TCP/IP • STACK

Our robust, MISRA-compliant, embedded IPv4/IPv6 networking stack

High-quality dual IPv4/v6 stack

The key to a successful embedded application is to use high-quality software that is verifiably developed and ensures a stable, low-risk development platform. Our networking solution provides a significant range of protocols as well as support for both IPv4 and IPv6 standards, delivering reliability and long-term network compatibility. Tuxera's "clean" stack, precision-engineered for embedded systems, offers unrivalled performance and security.

We provide optimized Ethernet drivers with our stack, and the software integrates into virtually any embedded environment – with or without an RTOS. The software is designed for high performance on embedded microcontrollers. Our stack has no unnecessary copies, static memory management is carefully thought out, and it fully exploits dedicated memory areas and cache.

Full MISRA compliance

Network quality and security issues are not typically caused by problems with the requirements or security protocols, but with their implementation. Traditional freestyle "code-then-test" methods cannot guarantee correctness and security. To minimize the risk of errors, many industries use standardized or widely adopted, formalized development methods.

Tuxera's TCP/IP Stack was designed to mitigate any potential risks. All the included software components are developed with a rigorous approach to quality, using a strongly typed subset of the "C" language. Tuxera supplies quality verification including a full MISRA[1]-compliant static analysis report.

[1] "MISRA" is a registered trademark of MIRA Ltd, held on behalf of the MISRA Consortium. No endorsement by MISRA is claimed or implied for any product.

Small footprint, high throughput, low CPU cycle operation

Tuxera's innovative approach to design means that our network stack delivers rapid data transfer rates, with minimal system resource requirements. Our testing shows that Tuxera's packet processing runs faster than comparable embedded stacks, while using around 14 kB of ROM in a typical application scenario.[2]

RAM requirements can vary widely depending on application needs, but are typically as low as 12 kB. With minimum configuration UDP applications, it's possible to use less than 5 kB of ROM and only a few hundred bytes of RAM (plus network buffers).

[2] Based on measurements taken using the LPC2468 MCU. Actual performance may vary based on the hardware, software, and testing protocols used.

Core features of Tuxera TCP/IP Stack:

- MISRA-compliant static and dynamic test reports
- Test suites for interoperability, code integrity
- Extensive range of supported protocols
- Dual IPv4 and IPv6 standards support
- Specialized modules
- No dynamic memory allocation (no malloc/free)
- Standard BSD sockets interface
- Zero copy
- Small footprint (RAM/ROM)
- High-speed data transfer
- Low power consumption due to low CPU overhead
- Verified compatibility with most popular embedded RTOSes
- Efficient operation without an RTOS

