als unicast te verzenden. Voor het instellen van het routing multicast-adres zie [Routing multicast-adres](#).
- *Unicast*: de routing voor dit apparaat wordt uitgeschakeld.

Deze speciale communicatie is niet volgens de KNXnet/IP-specificatie. Voor de configuratie is de ABB i-bus® Tool nodig.

De communicatiewijze *Unicast* kan niet worden gebruikt wanneer het apparaat in de KNX Secure-Modus staat. Als bij een geactiveerde KNX Secure-modus *Unicast* wordt geselecteerd, dan schakelt de ETS over op *Multicast*. De parametring *Unicast* in de applicatie wordt dan genegeerd.

Om de communicatiewijze *Unicast* te kunnen gebruiken, moet de KNX Secure-modus in de ETS worden uitgeschakeld.

Opmerking

Een beschrijving van de functies is in de online Help van de i-bus® Tools opgenomen.

ABB i-bus® KNX

Ingebruikname

Zowel bij de selectie van *Multicast* als bij die van *Unicast* verschijnt de volgende opmerking:

De instelling van apparaatnaam, IP-adres en tunnelingservers gebeurt in het eigenschappenvenster van ETS.

Als *Unicast* wordt geselecteerd, verschijnt tevens de volgende opmerking:

Let op! Deze instelling schakelt de routing voor dit apparaat uit. IP-telegrammen worden nu als unicast naar maximaal 9 doeladressen verstuurd.

De unicast-configuratie wordt uitgevoerd met de ABB i-bus® Tool.

Zie beschrijving *Communicatie unicast*, hoofdstuk 4.1.2, [KNX-telegrammen in het netwerk](#).

De i-bus® Tool kan gratis van onze homepage (www.abb.com/knx) worden gedownload.

Voor de i-bus® Tool is geen ETS en ook geen installatie van Falcon vereist.

De systeemvereisten zijn een Windows-systeem vanaf besturingssysteemversie Windows 7 (Service Pack 3) en .NET Framework vanaf versie 4.7.2.

Het geïntegreerde Falcon 5.0 ondersteunt alleen USB- en IP-interfaces (geen RS232).

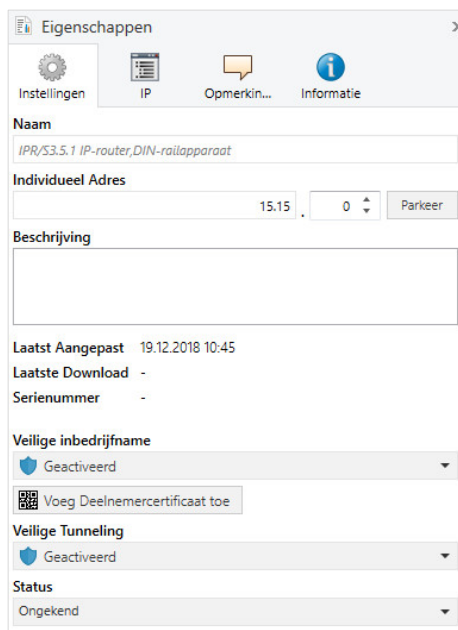
Opmerking
Een beschrijving van de functies is in de online Help van de i-bus® Tools opgenomen.

Belangrijk
De unicast-communicatie kan niet worden gebruikt als de KNX Secure-modus is geactiveerd. Als de KNX Secure-modus is geactiveerd en de parameter <i>IP-communicatiewijze</i> is ingesteld op <i>Unicast</i> , dan wordt toch de multicast-communicatie geactiveerd. Bij de parametring van de unicast-adressen via de i-bus® Tool wordt een passende opmerking getoond.

ABB i-bus® KNX

Ingebruikname

De verdere configuratie van de IP-parameters (apparaatnaam, toewijzing van het IP-adres per DHCP of vast) gebeurt in het eigenschappenvenster van de ETS.



Eigenschappen

Instellingen IP Opmerkin... Informatie

Naam
IPR/S3.5.1 IP-router, DIN-railapparaat

Individueel Adres
15.15 0 Parkeer

Beschrijving

Laatst Aangepast 19.12.2018 10:45
Laatste Download -
Serienummer -

Veilige inbedrijfname
Geactiveerd

Voeg Deelnemercertificaat toe

Veilige Tunneling
Geactiveerd

Status
Ongekend

In het eigenschappenvenster *Instellingen* kan de apparaatnaam worden ingevoerd. In het veld *Naam* kan de apparaatnaam, die in het apparaat wordt geladen, worden gewijzigd.

De apparaatnaam dient ter identificatie van het apparaat in het LAN. Bij een zoekopdracht, bijvoorbeeld door ETS, meldt elk KNXnet/IP-apparaat zijn naam en kan op basis daarvan worden toegewezen. Zo kan bijvoorbeeld door de naam IPR/S, EG, UV7 ook de inbouwlocatie van het apparaat worden meegedeeld.

Opmerking

Bij levering is de apparaatnaam standaard "IP-router Secure". Na de eerste download wordt de apparaatnaam die in het eigenschappenvenster van ETS wordt ingevoerd in het apparaat geladen.

Let op

Alleen de eerste 30 tekens van de apparaatnaam worden in het apparaat geladen, de rest wordt eraf gesneden.

ABB i-bus® KNX

Ingebruikname

In het eigenschappenvenster *IP* kan het IP-adres worden gedefinieerd.

