enertexbayern gmbh
simulation entwicklung consulting

Handbuch und Konfiguration

Enertex® KNX IP Secure Interface

Enertex® Bayern GmbH – Ebermannstädter Straße 8 - 91301 Forchheim - Deutschland - mail@enertex.de

Hinweis

Der Inhalt dieses Dokuments darf ohne vorherige schriftliche Genehmigung durch die Enertex® Bayern GmbH in keiner Form, weder ganz noch teilweise, vervielfältigt, weitergegeben, verbreitet werden.

Enertex® ist eine eingetragene Marke der Enertex® Bayern GmbH. Andere in diesem Handbuch erwähnte Produkt- und Firmennamen können Marken- oder Handelsnamen ihrer jeweiligen Eigentümer sein.

Dieses Handbuch kann ohne Benachrichtigung oder Ankündigung geändert werden und erhebt keinen Anspruch auf Vollständigkeit oder Korrektheit.

Inhalt

Sicherheitshinweise

- Einbau und Montage elektrischer Geräte darf nur durch Elektrofachkräfte erfolgen.
- Beim Anschluss von KNX IP Secure Schnittstellen werden Fachkenntnisse durch KNX™-Schulungen vorausgesetzt.
- Bei Nichtbeachtung der Anleitung können Schäden am Gerät, sowie ein Brand oder andere Gefahren entstehen.
- Diese Anleitung ist Bestandteil des Produkts und muss beim Endanwender verbleiben.
- Der Hersteller haftet nicht für Kosten oder Schäden, die dem Benutzer oder Dritten durch den Einsatz dieses Gerätes, Missbrauch oder Störungen des Anschlusses, Störungen des Gerätes oder der Teilnehmergeräte entstehen.
- Das Öffnen des Gehäuses, andere eigenmächtige Veränderungen und / oder Umbauten am Gerät führen zum Erlöschen der Gewährleistung!
- Für eine nicht bestimmungsgemäße Verwendung haftet der Hersteller nicht.

Montage und Anschluss

Für den Betrieb des Enertex® KNX IP Secure Interfaces wird benötigt:

- Eine 10/100 Mbit kompatible Ethernetverbindung
- Eine KNX/EIB Busverbindung

Inbetriebnahme

Boot

Beim Einschalten zeigt das Display den Produktnamen an. Voreinstellung für das Netzwerk ist DHCP.

Die Bootzeit beträgt ca. 2 Sekunden. Währen dieser Zeit laufen die grüne/rote/gelbe LED als Lauflicht kurz los. Am Ende des Bootvorgangs wird die IP Adresse des Geräts im Display angezeigt.

Sollte die IP-Adressvergabe über DHCP-Server erfolgen, verlängert sich die Bootzeit entsprechend.

Alsbald im Display „KNX Ready“ erscheint, kann das Gerät über den Bus angesprochen und z.B. alternativ über eine USB Schnittstelle programmiert werden.

Die grüne LED blinkt im Sekundentakt mit einem Tastverhältnis 1:30.

Anzeigen

Nach einer Minute schaltet sich das Display automatisch aus. Um dieses wieder einzuschalten, muss die DISPLAY Taste auf der Gerätefront kurz betätigt werden.

Bei eingeschaltetem Display wird durch Betätigen der DISPLAY Taste ein Durchblättern von verschiedenen Informationsseiten ausgelöst.

Seite 1 zeigt die Firmware-Version, IP Adresse, Physikalische Adresse, Seriennummer, die Busspannung und genutzte Tunnelverbindungen

Seite 2 zeigt sämtliche IP Einstellungen, sowie die Bootzeit.

Seite 3 gibt Informationen zur Telegrammlast aus.

Seite 4 zeigt den FDSK, solange das Gerät nicht in den Secure – Zustand gesetzt wurde.

Auf der Frontseite befinden sich drei LEDs. Die grüne LED blinkt im Sekundentakt mit einem Tastverhältnis 1:30 und zeigt Betriebsbereitschaft an. Die rote LED dient zur Anzeige des Programmiermodus, die gelbe LED zeigt Busaktivität.

In der LAN Buchse sind zwei weitere LEDs verbaut. Die grüne zeigt eine Verbindung zu einem anderen IP Gerät oder Switch an („Link“), die gelbe LED zeigt den IP Datentransfer.

