



enertex bayern gmbh
simulation entwicklung consulting

Handbuch und Konfiguration

Enertex® KNX IP Secure Router



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.....	3
Montage und Anschluss.....	3
Inbetriebnahme.....	3
<i>Boot</i>	<i>3</i>
<i>Anzeigen.....</i>	<i>3</i>
<i>Reset.....</i>	<i>4</i>
<i>Zusatzapplikation.....</i>	<i>4</i>
Funktionsübersicht.....	4
ETS Parameter.....	5
<i>Begriffe.....</i>	<i>5</i>
<i>ETS 5.6.6 und ETS 5.7.0.....</i>	<i>5</i>
Versionsvoraussetzungen.....	5
Besonderheiten.....	6
<i>Topologie.....</i>	<i>6</i>
<i>Geräte Eigenschaften.....</i>	<i>8</i>
Allgemein.....	8
IP-Einstellungen.....	8
<i>Gerätespezifische Parameter.....</i>	<i>9</i>
Allgemein.....	9
Spezialfunktionen.....	9
Verhalten der KNX Seite	9
Standard Tunnel bevorzugte IP	10
Routing.....	12
Filter Geräteadresse (physikalisch adressierte Telegramme).....	12
Filter Gruppenadressen.....	13
Standard.....	13
Erweiterter Gruppenadressfilter.....	14
Telnet.....	16
Aktuelle Daten.....	19
Technische Daten.....	19
Open Source Software.....	20
<i>LWIP</i>	<i>20</i>

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 Routers 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. Während 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.

Als bald 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.

Zusatzapplikation

Ab Version 1.050 beinhaltet die Firmware eine Zusatzapplikation. Diese ermöglicht die Gruppenkommunikation mit Hilfe einer eigenen ETS Applikation und zweiter physikalischen Adresse.

Mit dieser Applikation wird es möglich, den Bus mit der aktuellen Uhrzeit und Datum per Gruppenadresse zu synchronisieren. Zusätzlich bietet die Applikation eine Möglichkeit, verschlüsselte (secure) und unverschlüsselte (plain) Gruppenadressen über das Gerät zu verknüpfen.

Das Handbuch zur Zusatzapplikation und die ETS Applikation finden Sie im Downloadbereich dieses Gerätes unter <http://www.enertex.de>.

Funktionsübersicht

Das Gerät weist folgende Funktionalitäten auf:

- KNX IP Secure
 - Acht unabhängige KNXnet/IP-Tunnelverbindungen
 - Kommunikation über TCP oder UDP
 - KNX IP Routing zur Kommunikation zwischen KNX Linien, Bereichen und Systemen
 - KNX IP Routing im verschlüsselten (Secure) Modus.
 - KNX IP Tunnelling im verschlüsselten (Secure) Modus.
 - Telegrammweiterleitung und Filterung nach physikalischer Adresse
 - Telegrammweiterleitung und Filterung nach Gruppenadresse mit bis zu 62 Filterblöcken
- 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 (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 bekannt 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 parametrierung 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 parametrierung wird, dass die Kommunikation nur unverschlüsselt erfolgt, spricht man vom nicht abgesicherten Modus oder engl. Plain Mode.

ETS 5.6.6 und ETS 5.7.0

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 den Router in ein ETS-Projekt einzufügen, muss dieses ein IP-Backbone besitzen. Beispiel: folgende ETS-Topologie:

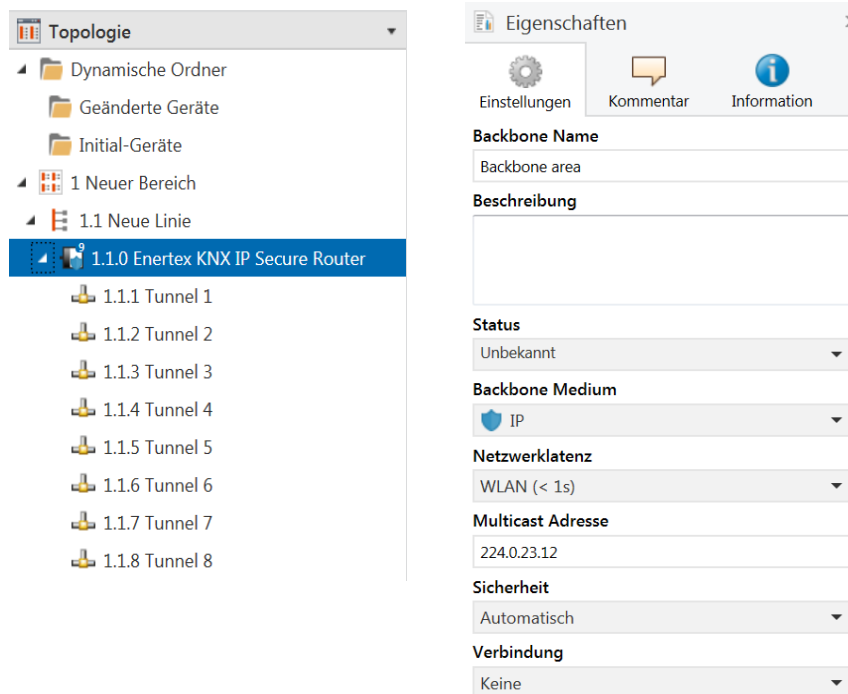


Abbildung 1: Topologie (links) und Eigenschaften des Backbone

Linien:

- 1: Backbone Medium IP
- 1.1: Linie Medium TP

Im Eigenschaftendiaglog des Backbones (HINWEIS: Hierzu auf Topologie, direkt oberhalb von „Dynamische Ordner“, vgl. Abbildung 1, klicken), finden sich die Einstellungen zum Multicast des Backbones. Die Netzwerklatenz (vgl. Abbildung 1) kann verändert werden, wenn das Routing über ein großes verteiltes System läuft. In diesem Fall ist die Zeitkonstante zu erhöhen.

Über die ETS 5.6.6 oder höher wird das Gerät parametrisiert. Der KNX IP Secure Router unterstützt bis zu acht KNX (Secure) IP-Tunnelverbindungen und kann als Linien- oder Bereichskoppler eingesetzt werden.

Geräte Eigenschaften

Allgemein

Abbildung 2: 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 Tunneling Wenn aktiviert, können die Tunnelverbindungen nur über KNX Secure Tunneling aufgebaut werden.

IP-Einstellungen

Abbildung 3: IP Einstellungen des Geräts

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

vergabe

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 Optional.

MAC Adresse Wird vom Gerät vorgegeben.

Multicast Adresse Wird vom Backbone (vgl. Abbildung 1) vorgegeben.

Gerätespezifische Parameter

Allgemein

1.1.0 Enertex KNX IP Secure Router > IP Einstellungen

IP Einstellungen

Voreinstellungen wie IP Adresse des Geräts, Gatewayadresse, Netzwerkmaske finden sich im Fenster "Eigenschaften" des Geräts, Reiter IP.

DHCP oder feste Geräteadresse für IP finden sich zudem im Fenster "Eigenschaften" des Geräts, Reiter IP.

IP Multicast Adresse des Backbones kann im Fenster Topologie angepasst werden. Dazu muss die Überschrift "Topologie" gewählt werden. Die Parameter erscheinen dann im Fenster "Einstellungen"

Aktivierung Spezialfunktionen ☐ aus ☒ ein

Spezialfunktionen

Verhalten der KNX Seite

Standard Tunnel

Routing

Filter

Filter Geräteadresse

Filter Gruppenadressen

Tunnel

Routing

Abbildung 4: 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

Verhalten der KNX Seite

1.1.0 Enertex KNX IP Secure Router > Spezialfunktionen > Verhalten der KNX Seite

IP Einstellungen	Hinweis: Wenn eine Tunnel-Verbindung aufgebaut wird, bestätigt diese Verbindung jedes Telegramm (ACK). Daher ist diese Einstellung nur für Router sinnvoll, bei denen die Tunnelverbindungen nicht genutzt werden.
Spezialfunktionen	Jedes Telegramm bestätigen (ACK) ☒ aus ☐ ein
Verhalten der KNX Seite	Richtung: Gerät als Empfänger (KNX Seite) Nur geroutete Telegramme bestätigen (ACK) ☒ ein ☐ aus
Standard Tunnel	Richtung: Gerät als Sender (KNX Seite) Wiederhole Telegeramme, wenn nicht bestätigt ☐ aus ☒ ein
Routing	Wenn die TP Linie einfach zugänglich ist (KNX Außenlinie), kann der Router gesperrt werden, sodass er nicht mehr über den KNX Bus programmiert werden kann. Dies generiert zusätzliche Sicherheit. Programmieren über IP ist noch möglich.
Filter	Programmiersperrung TP Seite ☒ aus ☐ ein
Filter Geräteadresse	Maximale Anzahl von Sende-Telegrammen (nur TP Seite). 50 Telegramme pro Sekunde entsprechen 100% Buslast.
Filter Gruppenadressen	Max. Telegrammrate (nur KNX TP) 50 T/s
Tunnel	
Routing	

