VOCAL Technologies
Ask Us or Call **+1-716-688-4675**

Search...

- Solutions
- Products
- Services
- About Us
- Contact Us

EAPoL – Extensible Authentication Protocol over LAN Software

Home → Secure Communication → EAPoL – Extensible Authentication Protocol over LAN Software

Extensible Authentication Protocol (EAP) over LAN (EAPoL) is a network port authentication protocol used in IEEE 802.1X (Port Based Network Access Control) developed to give a generic network sign-on to access network resources. EAPoL, similar to EAP, is a simple encapsulation that can run over any LAN. The same three main components are defined in EAP and EAPoL to accomplish the authentication conversation:

1. Supplicant (Port Authentication Entity (PAE) seeking access to netwrok resources)
2. Authenticator (PAE that controls network access)
3. Authentication Server (a RADIUS/AAA server)

The following figure shows how these LAN components are connected in a wired environment.
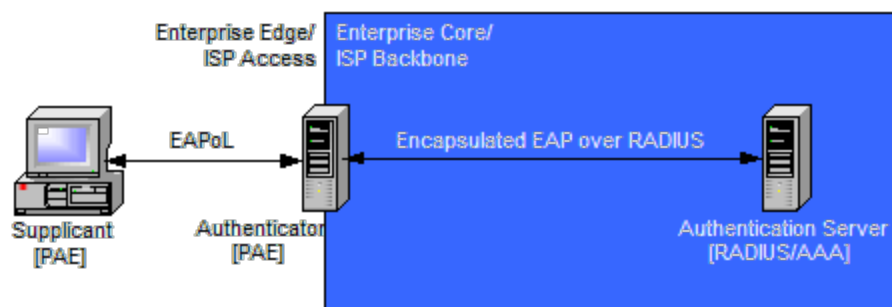
Figure 1: EAPoL Architecture

EAPoL Frame Format

MAC Header	Ethernet Type	Version	Packet Type	Packet Body Length	Packet Body	Frame Check Sequence
12 bytes	2 bytes	1 byte	1 byte	2 bytes	variable length	4 bytes

The fields in the frame are:

MAC Header

The first 6 bytes of the MAC header are the Destination Address and the last 6 bytes are the Source Address.

Ethernet Type

The Ethernet Type contains a 88-8e, this is the two byte type code assigned to EAPoL.

Version

In 2004 Version 2 was standardized, nothing has been satandardized since.

Packet Type

The Packet Type field is a byte long and represents the type of package the frame is.

Packet Type	Name	Description
0000 0000	EAP-Packet	Contains an encapsulated EAP frame (this is what majority of EAPoL frames are)
0000 0001	EAPOL-Start	A supplicant can issue an EAPOL-Start fram instead of waiting for a challenge from the authenticator

0000 0010	EAPOL-Logoff	Used to return the state of the port to unauthorized when the supplicant is finished using the network
0000 0011	EAPOL-Key	Used to exchange Cryptographic Keying information
0000 0100	EAPOL-Encapsulated-ASF-Alert	Provided as a method of allowing Alerting Standards Forum (ASF) alerts (ex. specific SNMP traps) to be forwarded through a port that is in the Unauthorized state
		All other possible values are reserved for future use

Packet Body Length

The Packet Body Length field is a 2 byte value representing packet body length (It is set to 0 when there is no packet body)

Packet Body

The Length field is two bytes long and contains the number of bytes in the entire packet. EAP assumes anything in excess of the Length is padding that can be ignored.