Reset

Wenn das Gerät in den Auslieferungszustand zurücksetzt werden soll, muss die PROG-Taste auf der Frontseite für 10 Sekunden gedrückt werden. Nach Ablauf dieser Zeit fängt die rote LED zu blinken an - dann kann die PROG-Taste losgelassen werden und das Gerät führt den Reset in den Auslieferungszustand durch.

Funktionsübersicht

Das Gerät weist folgende Funktionalitäten auf:

- KNX IP Secure
  - Acht unabhängige KNXnet/IP-Tunnelverbindungen
  - Kommunikation über TCP oder UDP
  - KNX IP Tunnelling im verschlüsselten (Secure) Modus.
- Anzeigen
  - LED-Anzeigen für KNX-Kommunikation, Ethernet-Kommunikation und Programmiermodus
  - Betriebsanzeige
  - OLED Display für Statusmeldungen, Parameteranzeigen etc.
- Sonderfunktionen
  - Konfiguration über ETS und Telnet
  - SNTP Server
  - Messung der TP Busspannung, TP Stromaufnahme und TP Temperatur (Telnet, OLED Display)
  - Maximale TP APDU Paketlänge des KNX Busses (248 Bytes)
  - Maximale TP Paketlänge einstellbar (Telnet) zwischen 55 und 248 Bytes (APDU)
  - Simulation von UDP Tunneln für ETS Kommunikation (Telnet)
- Performance
  - Vorgabe einer max. TP-Datenrate für das Schreiben von KNX Telegrammen
  - Pufferung bis zu 256 Telegrammen pro Tunnel (2048 insgesamt) im Gerät IP-seitig
  - Pufferung bis zu 1024 Telegrammen für Telegramme von IP nach TP

ETS Parameter

Begriffe

Verschlüsselung, Verschlüsselt Wenn Geräte Dateninformationen in Form von Telegrammen über den TP-Bus oder IP-Netzwerk schicken, so sind diese grundsätzlich von Dritten lesbar. Diese benötigen hierzu lediglich Zugang zum TP-Bus oder IP-Netzwerk. Verschlüsselung der Daten soll in diesem Zusammenhang bedeuten, dass die Inhalte der Telegramme nicht mehr zu deuten sind, wenn die Verschlüsselungsparameter (z.B. Kennwörter) nicht bekannt sind.

Schlüssel, Verschlüsselungsparameter Eine Folge von Zahlen, die nur dem ETS Projekt be-

kannt sind. Diese Zahlen dienen zur Umformung der Daten in beide Richtungen: Ver- und Entschlüsseln.

FDSK (Factory Default Setup Key) Der initiale Fabrikschlüssel. Dieser Schlüssel dient bei der Inbetriebnahme der initialen Programmierung. Dabei wird ein neuer Schlüssel in das Gerät geladen, wobei dieser Vorgang mit dem FDSK verschlüsselt wird. Der FDSK Schlüssel ist danach nicht mehr gültig. Erst beim Zurücksetzen auf den Werkszustand (Factory Reset) wird er wieder aktiviert.

Backbone Bei IP Routern ist dies immer das IP-Netzwerk.

Multicast Eine IP Adresse im Netzwerk, über die alle Router eines Backbones kommunizieren. Tunnelverbindungen benötigen diese Adresse nicht. Multicast-Verbindungen erfolgen immer über das UDP Protokoll. Anders als bei der TCP Kommunikation kann ein Telegramm grundsätzlich verloren gehen. Dies ist z.B. bei WLAN Verbindungen mit hoher Wahrscheinlichkeit der Fall. Daher sollte das Routing-Backbone immer über eine Ethernet-Kabelverbindung realisiert werden, da diese zu fast 100% übertragungssicher ist.

Backbonekey, Backboneschlüssel Das Routingprotokoll kommuniziert bei KNX IP Secure verschlüsselt. Der Schlüssel muss bei allen Teilnehmern gleich sein und wird in das Gerät geladen. Die ETS generiert einen möglichst sicheren Schlüssel selbstständig.