Abbildung 5: Verhalten der KNX Seite

Name	Auswahlmöglichkeiten	Beschreibung
Jedes Telegramm bestätigen (ACK)	<u>a</u> us/ein	Der Router bestätigt jedes Telegramm, auch wenn er dieses nicht weiterleitet (nur TP)
Nur geroutete Telegramme bestätigen (ACK)	<u>a</u> us/ein	Der Router bestätigt nur die Telegramme, die er weiterleitet (nur TP)
Wiederhole Telegramme, wenn nicht betätigt	<u>a</u> us/ein	Der Router wiederholt nicht bestätigte phy. adressierte Telegramme (nur TP)
Programmiersperrung TP Seite	<u>a</u> us/ein	Vgl. Parameterdialog
Max. Telegrammrate	5 .. <u>50</u>	Vgl. Parameterdialog

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.

1.1.0 Enertex KNX IP Secure Router > Spezialfunktionen > Standard Tunnel

IP Einstellungen	Langsame Verbindung (nur UDP Verbindungen) ☐ aus ☒ ein
Spezialfunktionen	UDP Verbindung Zeitüberschreitung 1 sec
Verhalten der KNX Seite	Für eine Verbindung z.B. über das Internet kann der Standard Timeout (1 Sek) zu gering sein. Parameterbereich [1,0 .. 8,0] Sekunden
Standard Tunnel	
Routing	Eine Standard Tunnel Verbindung (BasicCRI, Gerätegeneration bis ETS4) unterscheidet nicht, welcher Tunnel für die Verbindung genutzt wird. Mit dieser Einstellung wird der Tunnel der BasicCRI-Verbindung einer IP Adresse zugewiesen.
Filter	Hinweis: ETS Verbindungen oder erweiterte CRI Verbindungen überschreiben diese Zuordnung.
Filter Geräteadresse	Bevorzugte Verbindungs-IP für Tunnel 1 ☐ aus ☒ ein
Filter Gruppenadressen	IP Adresse des Endgeräts 192.168.1.131
Tunnel	Bevorzugte Verbindungs-IP für Tunnel 2 ☒ aus ☐ ein
Routing	Bevorzugte Verbindungs-IP für Tunnel 3 ☒ aus ☐ ein
	Bevorzugte Verbindungs-IP für Tunnel 4 ☒ aus ☐ ein
	Bevorzugte Verbindungs-IP für Tunnel 5 ☒ aus ☐ ein
	Bevorzugte Verbindungs-IP für Tunnel 6 ☒ aus ☐ ein
	Bevorzugte Verbindungs-IP für Tunnel 7 ☒ aus ☐ ein
	Bevorzugte Verbindungs-IP für Tunnel 8 ☒ aus ☐ ein

Abbildung 6: Verhalten der KNX Seite

Name	Auswahlmöglichkeiten	Beschreibung
Langsame Verbindung	<u>aus</u> /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	<u>1,0</u> ... 8,0 sec	Einstellung des Timeouts für UDP Tunnelverbindungen
Bevorzugte Verbindungs-IP für Tunnel X	<u>aus</u> /ein	Tunnel X soll bevorzugt für eine IP Adresse verwendet werden.
IP Adresse des Endgeräts	(IP-V4 Adresse)	IP Adresse des Endgeräts.

