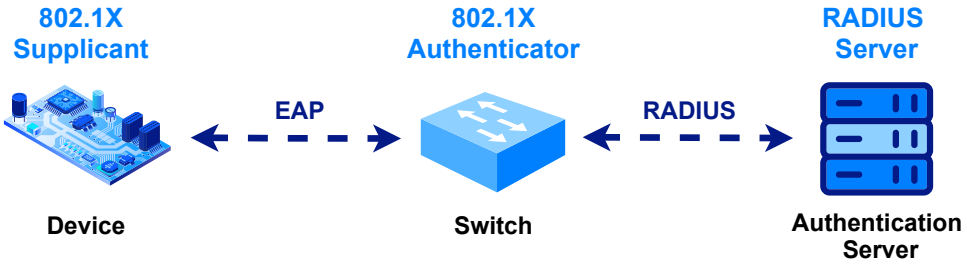
CycloneEAP

CycloneEAP is a 802.1X / EAP library dedicated to embedded applications. 802.1X standard specifies a protocol that prevents unauthorized access to a corporate LAN, by providing port-level authentication. The 802.1X protocol relies on EAP (Extensible Authentication Protocol) to manage various authentication methods, such as username/password and digital certificates.



An 802.1X architecture involves 3 parties: a **supplicant**, an **authenticator**, and an **authentication server**.

- The supplicant is a client device which wants to be authenticated.
- The authenticator acts as a proxy between the client and the authentication server and controls the authorized/unauthorized state of the port. It is typically implemented on Ethernet switches.
- The authentication server (generally a RADIUS server) verifies user's credentials and instructs the authenticator to authorize network access for the user.

Main Features

- 802.1X supplicant implementation
- Supports password-based authentication using EAP-MD5
- Supports X.509 certificate-based mutual authentication using EAP-TLS
- Supports TLS 1.3 with EAP-TLS (RFC 9190)
- 802.1X authenticator implementation in pass-through mode
- Supports RADIUS over UDP (RFC 2865)
- IEEE8021-PAE-MIB to remotely manage and monitor the authenticator
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Portable architecture (no processor dependencies)
- The library is distributed as a full ANSI C and highly maintainable source code

Supported Authentication Methods

- EAP-MD5 (RFC 3748)
- EAP-TLS (RFC 5216)

Supported Processors

- ARM Cortex-M3
- ARM Cortex-M4
- ARM Cortex-M7
- ARM Cortex-M33
- ARM Cortex-M85
- ARM Cortex-R4
- ARM Cortex-A5
- ARM Cortex-A7
- ARM Cortex-A8
- ARM Cortex-A9
- Legacy ARM7TDMI / ARM926EJ-S
- RISC-V
- MIPS M4K
- MIPS microAptiv / M-Class
- Infineon TriCore AURIX
- PowerPC e200
- Coldfire V2
- RX600
- AVR32
- Xtensa LX6

Supported Operating Systems

- Amazon FreeRTOS
- SafeRTOS
- ChibiOS/RT
- CMSIS-RTOS
- CMSIS-RTOS2
- CMX-RTX
- Keil RTXv4 and RTXv5
- Micrium µC/OS-II and µC/OS-III
- Microsoft Azure RTOS (ThreadX)
- PX5 RTOS
- Segger embOS
- TI-RTOS (SYS/BIOS)
- Zephyr RTOS
- Bare Metal programming (without RTOS)

Supported Compilers / Toolchains

Toolchain / IDE	Compiler
Makefile	GCC
AC6 System Workbench for STM32 (SW4STM32)	GCC
Atollic TrueSTUDIO	GCC
Espressif ESP-IDF	GCC
HighTec Toolset for TriCore	GCC
IAR Embedded Workbench	EWARM, EWRX
Infineon DAVE	GCC
Keil MDK-ARM	ARM Compiler v5, ARM Compiler v6 (CLANG)
Microchip Studio (Atmel Studio)	GCC
Microchip MPLAB X	GCC, XC32
Microsoft Visual Studio	MSVC
NXP MCUXpresso	GCC
NXP S32 Design Studio (S32DS)	GCC
Renesas e2Studio	GCC, CC-RX
Segger Embedded Studio	GCC
ST STM32CubeIDE	GCC
Tasking VX-Toolset	VX-Toolset for TriCore

IEEE

- IEEE Std 802.1X-2004: IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control

RFC

- RFC 2865: Remote Authentication Dial In User Service (RADIUS)
- RFC 2869: RADIUS Extensions
- RFC 3579: RADIUS (Remote Authentication Dial In User Service) Support For EAP
- RFC 3580: IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 4137: State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
- RFC 5216: The EAP-TLS Authentication Protocol
- RFC 9190: EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3