Tunnelling Eine KNX Punkt-zu-Punkt Verbindung auf dem TCP/IP Netzwerk, die entweder per UDP oder TCP Protokoll aufgebaut wird. Tunnelling hat immer eine Sicherungsschicht eingebaut, d.h. unabhängig von der Ethernetverbindung, z.B. Kabel oder WLAN, und unabhängig vom TCP/IP Protokoll (UDP oder TCP) gehen keine Daten verloren. Bei UDP gilt allerdings die Einschränkung, dass die Sicherungsschicht mit einem 1-Sekunden-Timeout arbeitet. Bei Enertex Geräten kann dieser Timeout im erweiterten Setup angepasst werden.

Telnet Ein einfacher TCP Server auf Port 23, der direkte textbasierte Kommunikation mit dem IP Gerät ermöglicht. Telnet ist ein de facto Standard, der auf der Windowsebene z.B. mit „Putty“ angesprochen wird.

Abgesicherter Modus, Secure Mode Wenn das Gerät über die ETS so parametriert wird, dass die Kommunikation nur verschlüsselt erfolgt, spricht man vom abgesicherten Modus oder engl. Secure Mode.

Nicht abgesicherter Modus, Plain Mode Wenn das Gerät über die ETS so parametriert wird, dass die Kommunikation nur unverschlüsselt erfolgt, spricht man vom nicht abgesicherten Modus oder engl. Plain Mode.

ETS 5.6.6 und ETS 5.7.1

Versionsvoraussetzungen

Für einen fehlerfreien Betrieb der Geräte im abgesicherten Modus (Secure Mode) benötigt man die ETS 5.7.x oder höher.

Im nicht abgesicherten Modus kann das Gerät grundsätzlich ab der ETS 5.6.6 programmiert werden. Der abgesicherte Modus ist zwar parametrierbar, ist jedoch in dieser Version nicht vollständig umgesetzt. Soll das Gerät daher abgesichert betrieben werden, empfehlen wir mit der Version 5.7 oder höher zu arbeiten.

Besonderheiten

Programmiert man in der ETS 5.6.6 die **physikalische Adresse** über das Gerät und einer Tunnelverbindung selbst, so wirft die ETS am Ende eine Fehlermeldung. Diese ist zu ignorieren, die Vergabe der Adresse ist dennoch vorgenommen worden.

Vergibt man keine Tunneladressen in der Applikation, so werden alle Tunnel von der ETS auf 15.15.255 gesetzt. Eine Kommunikation über die Tunnelverbindung kann dann erheblich gestört oder nicht möglich sein.

Ist das Gerät abgesichert in ein Projekt eingebunden, so speichert die ETS die Parametrierung. **Wird das Gerät zurück auf Werkseinstellungen gesetzt**, spricht die ETS (5.6 bzw. 5.7) das Gerät nur noch verschlüsselt an. Daher kann keine Kommunikation mit der ETS mehr aufgebaut werden. In diesem Fall hilft nur ein Löschen der Applikation und ein Neustart der ETS.

Läuft ein Update von Windows im Hintergrund, kann es zu merkwürdigen Phänomen bei der Kommunikation zwischen dem Gerät und der ETS kommen. In diesem Fall ist das Update abzuwarten und Windows neu starten.

Topologie

Um das Interface in ein ETS-Projekt einzufügen, muss dieses eine TP-Line besitzen, in welchen das Interface als Gerät eingefügt wird.

Geräte Eigenschaften

Allgemein

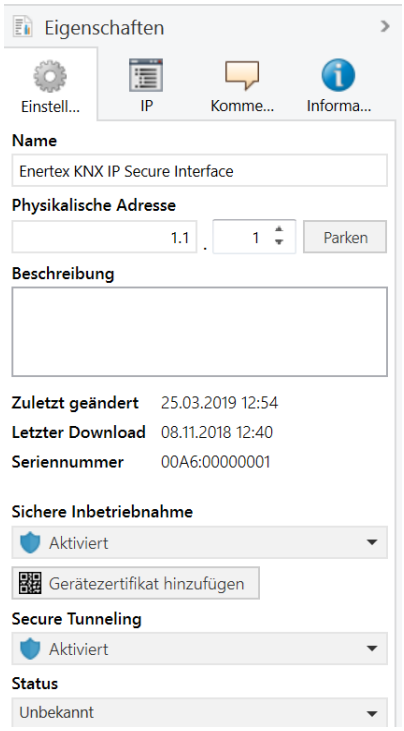

Abbildung 1: Eigenschaften des Geräts

Name Es kann ein beliebiger Name vergeben werden, max. 30 Zeichen

Sichere Inbetriebnahme Wenn aktiviert, ist die Verschlüsselung für die Inbetriebnahme aktiv: Es werden dann alle Parameter bereits verschlüsselt übertragen, wenngleich z.B. Tunnelverbindungen noch unverschlüsselt genutzt werden.