Routing

1.1.0 Enertex KNX IP Secure Router > Spezialfunktionen > Routing

IP Einstellungen	Topologieüberprüfung
Spezialfunktionen	Wenn aktiviert, erkennt der Router Topologiefehler und sendet eine Nachricht (A_Network_Parameter_Response) auf den KNX Bus oder IP Line. Das Telegramm erscheint auf der Linie, welche die Topologie verletzt.
Verhalten der KNX Seite	Im Telnet Interface und am Display ist dann die fehlerhafte KNX Adresse auszulesen. Das fehlerhafte Telegramm wird nicht geroutet.
Standard Tunnel	Überprüfung der Topologie ☒ aus ☐ ein
Routing	
Filter	Routing (vor 2018)
Filter Geräteadresse	Wenn aktiviert, arbeitet der Router nach Spezifikation vor 2018. Dies bedeutet im Wesentlichen ein anderer Routing Count Algorithmus. Dieses veraltete Routing ist gegen bestimmte IT-Angriffe leichter verwundbar.
Filter Gruppenadressen	Wenn der Router als Ersatz in eine bestehende Installation eingebaut wird, kann das veraltete Routing eventuell notwendig werden.
Tunnel	Aktivierung Routing Algorithmus (<2018) ☒ aus ☐ ein
Routing	

Abbildung 7: Verhalten der KNX Seite

Name	Auswahlmöglichkeiten	Beschreibung
Überprüfung der Topologie	<u>aus</u> /ein	Vgl. Dialogbeschreibung
Aktivierung Routing Algorithmus <2018	<u>aus</u> /ein	Vgl. Dialogbeschreibung

Filter Geräteadresse (physikalisch adressierte Telegramme)

1.1.0 Enertex KNX IP Secure Router > Filter > Filter Geräteadresse	
IP Einstellungen	Geräteadresse
Spezialfunktionen	IP => KNX filtern (Voreinstellung)
Verhalten der KNX Seite	KNX => IP filtern (Voreinstellung)
Standard Tunnel	Blockieren von Broadcast Telegrammen
Routing	IP => KNX ☒ aus ☐ ein
Filter	KNX => IP ☒ aus ☐ ein
Filter Geräteadresse	

Abbildung 8: Filter für physikalisch adressierte Telegramme

Name	Auswahlmöglichkeiten	Beschreibung
Geräteadresse	<u>filtern</u> , blockieren, weiterleiten	Die physikalisch adressierten Telegramme (z.B. Programmierung von Aktoren) können über das Routing weitergeleitet, blockiert oder gefiltert werden. Dies betrifft damit sämtliche Kommunikation, die sich auf die Geräteadresse bezieht.

Blockieren von Broadcast Telegrammen	<u>aus</u> /ein	Broadcast-Telegramme (z.B. Suchen nach Akteuren im Programmierzustand) können über den Router weitergeleitet oder blockiert werden.
--------------------------------------	-----------------	---

Filter Gruppenadressen

Standard

1.1.0 Enertex KNX IP Secure Router > Filter > Filter Gruppenadressen

IP Einstellungen	IP => KNX	
Spezialfunktionen	Hauptgruppe 0..13	<u>weiterleiten</u>
	Hauptgruppe 14..15	<u>filtern</u>
	Hauptgruppe 16..31	<u>filtern</u>
	Erw. Filter Gruppenadressen	☐ aus ☒ ein
Verhalten der KNX Seite		
Standard Tunnel		
Routing		
Filter	KNX => IP	
Filter Geräteadresse	Hauptgruppe 0..13	<u>weiterleiten</u>
	Hauptgruppe 14..15	<u>filtern</u>
	Hauptgruppe 16..31	<u>filtern</u>
	Erw. Filter Gruppenadressen	☐ aus ☒ ein
Filter Gruppenadressen		
Erw. Filter IP => KNX		
Erw. Filter KNX => IP		

Abbildung 9: Standard Filter für Gruppentelegramme

Name	Auswahlmöglichkeiten	Beschreibung
IP=>KNX		Richtung: Telegramme von der IP Seite auf die KNX Seite
Hauptgruppe 0 bis 13	<u>filtern</u> , blockieren, <u>weiterleiten</u>	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 0 bis 13 werden hier zu einen Block zusammengefasst.
Hauptgruppe 14 bis 15	<u>filtern</u> , blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 14 und 15 werden hier zu einen Block zusammengefasst.
Hauptgruppe 16 bis 31	<u>filtern</u> , blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 16 und 31 werden hier zu einen Block zusammengefasst.
Erweiterter Gruppenadressfilter	<u>aus</u> /ein	Neben der blockorientierten Filterung von Gruppenadresstelegrammen kann jede Gruppe auch einzeln für sich über das Routing weitergeleitet, blockiert oder gefiltert werden. Mit dieser Funktion kann der Parameterdialog hierzu geöffnet werden.