Eigenschappen

Instellingen IP Opmerkin... Informatie

☐ Wijs een IP adres automatisch toe

☒ Een statisch IP-adres gebruiken

IP Adres
127.0.0.1

Subnet Mask
255.255.255.255

Standaard Gateway
127.0.0.1

MAC Adres
Ongekend

Multicast adres
224.0.23.12

Wachtwoord voor inbedrijfname
Wrrt,0Qz

Goed

Authenticatie Code
_eT3j_o>

Goed

Het IP-adres kan op de volgende manieren worden ingesteld:

Opties: Wijs een IP adres automatisch toe
Gebruik een vast IP-adres

- *Wijs een IP adres automatisch toe:* in de standaardinstelling verwacht de IP-router Secure dat een DHCP-server (Dynamic Host Configuration Protocol) een IP-adres toewijst. Deze server wijst op verzoek een vrij IP-adres toe aan het apparaat. Als in het netwerk geen DHCP-server beschikbaar is, dan start het apparaat een automatische IP-procedure. Het wijst zichzelf een adres toe uit het gereserveerde bereik van automatische IP-adressen (169.254.1.0 tot 196.254.254.255).
Voor DHCP zie hoofdstuk 4.1.1, [Toekenning van het IP-adres](#).
- *Gebruik een vast IP-adres:* als er geen DHCP-server in het netwerk geïnstalleerd is of als het IP-adres altijd hetzelfde moet zijn, dan kan ook een vast IP-adres worden toegewezen. Wanneer er een vast IP-adres wordt toegewezen, let er dan op dat elk apparaat zijn eigen IP-adres krijgt.

Opmerking

Het routing multicast-adres wordt hier alleen weergegeven.
Voor het instellen van het routing multicast-adres zie [Routing multicast-adres](#).

Opmerking

Het MAC-adres wordt na een download uitgelezen uit het apparaat.
Bovendien is het MAC-adres op het apparaat aangebracht en kan het als alternatief via de i-bus® Tool worden vastgesteld.

Opmerking

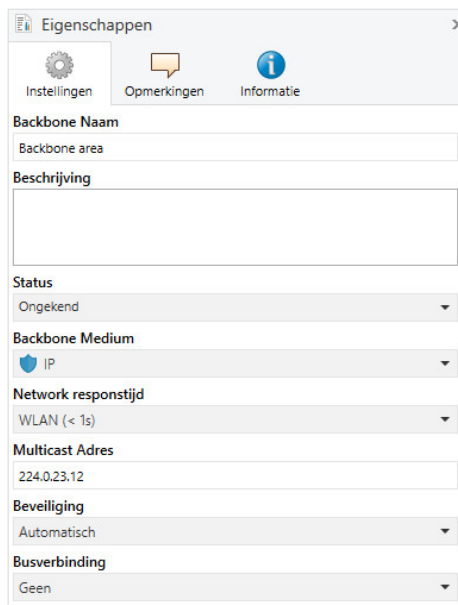
Een beschrijving van de functies is in de online Help van de i-bus® Tools opgenomen.

Routing multicast -adres (standaard = 224.0.23.12)

Opties: 224.0.23.12

Het routing multicast-adres legt het doeladres van IP-telegrammen van de IPR/S vast. Het van tevoren ingestelde adres 224.0.23.12 is het voor KNXnet/IP door de KNX Association samen met het IANA vastgelegde adres voor KNX-IP-apparaten. Dit adres moet zo worden gehouden en mag alleen worden gewijzigd als door het beschikbare netwerk de noodzaak bestaat een ander adres uit het bereik 224.0.0.0 tot 239.255.255.255 (gereserveerd bereik voor multicast-adressen) te gebruiken.

De instelling van het routing multicast-adres gebeurt in de ETS in de weergave *Topologie* (selecteer de topologie, dan kan in het eigenschappenvenster op het tabblad *Instellingen* het routing multicast-adres worden ingesteld):



Eigenschappen

Instellingen Opmerkingen Informatie

Backbone Naam
Backbone area

Beschrijving

Status
Ongekend

Backbone Medium
IP

Network responstijd
WLAN (< 1s)

Multicast Adres
224.0.23.12

Beveiliging
Automatisch

Busverbinding
Geen

Belangrijk

Alle IP-routers Secure of andere KNXnet/IP-apparaten die telegrammen uit moeten wisselen op het IP-netwerk, moeten hetzelfde routing multicast-adres gebruiken.

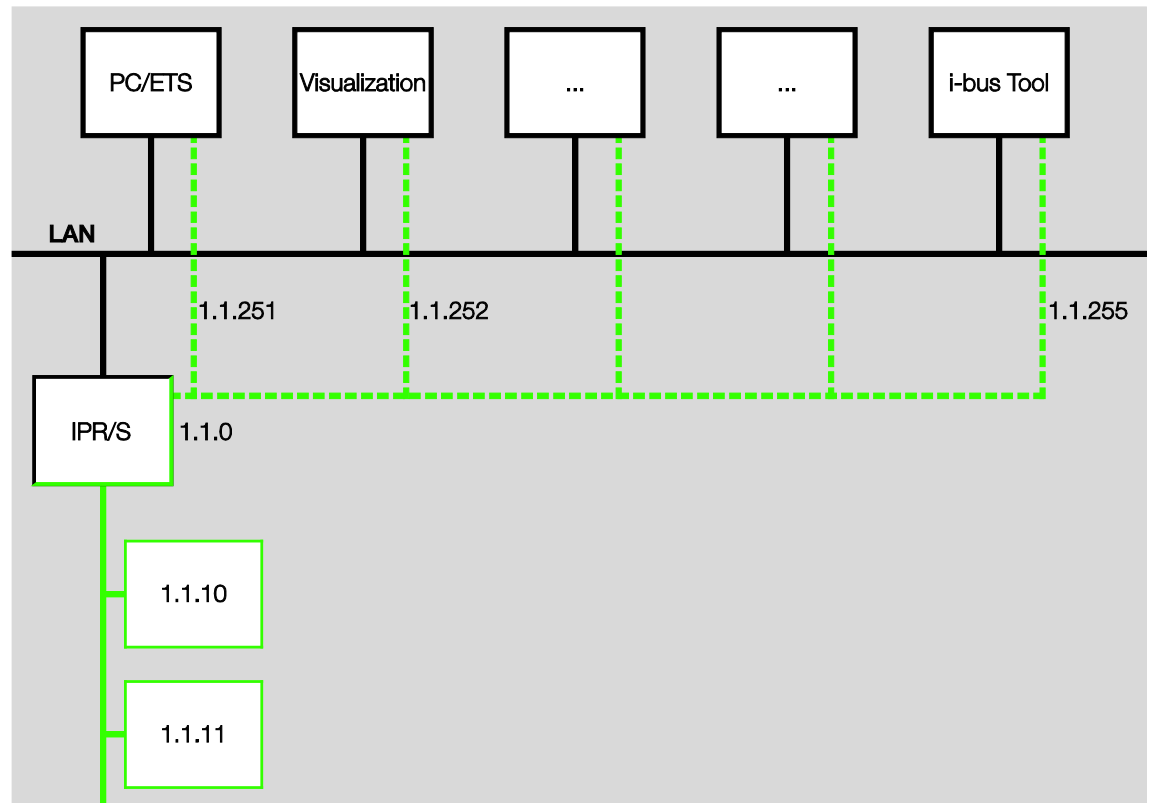
3.3 Communicatieobjecten

De IP-router Secure IPR/S heeft geen KNX-communicatieobjecten.

