

acticom 802.1x secure authentication

The use of IEEE 802.1x offers an efficient framework to a protected network for authenticating and administrating user traffic, as well as dynamically varying encryption keys. 802.1x ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

The acticom IEEE802.1x software module, an implementation of the IEEE802.1x standard, offers the functionality for providing secure authentication in WLAN-based wireless access networks

The acticom IEEE802.1x software module, an implementation of the IEEE802.1x standard, offers the functionality to provide secure authentication in WLAN-based wireless access networks. The 802.1x stack includes support for WEP-independent encryption based on EAP-TLS and the extended Protected-EAP.

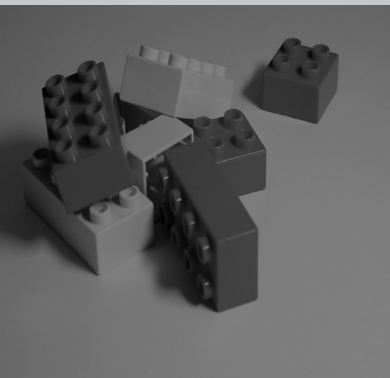
IEEE802.1x is part of the IEEE802.1 standard family that defines management functionality for IEEE802-based networks. Designed to secure wired and also wireless networks, as for example the IEEE802.11 WLAN standard, 802.1x defines a generic framework that is able to use different authentication mechanisms without implementing these mechanisms outside the backend authentication infrastructure and the client devices.

Independence of individual authentication methods is achieved by utilising the Extensible Authentication Protocol (EAP, RFC 2284) that defines a generic container to convey authentication method PDUs

Independence of individual authentication methods is achieved by utilising the Extensible Authentication Protocol (EAP, RFC 2284) that defines a generic container to convey authentication method PDUs. EAP messages are exchanged on the air interface between the mobile device (known as supplicant in 802.1x terminology) and base station (authenticator) by using an encapsulating protocol (EAP-over-LAN/EAPoL).

Initial 802.1x communication begins with an unauthenticated supplicant (e.g. a client device) attempting to connect with an authenticator (e.g. an 802.11-WLAN access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic such as HTTP, DHCP, or POP3 packets, until the access point can verify the client's identity using the authentication server (e.g. RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

*contact:
acticom GmbH
security@acticom.de
<http://www.acticom.de>
Am Borsigturm 42
13507 Berlin
Tel: +49(0)30 / 4303 2510
Fax: +49(0)30 / 4303 2519*



TLS (RFC2246) is the IETF successor to the Secure Socket Layer (SSL) technology and was defined to prevent eavesdropping, replay attack detection and message tampering offering protection to the authentication process

Although defining an authentication framework, IEEE 802.1x does not specify encryption, message integrity checking or message authentication by itself, but relies on an underlying secure communication channel. In wireless environments offering public access an encryption of the air interface might not be available while processing the authentication exchange. This is true especially for 802.11-WLAN systems for which a shared key between client and access point is required to run Wired-Equivalent-Privacy (WEP). Care must be taken to secure the authentication phase in 802.1x. A reasonable solution is the integration of Transport Layer Security (TLS) resulting in EAP-TLS as specified in RFC2716.

TLS (RFC 2246) is the IETF successor to the Secure Socket Layer (SSL) technology and was defined to prevent eavesdropping, replay attack detection and message tampering offering protection to the authentication process. TLS uses public key cryptography to provide mutual authentication and secure data exchange. However, TLS demands special requirements on network operators when deploying certificates to customers and network access systems. To overcome these problems that arise from certificate management an extension to EAP-TLS was suggested: Protected-EAP.

PEAP uses the TLS handshake solely for identifying the network to a client device, thus abandoning the need of assigning signed certificates to individual client devices. Client authentication is done inside the established TLS tunnel profiting from the benefits of TLS communication. Any EAP-based authentication method might be used inside the established secure channel.

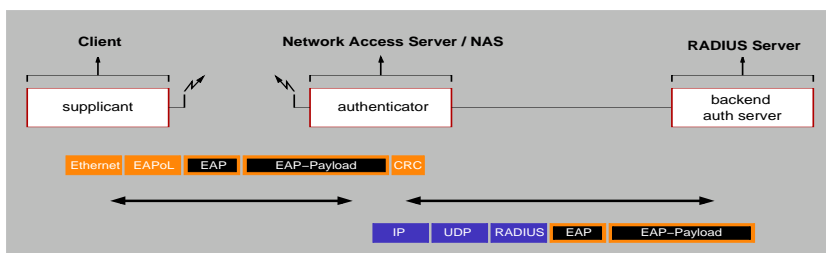


Figure 1: 802.1x authentication method

Two modules are available: supplicant for mobile clients and authenticator for access points

acticom_802.1x source code:

The full 802.1x protocol stack is available to manufacturers of network access devices and network operators requiring secure 802.1x based authentication in wireless and also wired environments.

Two modules are available :

- a supplicant for mobile clients and
- an authenticator for access points.