KNX=>IP		Richtung: Telegramme von der KNX Seite auf die IP Seite
Hauptgruppe 0 bis 13	<u>filtern</u> , blockieren, <u>weiterleiten</u>	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 0 bis 13 werden hier zu einen Block zusammengefasst.
Hauptgruppe 14 bis 15	<u>filtern</u> , blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 14 und 15 werden hier zu einen Block zusammengefasst.
Hauptgruppe 16 bis 31	<u>filtern</u> , blockieren, weiterleiten	Gruppentelegramme können über das Routing weitergeleitet, blockiert oder gefiltert werden. Die Gruppen 16 und 31 werden hier zu einen Block zusammengefasst.
Erweiterter Gruppenadressfilter	<u>aus/ein</u>	Neben der blockorientierten Filterung von Gruppenadresstelegrammen kann jede Gruppe auch einzeln für sich über das Routing weitergeleitet, blockiert oder gefiltert werden. Mit dieser Funktion kann der Parameterdialog hierzu geöffnet werden.

Erweiterter Gruppenadressfilter

Für beide Richtungen kann neben der blockorientierten Filterung von Gruppenadresstelegrammen jede Gruppe auch einzeln über das Routing weitergeleitet, blockiert oder gefiltert werden. Daher gibt es die links in der Navigationsleiste bei Aktivierung (vgl. Abbildung 8 bzw. Abbildung 9) die Einträge „Erw. Filter IP=>KNX“ und „Erw. Filter KNX=>IP“.

Für jeden dieser Einträge gibt es 32 weitere Gruppenadressfilter, die unabhängig von den blockorientierten Filtern arbeiten. Die Einstellungen der 32 Gruppenadressfilter überschreiben die der blockorientierten Filter.

1.1.0 Enertex KNX IP Secure Router > Filter > Filter Gruppenadressen > Erw. Filter IP => KNX

IP Einstellungen	Erweiterter Filter für Richtung IP=> KNX	
Spezialfunktionen	Es kann für jede Hauptgruppe ein Filter definiert werden. Dies überschreibt die jeweils Einstellung der Gruppenfilter (0..13, 14..15, oder 16..31). Wenn ein Einzelfilter deaktiviert wird, ist der entsprechende Gruppenfilter aktiv.	
Verhalten der KNX Seite	Hauptgruppe 00	inaktiv (Voreinstellung) ▼
Standard Tunnel	Hauptgruppe 01	inaktiv (Voreinstellung) ▼
Routing	Hauptgruppe 02	inaktiv (Voreinstellung) ▼
Filter	Hauptgruppe 03	inaktiv (Voreinstellung) ▼
Filter Geräteadresse	Hauptgruppe 04	inaktiv (Voreinstellung) ▼
Filter Gruppenadressen	Hauptgruppe 05	inaktiv (Voreinstellung) ▼
Erw. Filter IP => KNX	Hauptgruppe 06	inaktiv (Voreinstellung) ▼
Erw. Filter KNX => IP	Hauptgruppe 07	weiterleiten blockieren filtern
Tunnel	Hauptgruppe 08	inaktiv (Voreinstellung) ▼
Routing	Hauptgruppe 09	inaktiv (Voreinstellung) ▼
	Hauptgruppe 10	inaktiv (Voreinstellung) ▼
	Hauptgruppe 11	inaktiv (Voreinstellung) ▼
	Hauptgruppe 12	inaktiv (Voreinstellung) ▼
	Hauptgruppe 13	inaktiv (Voreinstellung) ▼
	Hauptgruppe 14	inaktiv (Voreinstellung) ▼
	Hauptgruppe 15	inaktiv (Voreinstellung) ▼
	Hauptgruppe 16	inaktiv (Voreinstellung) ▼
	Hauptgruppe 17	inaktiv (Voreinstellung) ▼

Abbildung 10: Standard Filter für Gruppentelegramme

Name	Auswahlmöglichkeiten	Beschreibung
Hauptgruppe 00	inaktiv, filtern, blockieren, weiterleiten	Gruppentelegramme dieser Hauptgruppe können über das Routing weitergeleitet, blockiert oder gefiltert werden. Wenn der Filter nicht aktiv ist, so gilt das Verhalten der Parameter von Abbildung 8 bzw. Abbildung 9.
Hauptgruppe NN NN= 1.. 31	S.O.	S.O.