Secure Tunnelling Wenn aktiviert, können die Tunnelverbindungen nur über KNX Secure Tunnelling aufgebaut werden.

IP-Einstellungen

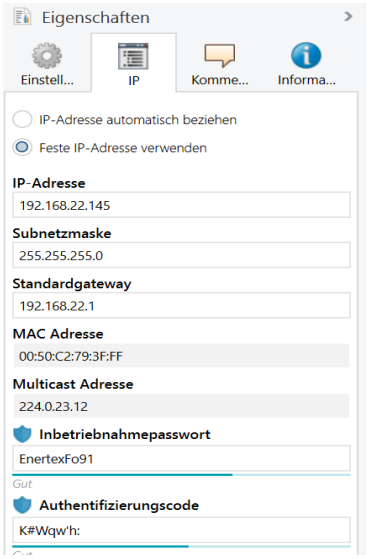

Abbildung 2: IP Einstellungen des Geräts

IP Adresse automatisch beziehen Das Gerät benötigt einen DHCP Server für die IP Adressvergabe

Feste IP Adresse verwenden Der Anwender gibt die IP Einstellungen selbst vor.

Inbetriebnahmepasswort Ein Passwort, aus welchem die ETS einen Schlüssel generiert. Dieser ist der Schlüssel für die Sichere Inbetriebnahme (s.o.).

Authentifizierungscode Mit dem Authentifizierungspasswort beweist der Anwender, dass er Zugriff auf das Projekt hat.

MAC Adresse Wird vom Gerät vorgegeben.

Multicast Adresse Wird vom Backbone vorgegeben.

Gerätespezifische Parameter

Allgemein

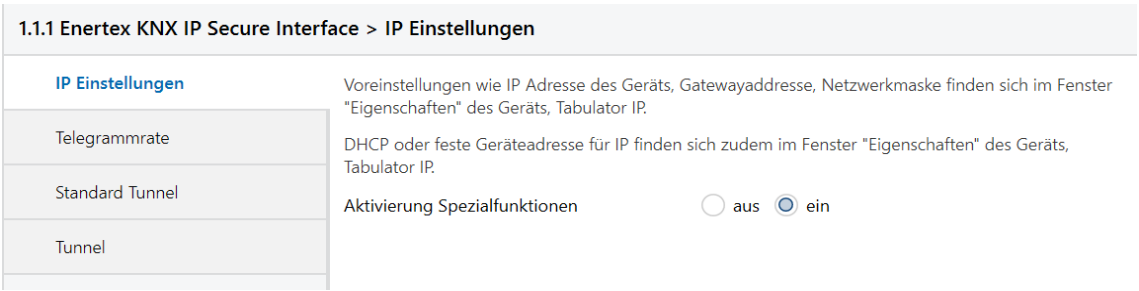

Abbildung 3: Allgemeine Einstellungen des Geräts

Name	Auswahlmöglichkeiten	Beschreibung
(Erläuternder Text)		Die ETS hat herstellerunabhängig einheitliche Parameterdialoge für verschiedene Einstellungen. Um die Anwendung zu vereinfachen, wird hier ein Hinweistext eingeblendet.
Aktivierung Spezialfunktionen	aus/ein	Enertex® Geräte bieten besondere Funktionen, um Anwendern max. Flexibilität zu gewährleisten.

Spezialfunktionen

Standard Tunnel bevorzugte IP

Enertex® Geräte bieten für Standard Tunnelverbindungen (vor 2019) die Möglichkeit, jede dieser Tunnelverbindungen jeweils einer IP Adresse zuzuordnen. Dies ermöglicht bei der Analyse von Gruppentelegrammen eine leichtere Zuordnung der Telegramme zum Sender, der hinter dem Tunnel „sitzt“, wie z.B. Visualisierungen oder Smartphone Apps.

Hinweis:

Diese Zuordnung kann allerdings jederzeit durch die ETS oder eine neue sog. erweiterte Tunnelverbindung (Stand 2019) aufgelöst werden.