3.4

De geïntegreerde tunnelingservers gebruiken

De IP-router Secure biedt vijf extra fysieke adressen die kunnen worden gebruikt voor een tunnelingverbinding. Deze zogenaamde tunnelingservers kunnen met de ETS als programmeerinterface of met een andere client, bijvoorbeeld een visualisatie, worden gebruikt.



Bij tunneling maakt een client verbinding met een buslijn. Het tunnelingproces gebruikt UDP, maar bevat een andere beveiligingslaag, zodat bij fouten telegrammen herhaald worden.

Vanaf ETS 5 wordt tunneling V2 ondersteund. Hier wordt TCP gebruikt in plaats van UDP en wordt de beveiligingslaag van de TCP voor de overdracht gebruikt.

Opmerking

Het fysieke adres voor de tunnelingverbinding moet in de topologie passen. Daarom moeten de adressen uit het adressenbereik van de ondergeschikte lijn gekozen worden. Bij levering hebben alle tunnelingservers het adres 15.15.100.

Bij de ETS 5 worden de eerste vijf vrije adressen in de lijn automatisch toegewezen nadat de router in een lijn is ingevoegd.

De tunnelingservers kunnen ook met KNX Secure worden versleuteld. Als de KNX Secure-modus is geactiveerd, heeft een client het wachtwoord uit de ETS nodig.

Voor details zie hoofdstuk 3.5, [KNX Secure](#).

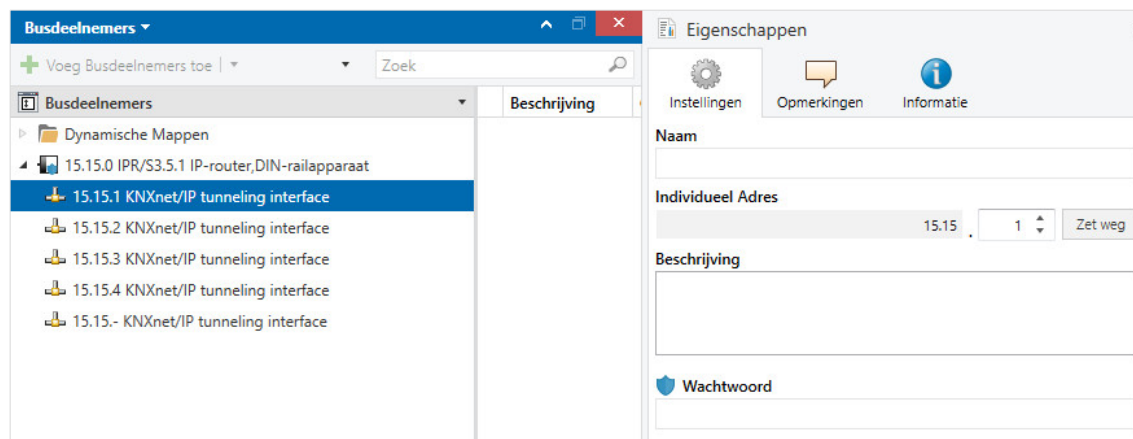
3.4.1 Instellingen in de ETS 5

In de ETS is voor de instelling van extra fysieke adressen een extra eigenschappenvenster beschikbaar.

De ETS reserveert automatisch na het invoegen van de router in de lijn de eerste vijf vrije adressen van deze lijn voor de tunnelingservers van de router. Dit is een eigenschap van ETS die niet kan worden gewijzigd.

Na de eerste download staan de adressen ter beschikking in het apparaat.

Als dit niet gewenst is, kan de instelling handmatig in het eigenschappenvenster worden veranderd.



Voor het wijzigen van het adres moet het actuele apparaatadres of het extra adres worden geselecteerd en moet met de pijltoetsen omhoog of omlaag het gewenste cijfer worden gekozen. Door een ander adres te selecteren wordt het gewijzigde adres opgeslagen.

De gewijzigde adressen worden pas na een download van het apparaat uitgevoerd.

Parkeren

Als voor een tunnel de optie *Parkeer* is geactiveerd, dan krijgt deze tunnel het adres 15.15.255.

Als bij alle tunnelingservers de optie *Parkeer* gekozen is, dan krijgen alle tunnelingservers het adres 15.15.255. Er is dan slechts één tunnelingserver beschikbaar.

3.5 KNX Secure

De ABB IP-router Secure is een KNX-apparaat conform de KNX Secure-standaard. Dat wil zeggen dat het apparaat veilig is in gebruik, dat de communicatie via de IP-backbone is beveiligd (alle KNX IP-apparaten moeten daarvoor het KNXnet/IP-beveiligingsprotocol ondersteunen) en de tunnelingverbindingen zijn versleuteld.

Bij de ingebruikname van het apparaat moet daarom op de volgende dingen worden gelet.

- Zodra er een KNX Secure-apparaat in een project wordt geïmporteerd, moet er een projectwachtwoord worden toegekend. Het project is op die manier tegen onbevoegde toegang beveiligd.
Het wachtwoord moet op een veilige plaats worden bewaard, want zonder dit wachtwoord is toegang tot het project niet mogelijk (ook niet door de KNX Association of door ABB)!
- Bij ingebruikname van een KNX Secure-apparaat (eerste download) is er een ingebruiknamesleutel nodig. Deze sleutel (FDSK = Factory Default Setup Key) is op een sticker aan de zijkant van het apparaat geplakt en moet voorafgaand aan de eerste download in de ETS worden geïmporteerd.
 - Bij de eerste download van het apparaat verschijnt er een venster in de ETS, waarin om invoer van de sleutel wordt gevraagd. Het certificaat ook met een QR-scanner worden ingelezen (aanbevolen methode).
 - Of de certificaten van alle Secure-apparaten worden eerst in de ETS ingevoerd. Dit wordt gedaan via de projectoverzichtspagina op het tabblad "Beveiliging".
 - Er zijn twee FDSK-stickers op het apparaat geplakt. Eén exemplaar kan voor de projectdocumentatie worden gebruikt, de andere kan op het apparaat blijven.
Zonder de FDSK kan het apparaat na een reset niet meer in de KNX Secure-modus worden gebruikt.