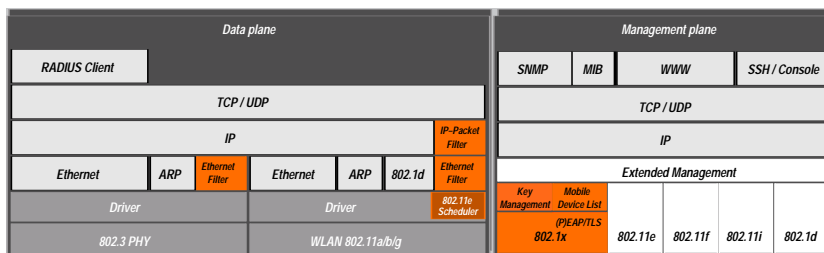
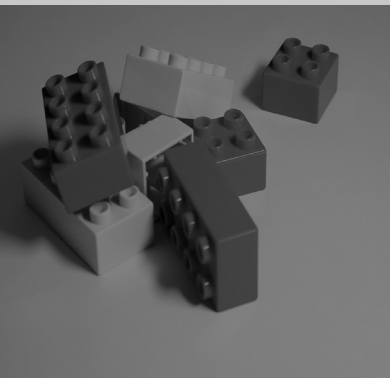


figure 2: 802.1x software modules within access point stack

The acticom_802.1x software stack is available as independent supplicant and authenticator or as fully featured 802.1x stack comprising both modules. The software is shipping as C++ source code implementation for easy integration. Full documentation of source code, Interfaces, APIs is also included.

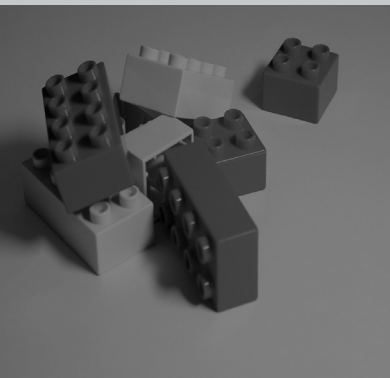
Feature list of the acticom_8021x stack:

1. base functionality

- Authenticator Port Access Entity (PAE) FSM
- Supplicant Port Access Entity (PAE) FSM
- Controlled Directions FSM
- Backend authentication FSM
- Reauthentication FSM
- Port Timer FSM
- Bridge Detection FSM
- Supplicant/Authenticator Key Transmission FSM
- Key Reception FSM
- Full EAP-over-LAN implementation including EAPoL-Key exchange
- EAPoL encapsulation over IEEE 802.3/IEEE 802.11
- RADIUS implementation comprising:
 - RFC 2865 (basic authentication),
 - RFC 2866 (basic accounting)
 - RFC 2869 (EAP extensions)
- Preparation for RADIUS tunneling extensions according to RFC 2868
- Accounting interface to underlying operating system
- Full-Duplex key exchange between authenticator and supplicant
- Support for independent dynamic WEP rekeying
- Key encryption based on RFC 2548 compliant Microsoft Point-to-Point-Encryption (MPPE) protocol attributes
- Interface to external EAP libraries
- Hot-Plugging of arbitrary EAP modules, e.g. PEAP, UMTS-AKA, or EAP-SIM

2. management functionality

- authenticator diagnostics, statistics and system configuration
- also accessible by remote management
- management library for integration into external SNMP packages
- library enables access to the stack's internal state



acticom offers a set of EAP library modules for hot-plugging in the supplicant stack. These include EAP-MD5, EAP-MS-CHAP-v2 and EAP-TLS. Additional EAP modules can be easily integrated by the customer or will be provided by acticom

acticom offers adaptation and integration to the customers target platform

*contact:
acticom GmbH
security@acticom.de
http://www.acticom.de
Am Borsigturm 42
13507 Berlin
Tel: +49(0)30 / 4303 2510
Fax: +49(0)30 / 4303 2519*

Additional features:

1. acticom offers a set of EAP library modules for hot-plugging in the supplicant stack. These include EAP-MD5, EAP-MS-CHAP-v2 and EAP-TLS.

Additional EAP modules can be easily integrated by the customer or will be provided by acticom.

2. acticom has implemented a full featured PEAP module as defined in draft-josefsson-pppext-eap-tls-eap-02 to protect non-encrypted EAP (e.g. MD5) authentication modules while being exchanged between the supplicant and a backend authentication server.

For non-PEAP-aware RADIUS servers acticom is able to provide a PEAP-enhanced RADIUS proxy that might act as a PEAP termination point while relaying the unencrypted inner EAP protocol.

3. Compatible with the following RADIUS Servers:

- Microsoft IAS with EAP-MD5
- Linux Free RADIUS
- Funk Steel-Belted Radius with EAP-MD5, EAP-TLS
- Funk Odyssey with EAP-TLS
- HP Interlink with EAP-TLS, EAP-MD5

Future features:

acticom plans to release additional EAP library modules as additional EAP library modules are work in progress. These will include EAP-SIM authentication and EAP-UMTS/AKA authentication and will be released as soon as the full standards become available.

acticom Services:

OEMs can use the acticom secure_802.1x source code for integration into their own products. acticom offers adaptation and integration to the customers target platform. In addition consulting and support regarding 802.1x will be available.

Licensing:

Customers can choose from a range of flexible licensing models for the 802.1x source code.

Licensing for the acticom 802.1x authenticator source code starts at 48.000 .

For more detailed information please contact: security@acticom.de