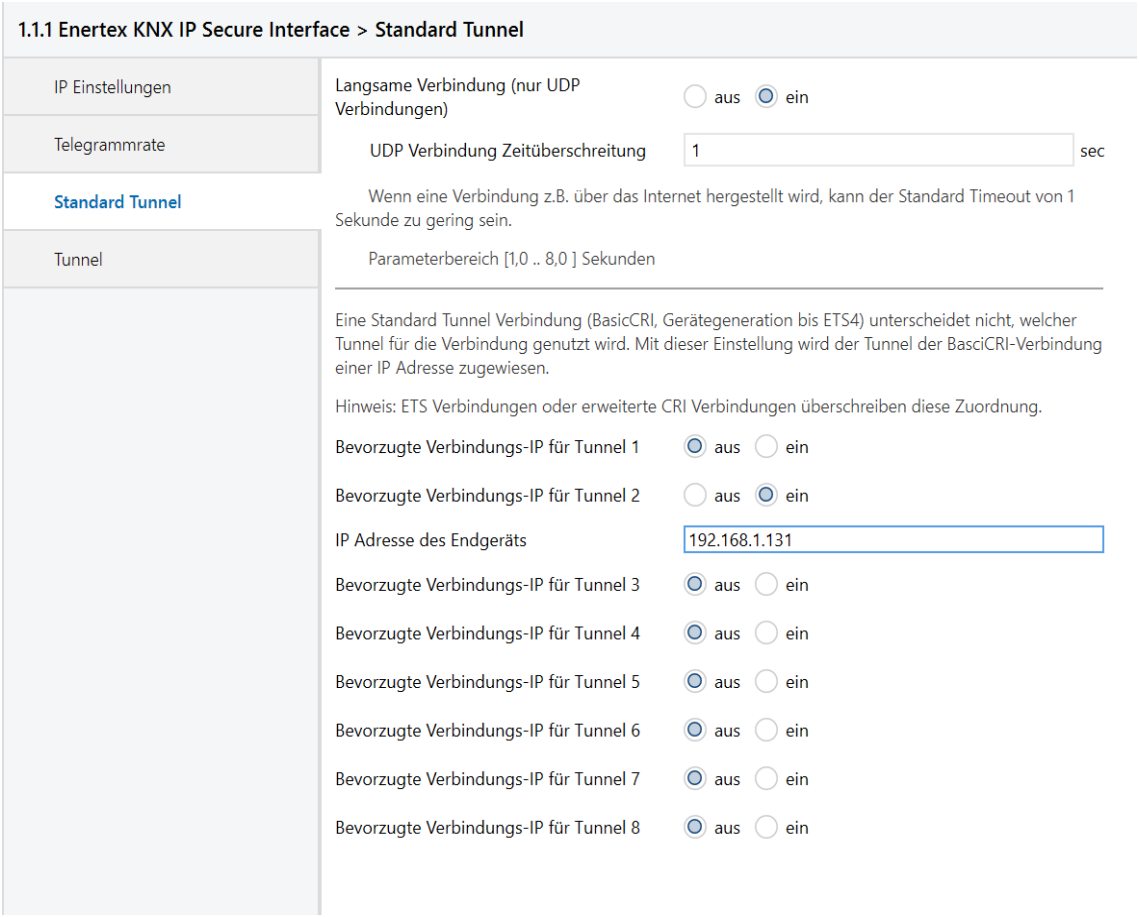

Abbildung 4: Verhalten der KNX Seite

Name	**Auswahlmöglichkeiten**	**Beschreibung**
Langsame Verbindung	aus/ein	Die Tunnelverbindungen über UDP werden standardmäßig mit einem Verbindungstimeout von 1 Sekunde betrieben. Dies kann bei Verbindungen über das Internet zu kurz sein.
UDP Verbindung Zeitüberschreibung	1,0 ... 8,0 sec	Einstellung des Timeouts für UDP Tunnelverbindungen
Bevorzugte Verbindungs-IP für Tunnel X	aus/ein	Tunnel X soll bevorzugt für eine IP Adresse verwendet werden.
IP Adresse des Endgeräts	(IP-V4 Adresse)	IP Adresse des Endgeräts.