De FDSK is alleen bij de eerste ingebruikname nodig. Daarna wijst de ETS nieuwe sleutels toe. De FDSK is pas weer nodig wanneer het apparaat op de fabrieksinstellingen is gereset (bijvoorbeeld wanneer het apparaat in een andere installatie met een ander ETS-project moet worden gebruikt).

De ETS kent aan alle KNX IP Secure-apparaten van het project de backbone-sleutel toe en stelt voor elke tunnelingserver een ander wachtwoord op. De wachtwoorden kunnen indien gewenst worden veranderd. De sleutels worden door de ETS opgesteld en beheerd. Indien nodig kunnen de sleutels en wachtwoorden worden geëxporteerd (bijvoorbeeld wanneer een client toegang tot een tunnel wil).

Indien nodig, kan de router weer op de fabrieksinstellingen worden gereset; zie hoofdstuk 2.4.5, [Software van apparaat verwijderen en apparaat op fabrieksinstellingen resetten](#).

4 Ontwerp en toepassing

4.1 De IP-router Secure in het netwerk

De IP-router Secure is bedoeld voor gebruik in 10/100 BaseT-netwerken volgens IEEE 802.3. Het apparaat bezit een AutoSensing-functie en stelt de overdrachtssnelheid (10 of 100 Mbit) automatisch in.

4.1.1 Toekenning van het IP-adres

DHCP/AutoIP

Het IP-adres van het apparaat kan van een DHCP-server verkregen worden. Daarvoor moeten IP-adressen in de ETS automatisch worden toegekend; zie parametervenster [IP-instellingen](#). Als bij deze instelling geen DHCP-server wordt gevonden, dan start het apparaat een AutoIP-procedure en kent het zelfstandig een IP-adres uit het bereik 169.254.xxx.yyy toe.

Het IP-adres dat het apparaat bij het starten toegewezen krijgt (per DHCP of AutoIP), wordt gebruikt tot

- de volgende herstart (uit-/inschakelen of nieuwe programmering)
- er een DHCP-server beschikbaar is
- de DHCP-lease is verlopen

Bij het starten is geen DHCP-server beschikbaar

Als bij het starten van de IP-router Secure geen DHCP-server beschikbaar is, dan geeft het apparaat zichzelf een AutoIP-adres. De router zoekt dan cyclisch (3 telegrammen met een tussenafstand van 3 seconden, aansluitend 20 seconden pauze) naar een DHCP-server. Zodra weer een server beschikbaar is, wordt het door de DHCP-server toegewezen adres gebruikt.

DHCP-server valt uit (apparaat heeft IP-adres al van DHCP verkregen)

Tot het einde van de leasetijd (geldigheidsduur van het IP-adres, wordt bij toekenning van het IP-adres door de DHCP-server vastgelegd) lopen de aanvragen voor verlenging van de gebruiksrechten van dit IP-adres dood. Het IP-adres wordt verder gebruikt.

Aan het einde van de leasetijd of na een download zoekt het apparaat een AutoIP-adres.

Vast IP-adres

Als het IP-adres van de IPR/S vast is toegewezen, dan kan in de ETS een vast IP-adres (en een subnetmasker en standaardgateway) worden ingesteld, zie parametervenster [IP-instellingen](#).

ABB i-bus® KNX

Ontwerp en toepassing

4.1.2

KNX-telegrammen in het netwerk

Opmerking

Bij het uitrollen van het KNX-systeem moet erop worden gelet dat het aantal overgebrachte telegrammen ook bij gebruik van de IP-router Secure beperkt is. Door de hoge overdrachtssnelheid aan de IP-zijde (10/100 Mbit/s) kunnen bij hogere hoeveelheden gegevens, afhankelijk van het systeem, in de TP1-lijn (9,6 kbit/s) telegrammen verloren gaan.

Multicast

Multicasten is de communicatie van een zender met een groep ontvangers. De IP-router Secure verstuurt de KNX-telegrammen verpakt als UDP/IP-telegrammen naar het IP-netwerk. Alle IP-routers Secure waarbij hetzelfde multicast-adres is ingesteld, ontvangen dit telegram en evalueren het. Als een telegram voor de bijbehorende sublijn bestemd is, routeert de IP-router Secure het telegram in de lijn, anders wordt het verworpen.

De IP-router Secure verstuurt telegrammen vanuit de KNX naar het IP-netwerk volgens de KNXnet/IP-protocolspecificatie. Deze telegrammen worden in de standaardinstelling als multicast-telegrammen naar het multicast-IP-adres 224.0.23.12 poort 3671 gestuurd. Dit multicast-IP-adres is het voor KNXnet/IP door de KNX Association samen met het IANA vastgelegde adres voor KNX-IP-apparaten. Dit adres moet zo worden gehouden en mag alleen worden gewijzigd als door het beschikbare netwerk de noodzaak bestaat een ander adres te gebruiken.

Om ervoor te zorgen dat meerdere IP-routers Secure in het netwerk met elkaar kunnen communiceren, moeten tussen de apparaten multicast-communicatie mogelijk zijn. Afhankelijk van het soort netwerk en de instelling van de gebruikte netwerkcomponenten, bijvoorbeeld router, switch of firewall, moet het multicast-IP-adres 224.0.23.12 eventueel eerst nog expliciet vrijgeschakeld worden. Neem hiervoor contact op met de netwerkbeheerder.

Voor verdere informatie zie hoofdstuk 3.2.3, [Parametervenster IP-instellingen](#).