Telnet

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

Sobald der Router 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.

<code>help</code>	Zeigt alle verfügbaren Kommandos an
<code>ifconfig</code>	Zeigt Netzwerkparameter an <pre> 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 </pre> Sys multicast: Multicastadresse für Systemtelegramme RT multicast: Multicastadresse für Routing-Telegramme
<code>ifconfig [help dhcp ip [mask]</code>	Netzwerkparameter über das Telnetinterface einstellen. Beispiele : Die IP Adresse per DHCP vergeben: <code>ifconfig dhcp</code> Die IP Adresse statisch auf 192.168.1.2 setzen (in diesem Fall sollte auch Gateway und Maske angepasst werden, s.u.) <pre>ifconfig ip 192.168.1.2</pre> Das Gateway auf 192.168.1.1 setzen: <code>ifconfig gw 192.168.1.1</code> Die Maske auf 255.255.255.0 setzen: <code>ifconfig mask 255.255.255.0</code>
<code>tpconfig</code>	Zeigt KNX Parameter an <pre> KNX bus state.: up KNX address...: 15.15.000 Serial number.: 00-a6-00-00-00-01 </pre>
<code>tpconfig [help set]</code>	KNX Parameter über das Telnetinterface einstellen. Die TP Adresse auf 1.1.0 setzen: <code>tpconfig set 1.1.0</code>
<code>lcconfig</code>	<pre> Coupler type..: line coupler IP -> KNX: GA 0-13.....: route GA 14-15.....: filter GA 16-31.....: block Ph. addr.....: filter Broadcast.....: route KNX -> IP: GA 0-13.....: route GA 14-16.....: filter GA 16-31.....: block Ind.addr.....: filter Broadcast.....: route Check IA rout.: disabled Ind.Addr.tlg..: individually addressed telegrams are 3 times repeated </pre>
<code>systembc [0 1]</code>	Bestimmte Bits im System Broadcasts setzen, sodass IP Routing auch über ältere Geräte möglich ist (z.B. Gira Homerserver). Standardmäßig ist dieser Kompatibilitätsmodus eingeschaltet Wrong handling of bits in system broadcasts (necessary for e.g. Gira Homerserver) is 1 (on)
<code>progmode [0 1]</code>	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. <pre># apdu maximal len of a KNX telegram 248. Usage: apdu [55 .. 248]</pre>
tpratemax [5..50]	Maximale Telegrammrate (IP=>TP) lesen oder konfigurieren; 50 T/s entsprechen 100% Buslast. <pre># tpratemax no limit, sending with maximum performance to TP. Usage: tpratemax [5 .. 50]</pre>
stats	Zeigt diverse Statistiken zu Geräte- und Busstatus <pre>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 %)</pre> 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 Busspannung (zum Zeitpunkt des Aufruf von stats) TX TP rate: maximale Telegrammrate (TP)
busload	Zeigt die Buslast wie folgt: <pre>----- Measure 1 min. 5 min 15 min since start ----- RX Bit/s 0035 0091 0080 0079 TX Bit/s 0007 0006 0002 0004 RT Bit/s 0042 0098 0083 0083 ----- RX T/s 00.26 00.94 00.70 00.69 TX T/s 00.12 00.08 00.03 00.05 RT T/s 00.38 01.02 00.73 00.75 ----- RX % 00.52 01.88 01.40 01.39 TX % 00.24 00.16 00.07 00.11 RT % 00.76 02.04 01.47 01.51 ----- MaxR T/s 08 08 24 29 MaxT T/s 03 03 03 08 MxRT T/s 08 08 24 29 ----- Maximum load at 16:50:08 06.10.2020 (UTC)</pre> Dabei steht RX für Empfangen, TX für Gesendet, RT die Summe aus Empfangen und Gesendet entsprechend dieser Tabelle alle Minute, 5 Minuten, 15 Minuten und seit Start des Geräts. Die Angabe Bit/s zeigt die tatsächliche Baudrate auf dem TP Bus, wobei diese die Summe von die Applikationsdaten und Offset der KNX Protokoll-Schichten darstellt. Die % Auslastung ist bezogen auf 50 Telegramme pro Sekunde. Die Maxima sind im angegebenen Intervall jeweils neu berechnet.