Telnet

Per Telnet können zusätzliche Informationen vom IP Interface abgefragt werden. Der Telnet-Zugang ist ab Werk mit dem Passwort „knxsecure“ geschützt.

Sobald das Interface im Secure Modus betrieben wird, ist das Telnet-Interface deaktiviert. Es kann zwar für Entwicklerzwecke vor dem Programmieren des Secure-Modus aktiv geschaltet werden - dies birgt jedoch ein Sicherheitsrisiko.

`help`	Zeigt alle verfügbaren Kommandos an
`ifconfig`	Zeigt Netzwerkparameter an **IP mode.....: DHCP** **IP.....: 192.168.33.142** **Subnet mask...: 255.255.0.0** **Gateway.....: 192.168.33.1** **NTP server....: 192.53.103.108** **Sys multicast.: 224.0.23.12** **RT multicast..: 224.0.23.12** **Hardware addr.: 00:50:c2:79:3f:ff** Sys multicast: Multicastadresse für Systemtelegramme RT multicast: Multicastadresse für Routing-Telegramme
`ifconfig [help|dhcp|ip |mask]`	Netzwerkparameter über das Telnetinterface einstellen. Beispiele : Die IP Adresse per DHCP vergeben: **ifconfig dhcp** Die IP Adresse statisch auf 192.168.1.2 setzen (in diesem Fall sollte auch Gateway und Maske angepasst werden, s.u.) **ifconfig ip 192.168.1.2** Das Gateway auf 192.168.1.1 setzen: **ifconfig gw 192.168.1.1** Die Maske auf 255.255.255.0 setzen: **ifconfig mask 255.255.255.0**
`tpconfig`	Zeigt KNX Parameter an **KNX bus state.: up** **KNX address...: 15.15.000** **Serial number.: 00-a6-00-00-00-01**
`tpconfig [help|set]`	KNX Parameter über das Telnetinterface einstellen. Die TP Adresse auf 1.1.0 setzen: **tpconfig set 1.1.0**
`progmode [0|1]`	Programmiermodus abfragen oder ändern (0 = aus, 1 = ein)
`apdu [55..248]`	Die maximale Länge der KNX TP Telegramme lesen oder konfigurieren. Dies kann notwendig werden, wenn eine fehlerhafte Implementierung eines TP Stacks vorliegt, sodass die ETS eine Programmierung mit Telegrammen mit 248 Nutzbytes vornimmt, die das TP Gerät aber nicht verarbeiten kann (z.b. Zennio Z35i). Default ist 248 und sollte nur bei Bedarf verändert werden. **# apdu** **maximal len of a KNX telegram 248.** **Usage: apdu [55 .. 248]**
`tpratemax [5..50]`	Maximale Telegrammrate (IP=>TP) lesen oder konfigurieren; 50 T/s entsprechen 100% Buslast. **# tpratemax** **no limit, sending with maximum performance to TP.** **Usage: tpratemax [5 .. 50]**