Unicast

Unicasten betekent in het algemeen de communicatie tussen één verzender en één ontvanger. De router maakt dus voor elke IP-router binnen de unicast-groep een communicatieverbinding.

Als in een netwerk geen multicast-communicatie mogelijk is, kunnen de ABB IP-routers ook via unicast met elkaar communiceren. Er kunnen maximaal tien ABB IP-routers tot een unicast-groep worden samengevoegd. De unicast-groep kan bestaan uit IPR/S 3.1.1 of uit IPR/S 3.5.1 of uit een combinatie van beide. Elke router krijgt dan negen IP-adressen toegewezen, waaraan hij zijn telegrammen verstuurt.

De configuratie van deze unicast-groep gebeurt eenvoudig en automatisch met de ABB i-bus® Tool.

Het is ook mogelijk een client (bijvoorbeeld een visualisering) aan deze unicast-groep te koppelen. In dit geval is een van de tien unicast-adressen bezet door de client en kunnen er nog negen IP-routers Secure worden gekoppeld.

De exacte beschrijving over hoe de configuratie met de i-bus® Tool werkt, staat in de Help van de i-bus® Tools (zie hoofdstuk 4.2, [De i-bus® Tool](#)).

Opmerking

Zodra in de ETS onder IP-communicatiewijze de parameter wordt omgezet op *Unicast*, wordt de functie *Multicast* gedeactiveerd. De apparaten kunnen dan niet meer via de multicast-routing, maar alleen nog via een van de geïntegreerde tunnelingservers of een aparte programmeerinterface worden geprogrammeerd.

De communicatiewijze wordt echter pas veranderd wanneer de parametrering met de i-bus® Tool is uitgevoerd. Tot dan staat de router intern nog op Multicast. Dit heeft het voordeel dat de router via Multicast kan worden geprogrammeerd.

Voor verdere informatie zie het parametervenster [IP-instellingen](#).

ABB i-bus® KNX

Ontwerp en toepassing

Opmerking

Een beschrijving van de functies is in de online Help van de i-bus® Tools opgenomen.

Opmerking

- Bij het gebruik van de communicatiewijze Unicast moet ervoor worden gezorgd dat het IP-adres van de router tijdens het gebruik niet wijzigt. Daarom moet ofwel een vast IP-adres worden toegewezen, ofwel moet een overeenkomstige instelling in de DHCP-server worden uitgevoerd.
- De ETS updatet eveneens alle IP-parameters wanneer het fysieke adres wordt gewijzigd. Dus ook als alleen de optie *Programmerenfysiek adres* in de ETS wordt gekozen, worden de apparaatnaam, het multicast-adres, de IP-communicatiewijze (DHCP, AutoIP, vast), het IP-adres, het subnetmasker, de standaardgateway en alle tunnelingadressen opnieuw geladen. Als het IP-adres dan verandert, moet de unicast-configuratie met de i-bus® Tool opnieuw worden uitgevoerd.

De communicatiewijze *Unicast* kan niet worden gebruikt wanneer het apparaat in de KNX Secure-Modus staat. Als bij een geactiveerde KNX Secure-modus *Unicast* wordt geselecteerd, dan schakelt de ETS over op *Multicast*. De parametrisering *Unicast* in de applicatie wordt dan genegeerd.

Om de communicatiewijze *Unicast* te kunnen gebruiken, moet de KNX Secure-modus in de ETS worden uitgeschakeld.

4.1.3

Een IPR/S 3.5.1 bewaken

Een tunnelingverbinding moet bij een actieve tunnelingverbinding via een "CONNECTIONSTATE_REQUEST" worden bewaakt. Dit is echter ook via T-Connect mogelijk.

Als een apparaat via T-Connect wordt bewaakt, kan dat nadelen hebben, bijvoorbeeld bij bewakings-, programmerings- of scanprocedures in de lijn.

4.1.4

Systeembroadcast

Binnen een KNX-installatie moeten alle IP-apparaten die met elkaar willen communiceren, hetzelfde multicast-adres gebruiken. Standaard wordt hiervoor het adres 224.0.23.12 Port 3671 gebruikt; zie [Multicast](#).

Als in een installatie het multicast-adres wordt gewijzigd, kunnen er bij de ingebruikname mogelijk problemen ontstaan. Als bijvoorbeeld eerst het multicast-adres van de dichtstbijzijnde router gewijzigd, dan schakelt deze na de programmering op het nieuwe multicast-adres over. Hij kan de rest van de installatie dan niet meer bereiken en de overige routers in de installatie kunnen niet meer worden geprogrammeerd.

De ETS kan deze apparaten dan via het "systeembroadcastadres" bereiken. Via het systeembroadcastadres kan het multicast-adres van alle KNX IP-apparaten en ook de backbone-sleutel worden gewijzigd. Dit is alleen mogelijk wanneer het apparaat of niet in de KNX Secure-modus wordt gebruikt of wanneer de ETS de backbone-sleutel kent.

Het doorgeven van systeembroadcasttelegrammen kan dan via de parameter *Broadcasttelegrammen doorgeven/blokken* worden ingesteld, d.w.z. deze parameter doelt op (standaard) broadcasttelegrammen en systeembroadcasttelegrammen.

4.1.5

IGMP

Het apparaat ondersteunt IGMP snooping in versie V3.

IGMP snooping verwijst naar de mogelijkheid om multicast routing-verkeer alleen daarheen door te geven waar het nodig is. De IT-infrastructuur en het apparaat moeten dezelfde IGMP-versie gebruiken, omdat anders het IGMP-mechanisme niet werkt.

Als er een multicast-adres moet worden vrijgeschakeld, meldt het apparaat zich met een lidmaatschapsrapport bij dit multicast-adres aan.

4.1.6

IPR/S als zonekoppelaar

De IP-router Secure kan in KNX-installaties de functie van een zonekoppelaar overnemen. Daarvoor moet hij het fysieke zonekoppelaar (1.0.0...15.0.0) krijgen. In een ETS-project kunnen maximaal 15 zonekoppelaars worden aangemaakt.

De volgende afbeelding toont deze topologie met IP-routers zonekoppelaars en KNX-lijnkoppelaars (LK/S).

