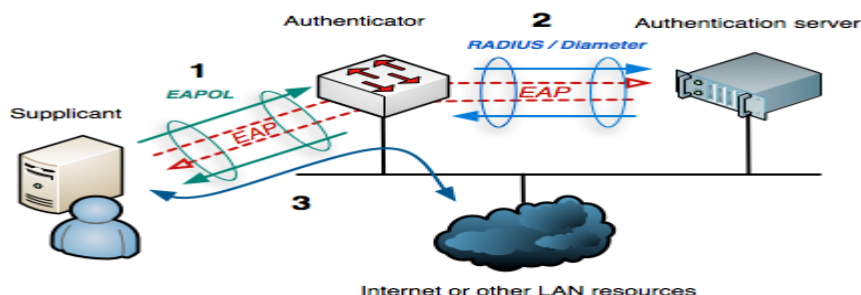


## IEEE 802.1X

**IEEE 802.1X** is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802,<sup>[1][2]</sup> which is known as "EAP over LAN" or EAPOL.<sup>[3]</sup> EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004.<sup>[4]</sup> The EAPOL protocol was also modified for use with IEEE 802.1AE ("MACsec") and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010<sup>[5][6]</sup> to support service identification and optional point to point encryption over the local LAN segment.

## Overview



EAP data is first encapsulated in EAPOL frames between the Supplicant and Authenticator, then re-encapsulated between the Authenticator and the Authentication server using RADIUS or Diameter.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The **supplicant** is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The **authenticator** is a network device, such as an Ethernet switch or wireless access point; and the **authentication server** is typically a host running software supporting the RADIUS and EAP protocols. In some cases, the authentication server software may be running on the authenticator hardware.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.