`stats`	Zeigt diverse Statistiken zu Geräte- und Busstatus **uptime: 114 days, 2:19** **KNX communication statistics:** **TX to IP (all)..: 333729 (ca. 233 t/m)** **TX to KNX.....: 23244 (ca. 16 t/m)** **RX from KNX.....: 94559 (ca. 66 t/m)** **Overflow to IP..: 0** **Overflow to KNX.: 0** **TX tunnel re-req: 260** **TP bus voltage..: 28.95 V** **TX TP rate.....: 50 T/s (= 100 %)** Uptime: Laufzeit der Schnittstelle seit letztem Neustart TX to IP (all): Anzahl aller auf IP verschickten Telegramme TX to KNX: Anzahl der auf den KNX-Bus geschickten Telegramme RX from KNX: Anzahl der vom KNX-Bus empfangenen Telegramme Overflow to IP: Anzahl der Telegramme, die nicht auf IP geschickt werden konnten Overflow to KNX: Anzahl der Telegramme, die nicht auf den KNX-Bus geschickt werden konnten TX tunnel re-req: Anzahl der Telegramme, die in den Tunnelverbindungen wiederholt werden mussten TP bus voltage: Aktuelle Bussspannung (zum Zeitpunkt des Aufruf von stats) TX TP rate: maximale Telegrammrate (TP)
`free [clear]`	Zeigt Statistiken über die Speicherauslastung **Used stack memory...: 14 %** **Allocated memory....: 64 %** **Unused memory.....: 35 %** **TP-Tx buffer.....: 0 %** **TP-Tx buffer max....: 0 %** **TP-Rx buffer max....: 0 %** **Tunnel-T8 buffer max: 92 %** Used stack memory: Funktionsstapelauslastung Allocated memory: Allokierter Gerätespeicher Unused memory: Nicht genutzter Gerätespeicher TP-Tx buffer: Derzeit genutzter TP Sendepuffer TP-Tx buffer max: Max. Auslastung TP Sendepuffer (IP=>TP) seit Systemstart TP-Rx buffer max: Max. Auslastung TP Empfangspuffer (IP<=TP) seit Systemstart Tunnel-XX (XX=1..8) buffer max: Max. Auslastung des Tunnelling Buffers. Es werden nur Tunnel angezeigt, deren Puffer überhaupt benutzt wurde Löschen der Pufferstatistik: **free clear**
`tunnel [1..8]`	Zeigt aktive Tunnelverbindungen (ohne Argument), bzw. detaillierte Informationen zur angegebenen Tunnelverbindung an (mit Argument 1..8) **# tunnel** **Tunnels open: 1/8** **1: 00.02.246, closed** **2: 00.02.247, open (CCID: 82)** **3: 00.02.248, closed** **4: 00.02.249, closed** **5: 00.02.250, closed** **6: 00.02.251, closed** **7: 00.02.252, closed** **8: 00.02.253, closed** **# tunnel 2** **Tunnel 2.....: open (CCID 82)** **KNX address.....: 00.02.247** **HPAI control.....: 192.168.22.252:4808** **HPAI data.....: 192.168.22.252:4808** **Connect. type.....: TUNNEL_CONNECTION** **Communication.....: UDP CONNECTION** **TX tun req.....: 23169** **TX tun re-req.....: 0** **RX tun req.....: 821** **RX tun re-req (identified): 0** **RX tun req (wrong seq.)...: 0** **Current tunnel buffer.....: 0 %** **Connected since (UTC).....: 16:26:16 29-01-2019** CCID: Verbindungs-ID der Tunnelverbindung KNX address: Tunneladresse HPAI control: Kontrollendpunkt des Verbindungspartners HPAI data: Datenendpunkt des Verbindungspartners Connect. Type: Verbindungstyp Tunnel oder Management Verbindung Communication: UDP oder TCP Verbindung TX tun req: Anzahl der Telegramme, die in die Tunnelverbindungen geschickt wurden TX tun re-req: Anzahl der Telegramme, die in den Tunnelverbindungen wiederholt werden mussten RX tun req: Anzahl der Telegramme, die von der Tunnelverbindungen empfangen wurden RX tun re-req: Anzahl der Telegramme, die von der Tunnelverbindungen doppelt empfangen wurden RX tun req (wrong seq.): Anzahl der Telegramme, die von der Tunnelverbindungen mit falscher Sequenznummer empfangen wurden Current tunnel buffer: Auslastung aktuell des IP Puffers des Tunnels Connected since (UTC): Uhrzeit, seitdem die Tunnelverbindung besteht.
`version`	Firmware-Version abfragen

`mask`	Masken-Version abfragen
`display [0|1]`	Displaymodus abfragen oder ändern (0 = Standard, 1 = invertiert)

`tunaddr 1..8 address`
`tunaddr reset`
`tunaddr setall`
`tunaddr help`
	KNX-Adresse eines Tunnels lesen (*`tunaddr`*) oder ändern, z.B. *`tunaddr 1 15.15.240`*, alle Tunneladressen fortlaufend ab einer bestimmten Startadresse vergeben (*`tunaddr setall 15.15.15`*), oder die KNX-Adressen aller Tunnel auf Werkseinstellung zurücksetzen (*`tunaddr reset`*)
	
	`# tunaddr`
	`1: KNX address: 15.15.010`
	`2: KNX address: 15.15.011`
	`3: KNX address: 15.15.012`
	`4: KNX address: 15.15.013`
	`5: KNX address: 15.15.014`
	`6: KNX address: 15.15.015`
	`7: KNX address: 15.15.016`
	`8: KNX address: 15.15.017`