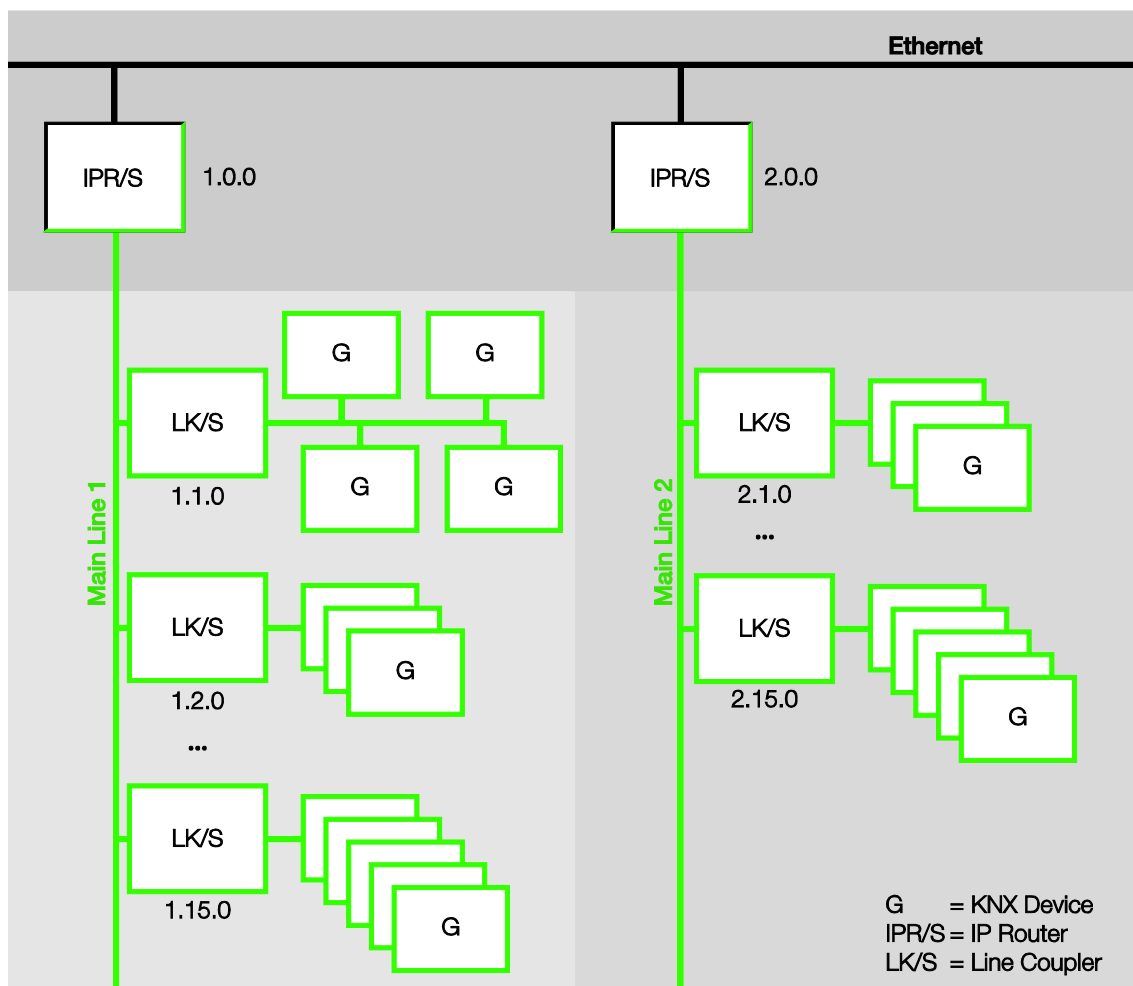


ABB i-bus® KNX

Ontwerp en toepassing

4.1.7

IPR/S als lijnkoppelaar

De IP-router Secure kan in KNX-installaties de functie van een lijnkoppelaar overnemen. Daarvoor moet hij het fysieke adres van een lijnkoppelaar (1.1.0...15.15.0) krijgen.

De volgende afbeelding toont deze topologie met IP-routers Secure als lijnkoppelaars.