Supported protocols, modules, and environments

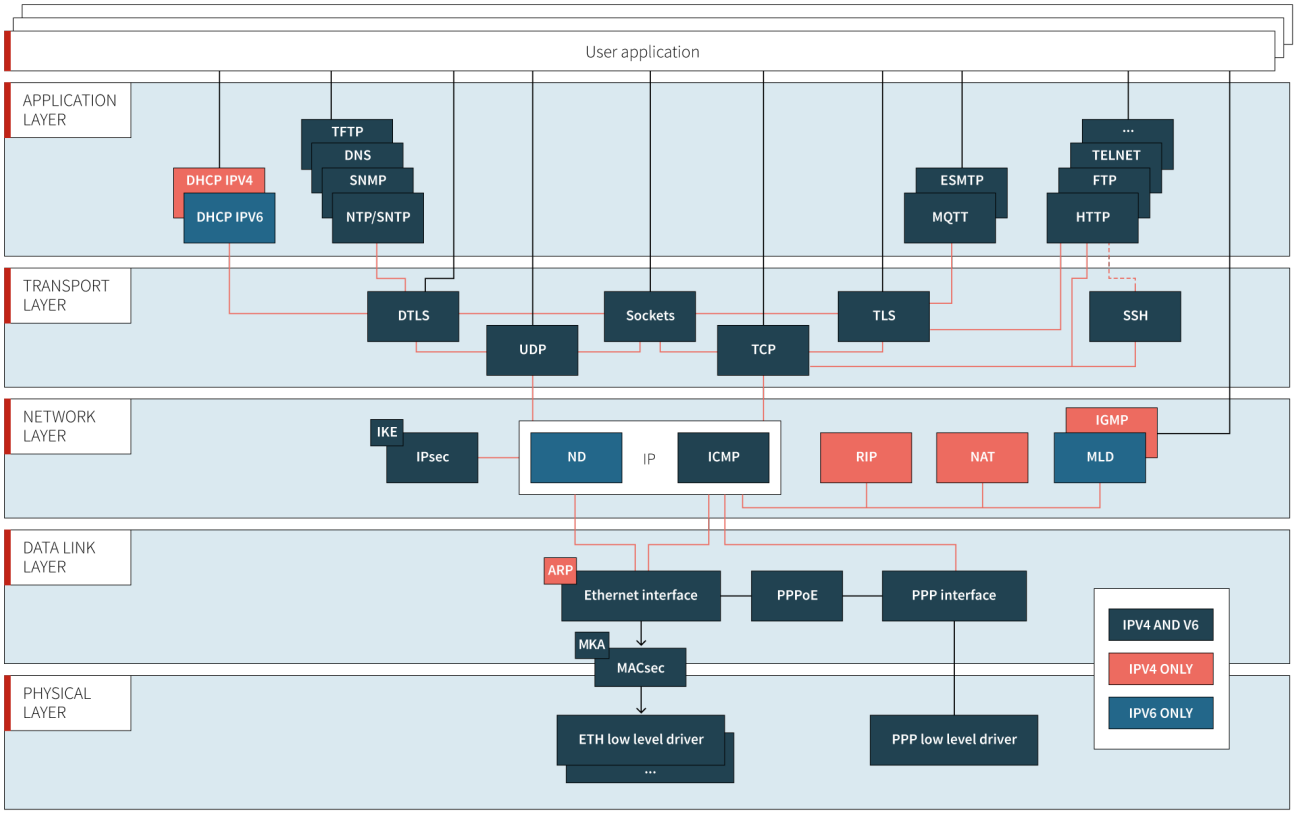
Tuxera TCP/IP Stack protocols

Tuxera TCP/IP Stack supports a significant range of protocols, as well as IPv4 and IPv6 standards. Our networking stack includes all the standard modules and connectivity features you expect – plus we go above and beyond to provide enhanced features with specialized modules, as detailed in the following sections.

Tuxera TCP/IP Stack supported protocols

7 - Application	DHCP, DNS, FTP, HTTP, MQTT, NTP, SMTP, SNMP, SNTP, Telnet, TFTP		SFTP, SCP		
6 - Presentation	DTLS	TLS	SSH	EST	EAP
5 - Session	Sockets				
4 - Transport	UDP	TCP			
3 - Network	IPsec/IKEv2				
	IPv4	IPv6			
	ICMP, IGMP, ARP, NAT, AutoIP	ICMP, ND, MLD			
2 - Data link	Ethernet Interface, PPP, MACsec Interface				EAPoL
1 - Physical	Ethernet low-level drivers, PPP Driver, MACsec				

Tuxera TCP/IP Stack architecture



Tuxera TCP/IP Stack specialized modules

Tuxera CryptoCore™

Protect embedded systems data from potential hackers looking for backdoor access. CryptoCore™ is Tuxera's encryption and security library, managed through our Embedded Encryption Manager (EEM). Our advanced software feature secures embedded systems using multiple encryption or hash algorithms through a uniform interface. This saves you significant development time – just drop in CryptoCore and encrypt data stored on flash or transmitted across a network.

CryptoCore is developed using strict processes to ensure verifiable stability and enhanced integrity. We also deliver CryptoCore with a full MISRA compliance report. This level of verifiable quality in security and encryption stands in direct contrast with the widely used “code-then-test” methods, which have resulted in serious security breaches, such as the Heartbleed vulnerability in OpenSSL.