Frame Check Sequence

The Frame Check Sequence (FCS) is checksum value added to the frame for error detection and correction. A sample of a typical EAPoL exchange is shown in following figure.
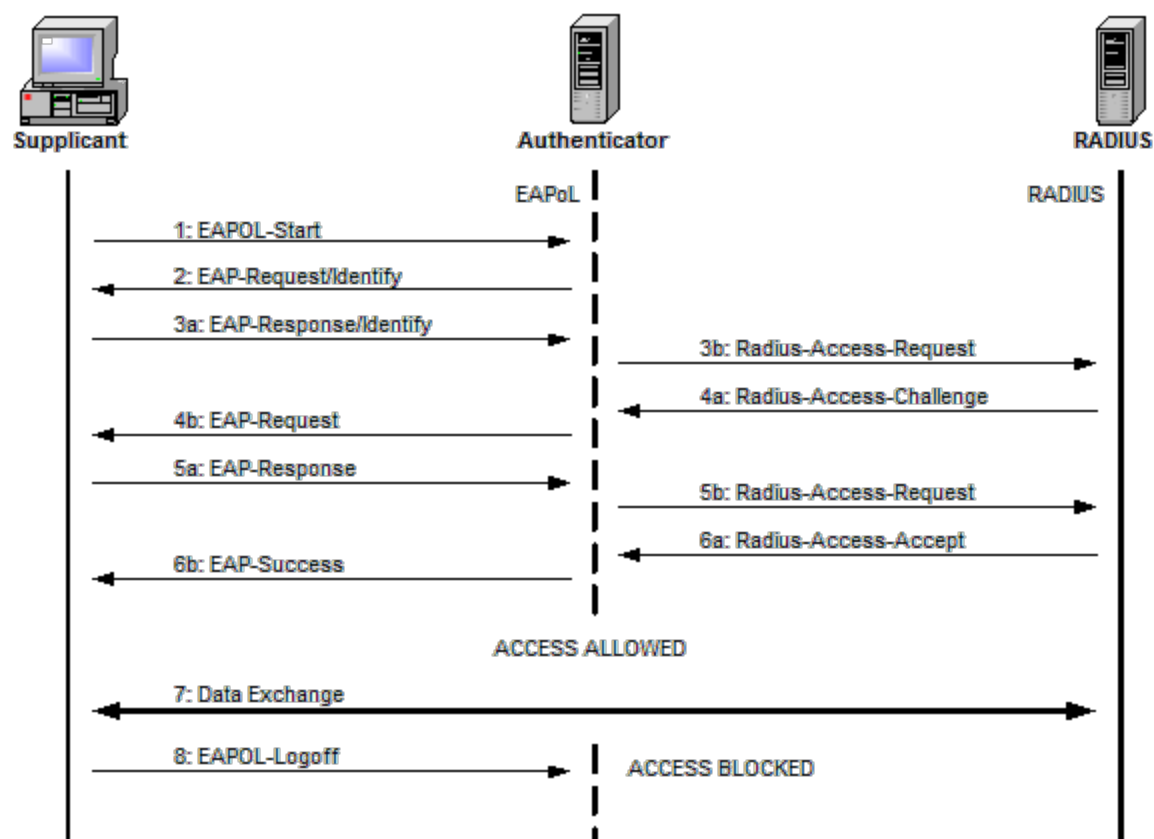
Figure 2: Sample EAPoL Exchange

IEEE 802.1X not only defines the EAP over LAN (EAPoL) implementation, but also the EAP over Wireless (EAPoW) for use with IEEE 802.11 for getting WEP key information.

Software Libraries

VOCAL's embedded software libraries include a complete range of ETSI / ITU / IEEE compliant algorithms, in addition to many other standard and proprietary algorithms. Our software is optimized for execution on ANSI C and leading DSP architectures from TI, ADI, AMD,Intel, ARM, MIPS and other vendors. These libraries are modular and can be executed as a single task under a variety of operating systems or standalone with its own microkernel.

- VoIP
- Mobile VoIP
- Lawful Intercept
- Voice
- Video
- Fax Modem
- Data Modem
- Speech Enhancement
- Echo Cancellation
- Noise Reduction

- Error Correction
- Cryptography
- Secure Communication
- Network
- Engineering
- System Designs
- Reference Designs
- Custom Designs

- Home
- About Us
- Sitemap
- Contact Us

VOCAL Technologies, Ltd.
520 Lee Entrance, Suite 202
Amherst New York 14228
Phone: +1-716-688-4675
Fax: +1-716-639-0713

© 2014 **VOCAL Technologies**

Back to Top