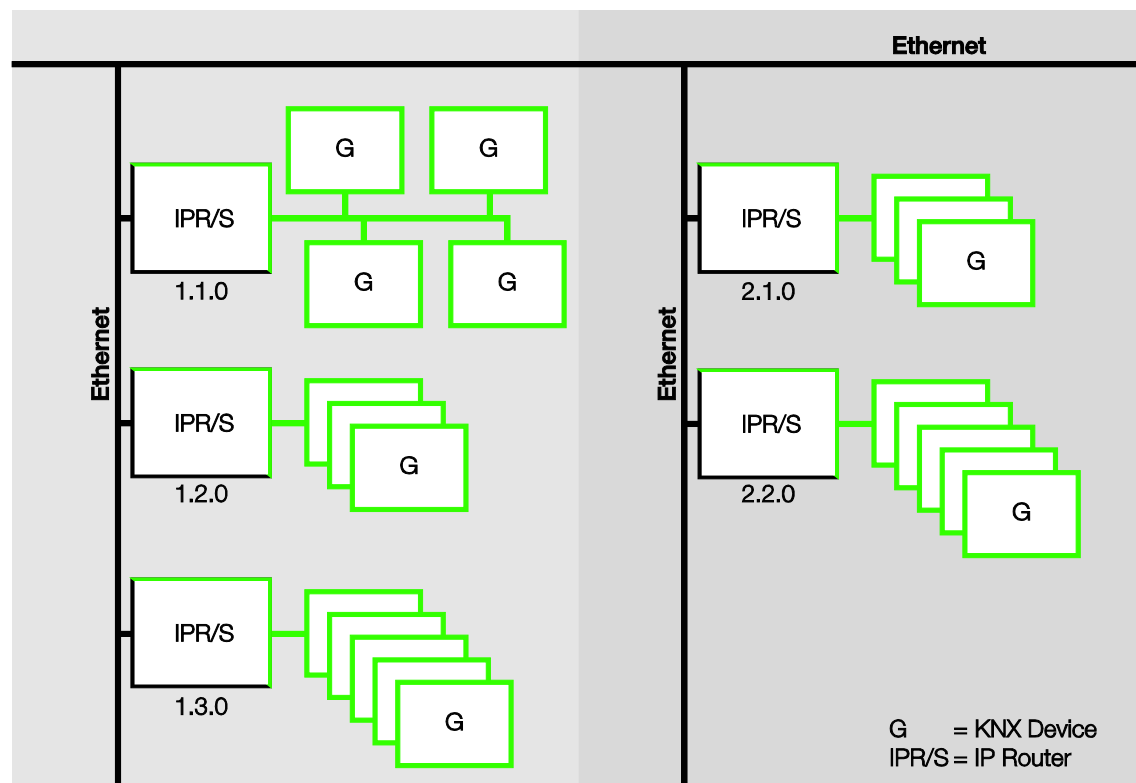


ABB i-bus® KNX

Ontwerp en toepassing

4.1.8

Gemengde topologie

Als het binnen een KNX-installatie nodig is de IP-router Secure op de ene locatie, bijvoorbeeld kantoor, als zonekoppelaar en op de andere locatie, bijvoorbeeld ondergrondse parkeergarage, als lijnkoppelaar te gebruiken, dan is dit mogelijk.

Daarbij moet er alleen op worden gelet dat de IP-router als lijnkoppelaar het lijnkoppelaaradres uit een vrij bereik gebruikt, bijvoorbeeld hier in afbeelding 2.1.0.