Tuxera CryptoCore’s available algorithms

Package	Algorithms	Used for	Type
AES	10 AES algorithm variants	IPsec, TLS, SNMP, EAP, IKE	Encrypt, hash
Base64	Base64	SMTP, SSH	Encode binary over text stream
ChaCha20	ChaCha20	TLS	Signing and key exchange
ECC	ECDH, ECDHE, ECDSA	TLS	Key exchange and digital signature
EDH	EDH	IKEv2, TLS	Key exchange
FPE	FPE	IPsec, TLS	Encryption
MD5	MD4, MD5, MD5-HMAC	PPP, TLS, IPsec, SNMP	Hash
RSA	RSA, RSA-PSS	TLS	Encrypt
SHA	SHA-256/-384/-512/, SHA-1/2-HMAC, SHA3-224/256/384/512, SHAKE-128/256	TLS, IPsec, IKE, SSH, SNMP	Hash
TDES	DES, TDES-CBC, TDES-CBC-RAW	TLS, SNMP	Encrypt
TIGER	TIGER128, TIGER-160, TIGER-192, TIGER-HMAC	IKE	Hash

Simple Network Management Protocol (SNMP)

SNMP gives devices connected on a network a consistent and reliable way to share information. We developed a high-quality SNMPv2 and SNMPv3 implementation to bring secure network management capability to embedded devices. Using SNMP, you can monitor device operation, usage, detect network faults or inappropriate access, and configure remote devices. Our robust SNMP is designed for use on many network devices with minimal impact on the managed nodes, low transport overheads, and it keeps working when other applications fail.

Tuxera’s HTTP/HTTPS module features

- SNMP agent supporting v1, v2c, v3
- SNMP manager capability to query remote agents
- MIB compiler for easy integration of any MIB
- Uses standard UDP interface for integration with Tuxera’s network stack

HTTP/HTTPS

Our flexible web server solution for embedded systems allows the creation of dynamic content within a highly secure environment. HTTP Secure (HTTPS) provides secure communication over computer networks. It operates as a request-response protocol in the client/server model. The secure client may be a web browser, while an application hosting a website may be the secure server.

HTTPS resources are identified and located on the network using Uniform Resource Identifiers (URIs). HTTPS secure operation relies on Tuxera's Transport Layer Security (TLS) module. TLS provides security by encrypting the whole HTTPS message, including the header and the request/response content (read more on TLS in following sections).

Tuxera's HTTP/HTTPS module features

- Compliant with RFC 2818
- Designed for integration with both RTOS and non-RTOS based systems
  - Configurable to enable BSD sockets
- Supports all standard HTTP methods:
  - GET
  - PUT
  - POST
  - DELETE
- HTTP Secure (HTTPS) connections supported
- Configurable number of simultaneous connections
- Static ROMed pages
- Connects to any file system and processes pages received from it
- Supports dynamic content created by user-specified functions and dynamic variables from HTML tags
- Optional user authentication based on username and IP address (as a sample)

MQTT networking protocol

MQTT is a small, low-bandwidth networking protocol ideally suited for connecting embedded applications that are remotely monitored through an internet connection. Tuxera's MQTT implementation runs on its trusted TCP/IP stack and uses verifiable TLS for secure connections.

When a secure connection is required, we provide a verifiable TLS module to handle encryption independently of MQTT. Additionally, a client can provide a username and password so that the broker can authenticate the client. When MQTT operates over a TLS connection, both the client and the server can authenticate each other using x.509 certificates.

Tuxera's MQTT module features

- Complete implementation of all MQTT features
- Client operates as publisher and/or subscriber to a configurable range of topics on multiple MQTT brokers
- All QoS (Quality of Service) levels supported
- Full MISRA compliance report available
- Tested with many well-known brokers in secure & non-secure mode
- Use together with Tuxera's verifiable TLS for completely secure IoT cloud connections

Verifiable IPsec & IKE

IPsec provides VPN security in embedded applications such as cars, point-of-sale (POS) terminals, medical devices, industrial equipment, and many others. Our IPSec module ensures integrity, confidentiality, and authentication between two devices in a network, providing strong defense against threats such as "man in the middle" attacks and packet sniffers.

Like other components in Tuxera TCP/IP Stack, our verifiable IPSec module uses a strong development process and is supplied with quality verification, including a full MISRA-compliant static analysis report.