`tunmode [std/tpblk]`	Tunnelmodus lesen (ohne Parameter) oder setzen (*`tp`* bzw. *`tpblk`*); tunmode tpblock: IP=> KNX bei gleicher Backbone Line Frame an TP weiterleiten KNX=> IP bei gleicher Sub Line Frame an TP weiterleiten
`Tunneltime [1.0..8.0]`	Timeout für Tunnelverbindung abfragen oder ändern (1.0 bis 8.0). Einstellung ist identisch zu „Langsame Verbindung“, Abbildung 4
`tunudp`	Typ der Tunnelverbindung für die ETS abfragen oder ändern (0 = Standard, 1 = Nur UDP).
`date`	Datum und Uhrzeit anzeigen
`sntp [query|server IP]`	Anfrage an den NTP-Server schicken (*`sntp query`*) oder IP des NTP-Servers einstellen (*`sntp server 1.2.3.4`*)
`logmem`	Ereignisspeicher im Gerät. Geeignet für die Entwicklung von Clients. Bei Supportanfragen auslesen.

`passwd oldpw newpw`
`passwd oldpw`
`passwd newpw`
	Ändert das aktuelle Telnet-Passwort (*`passwd alt neu`*), löscht das aktuelle Passwort (*`passwd alt`*) oder setzt ein neues Passwort, falls momentan keines gesetzt ist (*`passwd neu`*)

`secure [0|1]`	Verhalten des Telnetinterface im Securemodus anzeigen oder ändern (0= deaktivieren, Standard, 1=aktivieren) **Hinweis: Es kann zwar für Entwicklerzwecke vor dem Programmieren des Secure-Modus aktiv geschaltet werden - dies birgt jedoch ein Sicherheitsrisiko.**
`factory_reset`	Auf Werkseinstellungen zurücksetzen und neustarten
`die`	Hardwarewatchdog testen. Führt Reset aus.
`reboot`	Neustart
`logout`	Telnet-Session beenden

Aktuelle Daten

Unter http://www.enertex.de/d-produkt.html finden Sie die aktuelle ETS Datenbankdatei sowie die aktuelle Produktbeschreibung.

Technische Daten

Symbole	 Darf nicht über den Hausmüll entsorgt werden.
KNX (Versorgung)	DC 21 ... 32 V SELV Stromaufnahme < 20 mA
Ethernet-Schnittstelle	Rj45-Buchse für 10M/100MBit Ethernet
Anzeigen	Grafisches OLED, 128x64 Programmier-LED (rot), Busaktivität-LED (gelb), Spannungs-LED (grün blinkend) Netzwerklink (grün), Netzwerkaktivität (gelb)

KNX Funktionen	• KNXIP Secure Tunnelling • Bis zu 48 Telegramme pro Sekunde • AES 128 Verschlüsselung • Asymmetrischer Schlüsselaustausch für Tunnelverbindungen • UDP und TCP Kommunikation • Bis zu 8 Tunnelverbindungen • APDU 248, parametrierbar zwischen 55 und 248 • TP Telegrammratenbegrenzung • TP Busspannungsmessung (Anzeige Telnet bzw. Display)
Umgebungstemperatur	-5 ... +45° C
Installation	• Nur zur Verwendung in trockenen Innenräumen. • Nur zum Einbau in Verteiler nach DIN 43880 auf Hutschiene 35 mm nach EN 50022. • Schutzart IP20
Abmessungen	35,0 mm x 89,6 mm x 62,9 mm (L x B x H)

Open Source Software

Dieses Produkt verwendet Software aus dritten Quellen folgender Autoren:
Adam Dunkels <adam@sics.se>
Marc Boucher <marc@mbsi.ca> and David Haas <dhaas@alum.rpi.edu>
Guy Lancaster <lancasterg@acm.org>, Global Election Systems Inc.
Martin Husemann <martin@NetBSD.org>.
Van Jacobson (van@helios.ee.lbl.gov)
Paul Mackerras, paulus@cs.anu.edu.au,
Christiaan Simons <christiaan.simons@axon.tv>
Jani Monoses <jani@iv.ro>
Leon Woestenberg <leon.woestenberg@gmx.net>

LWIP

Quelle: https://savannah.nongnu.org/projects/lwip/

```
Copyright (c) 2001-2004 Swedish Institute of Computer Science.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products
derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```