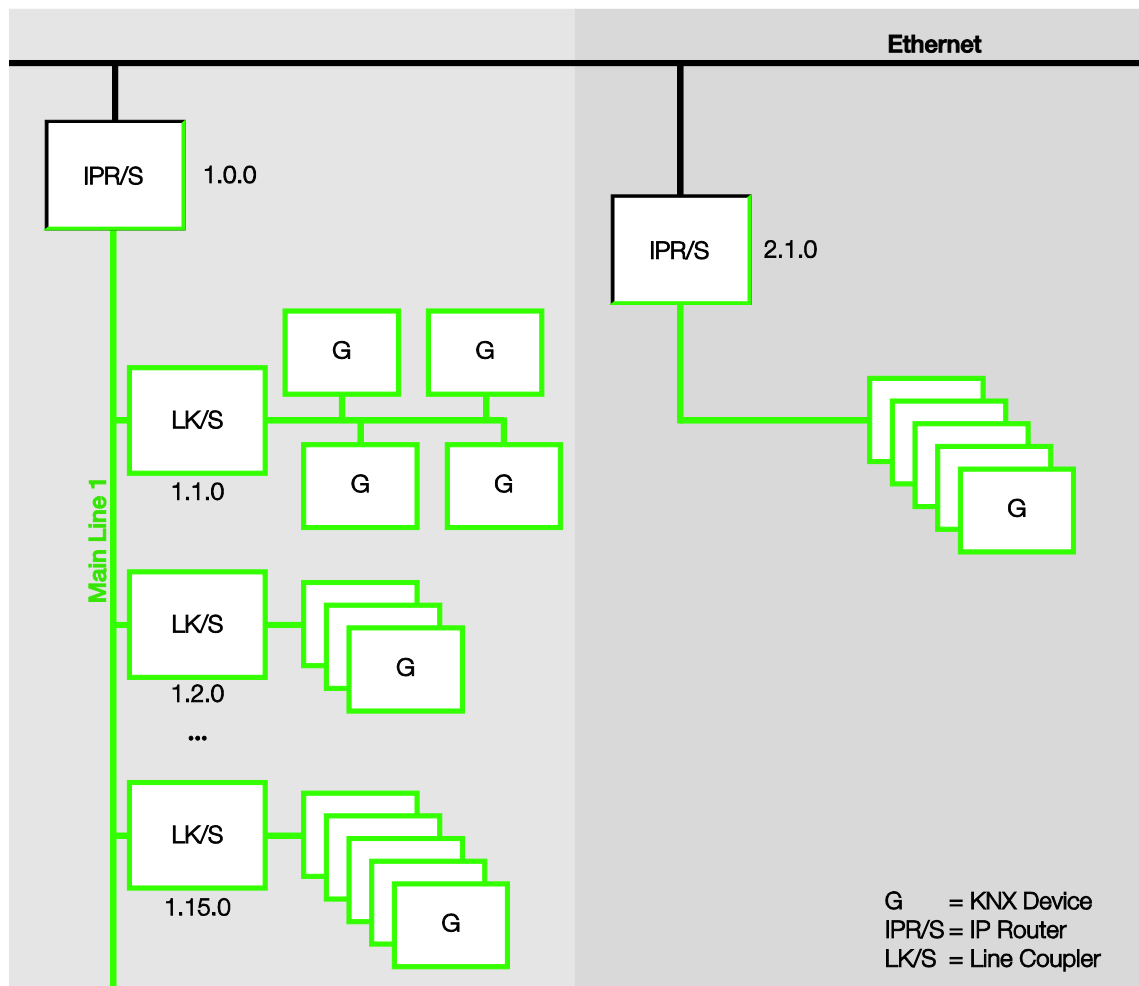


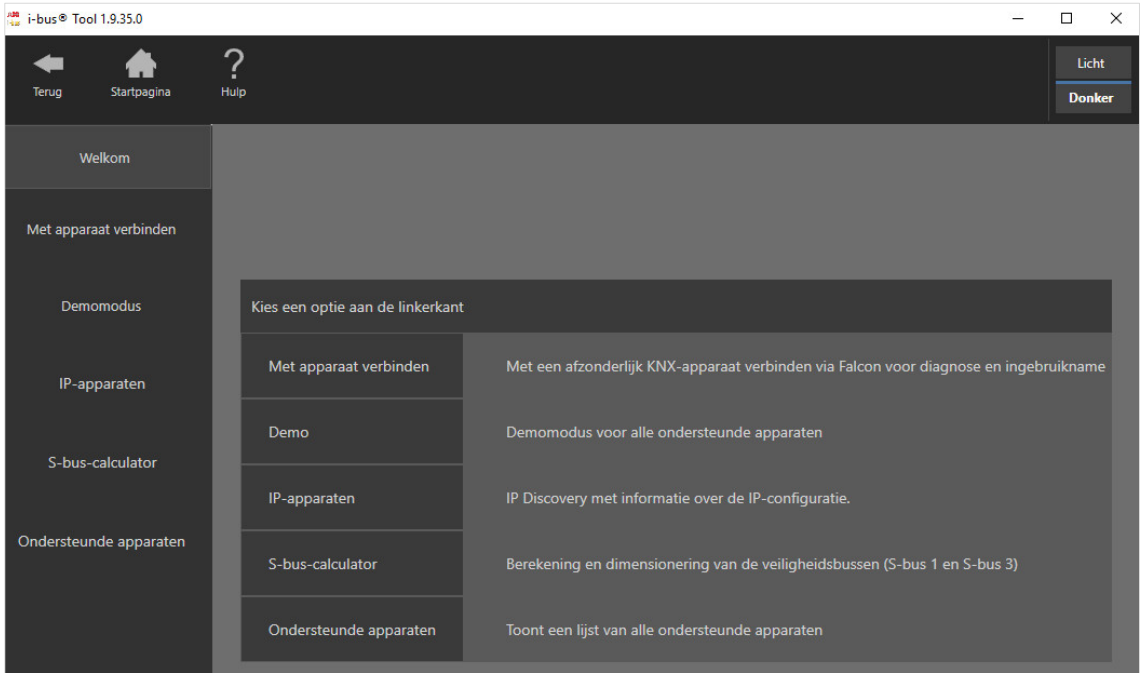
ABB i-bus® KNX

Ontwerp en toepassing

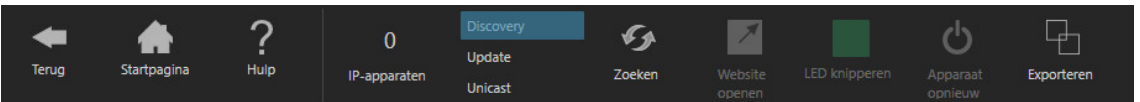
4.2 De i-bus® Tool

De ABB i-bus® Tool wordt gebruikt om bepaalde functies bij de ABB IP-apparaten in te stellen. Het maakt de ingebruikname aan de IP-zijde gemakkelijker.

Klik op de startzijde van de i-bus® Tools op *Verbinden*, in het volgende venster dan op *IP-apparaten*.



Werkbalk: omschakelen tussen Discovery, Firmware-update en Unicast



Klik op de betreffende knop om de modus *Discovery* of *Unicast* te selecteren.

4.2.1 Discovery

Kies in de werkbalk de modus *Discovery*. Deze functie dient voor het zoeken en weergeven van ABB IP-apparaten in het netwerk. Als de IP-router in de KNX Secure-modus wordt gebruikt, wordt niet alle informatie getoond.

Opmerking
Een beschrijving van de functies is in de online Help van de i-bus® Tool opgenomen.

ABB i-bus® KNX

Ontwerp en toepassing

4.2.2

Firmware-update

In de KNX Secure-modus kan het apparaat niet met de i-bus® Tool worden geüpdatet. De firmware-update kan in dit geval alleen met de ETS-app "ABB KNX Bus Update" worden uitgevoerd, die gratis in de KNX online shop kan worden gedownload.

Kies in de werkbalk de modus *Update*. Als het een keer nodig is, kan met deze functie de firmware worden bijgewerkt.

Belangrijk

De firmware moet van tevoren van internet worden gedownload (www.abb.com/knx). Daarvoor maakt de i-bus® Tool **bij een bestaande internetverbinding** verbinding met een server.

Voor het actualiseren van de apparaten op de installatie is dan geen internetverbinding meer nodig.

Belangrijk

Tijdens het updaten moet naast het IP-netwerk (LAN) ook de KNX-bus (TP) aangesloten zijn, zodat de KNX-parameters correct opnieuw kunnen worden ingesteld. Anders mislukt het updaten.

Tijdens het update mag de voeding niet wegvallen (KNX of IP), omdat het apparaat dan kan worden vernield.

Opmerking

Een beschrijving van de functies is in de online Help van de i-bus® Tool opgenomen.

Opmerking

Voor het updaten moet aan de i-bus® Tool beheerdersrechten worden toegekend.

Unicast

Kies in de werkbalk de modus *Unicast*.

Deze functie is alleen beschikbaar als eerder in de ETS-applicatie de parameter [*IP-communicatiewijze*](#) op *Unicast* is omgezet.

Opmerking

Een beschrijving van de functies is in de online Help van de i-bus® Tool opgenomen.

A Bijlage

A.1 Bestelgegevens

Apparaattype	Productnaam	Productnummer	bbn 40 16779 EAN	Gew. 1 st. [kg]	Verp.eenh. [st.]
IPR/S 3.5.1	IP-router Secure, DIN-railapparaat	2CDG110176R0011	90650 0	0,1	1

A.2 Opensourcecomponenten

Onder de volgende link staat een lijst van de gebruikte opensourcecomponenten:

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



ABB STOTZ-KONTAKT GmbH
Eppelheimer Straße 82
D-69123 Heidelberg, Duitsland
Telefoon: +49 (0)6221 701 607
Fax: +49 (0)6221 701 724
E-mail: knx.marketing@de.abb.com

Meer informatie en regionale contactpersonen
www.abb.com/knx

© Copyright 2019 ABB. Technische wijzigingen aan de producten, alsmede wijzigingen in de inhoud van dit document, zijn ons te allen tijde zonder voorafgaande kennisgeving voorbehouden. Bij bestellingen zijn de overeengekomen voorwaarden en bepalingen altijd van toepassing.
ABB AG is niet verantwoordelijk voor eventuele fouten of onjuistheden in dit document.
Alle rechten ten aanzien van dit document en de hierin opgenomen onderwerpen en afbeeldingen zijn voorbehouden.
Verveelvoudiging, bekendmaking aan derden of commercieel gebruik van de inhoud – ook gedeeltelijk – is niet toegestaan zonder voorafgaande schriftelijke toestemming van ABB AG.