Verifiable TLS/DTLS

The importance of using a strong development process and source code control has been emphasized by several high-profile security problems caused by source code errors. Traditional methods of “freestyle coding” and test do not provide sufficient guarantees of correctness.

Our verifiable Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) is a highly optimized, quality-assured software module designed to provide secure network communications for embedded devices. It provides a framework for secure communication in networks based on the TCP/IP or UDP protocols. The module also includes a full MISRA compliance report.

Tuxera’s verifiable TLS/DTLS features

- Easy integration using a standard Sockets interface
- Verifiable TLS up to 1.3 (RFC 8446)
- DTLS version 1.2 (RFC 6347)
- Heartbeat extensions (RFC 6520)
- HTTP over TLS (RFC 2818)
- HTTPS Secure Server, HTTPS Secure Client, and FTPS support
- Full certificate management with Tuxera CryptoCore™
- Supports wide range of cipher suites including the following algorithms:
  - DH/DHE/DSS/ECDHE/RSA
  - AES/RC4/3DES
  - POST
  - SHA/MD5

RTOS abstractions

Tuxera supports a range of RTOSes from various vendors, through RTOS abstractions. For custom schedulers and superloops, we offer a “No RTOS” abstraction. We also have our own small cooperative scheduler eTaskSync, which is designed to handle all processing and interface requirements of Tuxera middleware. This means you can choose our robust quality and outstanding performance regardless of legacy software.

We deliver RTOS abstractions for the following systems:

- CMX RTX
- CMSIS
- eCOS
- emBOS
- EUROS
- FreeRTOS
- Keil RTX
- MQX
- Nucleus
- QNX
- Quadros RTXC
- ThreadX
- µ-velOSity
- µC/OS-II/III
- and many others

Extensive compiler support

- Eclipse/GCC
- LLVM
- ADI CrossCore Embedded Studio
- IAR Embedded Workbench
- Keil Arm Compiler
- CodeWarrior
- AVR Studio
- Green Hills Multi
- Microchip MPLAB
- Renesas HEW
- TI Code Composer Studio
- Mentor CodeSourcery
- STM32Cube
- Atollic True Studio
- and many more

Microcontrollers

Analog Devices	SHARC+
Arm	Cortex-M0/M1/M3/M4/M7, R4/R52, A5/A8/A9/A53/A55, Arm7/9/11
Infineon	C16x, XE16x, FM0/FM3/FM4, XMC1000/4000, Traveo II, AURIX
Microchip	PIC24, PIC32, AVR32, SAM3/4/7/9
NXP	LPC1300/1700/1800/2000/3000/4000, ColdFire, Kinetis, PowerPC, i.MX, Vybrid, QorIQ
Renesas	SuperH, RA, RX, RL, RH850, R-Car, Synergy, 78k, H8
Silicon Labs	EFM32, SIM3
STMicroelectronics	STM32, SPC5, Stellar
Texas Instruments	MSP430, Stellaris, C2000, Hercules, DaVinci, Sitara, Tiva
Toshiba	TMP M0/M3
Xilinx AMD	Zynq, Microblaze

*Our software supports virtually any microcontroller. Please contact us if your specific MCU is not listed.

Comprehensive target processors support

Tuxera TCP/IP Stack operates efficiently on a wide range of target processors (microcontrollers). We've intelligently designed our networking stack so that it can be ported easily and quickly to new architectures. Our stack also comes with drivers to support a variety of leading processors.

Responsive, expert support

Providing knowledgeable embedded engineering services and customer support are Tuxera's company cornerstones. Our team of embedded software experts is committed to supporting your project from design to production and beyond. We understand the development challenges with embedded applications, proven through over 30 years of experience and our collaboration with the world's major operating system developers and chipset makers.

Each year, our technology is deployed in millions of cars and other devices in need of reliable embedded storage and networking software. Our software is also backed by a guarantee, ensuring that the product performs to the agreed requirements. Contact our sales team for more info on warranties.

Interested? Get in touch: sales@tuxera.com

Tuxera Inc. Global HQ
Westendintie 1
02160 Espoo
Finland
www.tuxera.com