<code>free [clear]</code>	Zeigt Statistiken über die Speicherauslastung <pre> 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 Tunneling Buffers. Es werden nur Tunnel angezeigt, deren Puffer überhaupt benutzt wurde Löschen der Pufferstatistik: free clear </pre>
<code>tunnel [1..8]</code>	Zeigt aktive Tunnelverbindungen (ohne Argument), bzw. detaillierte Informationen zur angegebenen Tunnelverbindung an (mit Argument 1..8) <pre> # 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. </pre>
<code>version</code>	Firmware-Version abfragen
<code>mask</code>	Masken-Version abfragen
<code>display [0 1]</code>	Displaymodus abfragen oder ändern (0 = Standard, 1 = invertiert)

tunaddr 1..8 address tunaddr reset tunaddr setall tunaddr help	KNX-Adresse eines Tunnels lesen (<i>tunaddr</i>) oder ändern, z.B. <i>tunaddr 1 15.15.240</i>, alle Tunneladressen fortlaufend ab einer bestimmten Startadresse vergeben (<i>tunaddr setall 15.15.15</i>), oder die KNX-Adressen aller Tunnel auf Werkseinstellung zurücksetzen (<i>tunaddr reset</i>) # <i>tunaddr</i> 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 (<i>tp</i> bzw. <i>tpblk</i>); tunmode tpblock: IP=> KNX bei gleicher Backbone Line Frame an TP weiterleiten KNX=> IP bei gleicher Sub Line Frame an TP weiterleiten
lock [0 1]	Lock-Status abfragen (ohne weiteren Parameter) oder ändern (0 = aus, 1 = ein). Einstellung ist identisch zu Programmiersperre TP Seite, Abbildung 5. Ein Router kann durch das Filtern das Weiterleiten von physikalisch adressierten Telegrammen unterbinden, d.h. das Umprogrammieren von Geräten über eine Linie hinweg ist nicht möglich. Dies wird bei Verwendung von Linien im Außenbereich interessant. Allerdings kann z.B. eine KNX-USB Schnittstelle auf eine Außenlinie direkt an den Bus angeschlossen werden und der Router in der Außenlinie selbst umprogrammiert werden, sodass er die physikalisch adressierten Telegramme weiterleitet. Mit dieser Telnet-Funktion kann dies unterbunden werden. Setzt man per telnet "lock" auf 1, so kann der Router nicht mehr über die KNX Linie programmiert werden und entsprechende Aktivierung des Weiterleitens über KNX TP ist nicht mehr möglich.
topology [0 1]	„Überprüfung der Toplogie“ abfragen oder ändern (0 = aus, 1 = ein). Einstellung ist identisch zu „Überprüfung der Toplogie“, Abbildung 7 Subline Topology has been violated with 1.2.3 Last logged at 18:28:31 09-11-2018 Mainline Topology has been violated with 1.2.3 Last logged at 18:24:31 09-11-2018
Tunneltime [1.0..8.0]	Timeout für Tunnelverbindung abfragen oder ändern (1.0 bis 8.0). Einstellung ist identisch zu „Langsame Verbindung“, Abbildung 6
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 (<i>sntp query</i>) oder IP des NTP-Servers einstellen (<i>sntp server 1.2.3.4</i>)
sendack [0 1]	„Jedes Telegramm bestätigen (ACK)“ abfragen oder ändern. Einstellung ist identisch zur Dokumentation zu Abbildung 5.
blockfilter [0 1]	Sämtliche Gruppenadressfilter deaktivieren (d.h. alles weiterleiten), unabhängig von den Einstellungen der ETS. Abfragen oder ändern (0 = aus, 1 = ein).
routingcounter [0 1]	Routingcounterhandling abfragen oder ändern (0 = Standard, 1 = Verhalten vor 2018). Diese Einstellung ist identisch zu Aktivierung Routing Algorithmus <2018, Abbildung 7
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 (<i>passwd alt neu</i>), löscht das aktuelle Passwort (<i>passwd alt</i>) oder setzt ein neues Passwort, falls momentan keines gesetzt ist (<i>passwd neu</i>)
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 Tunneling und Routing • Bis zu 48 Telegramme pro Sekunde • AES 128 Verschlüsselung • Asymmetrischer Schlüsselaustausch für Tunnelverbindungen • UDP und TCP Kommunikation • Bis zu 8 Tunnelverbindungen • Bis zu 62 Gruppenadressfilter • 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.