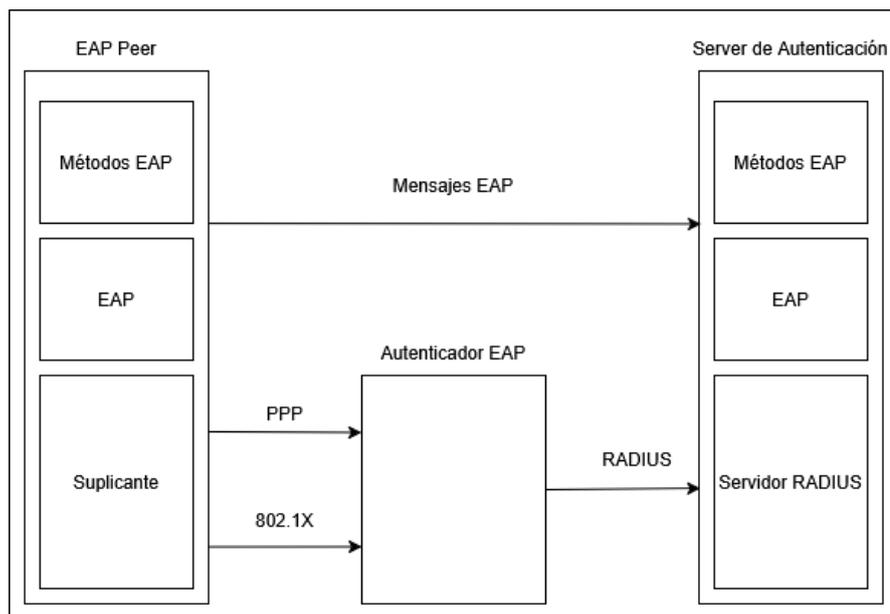


Control de Acceso Basado en Puertos (PBNAC en IEEE 802 LAN)

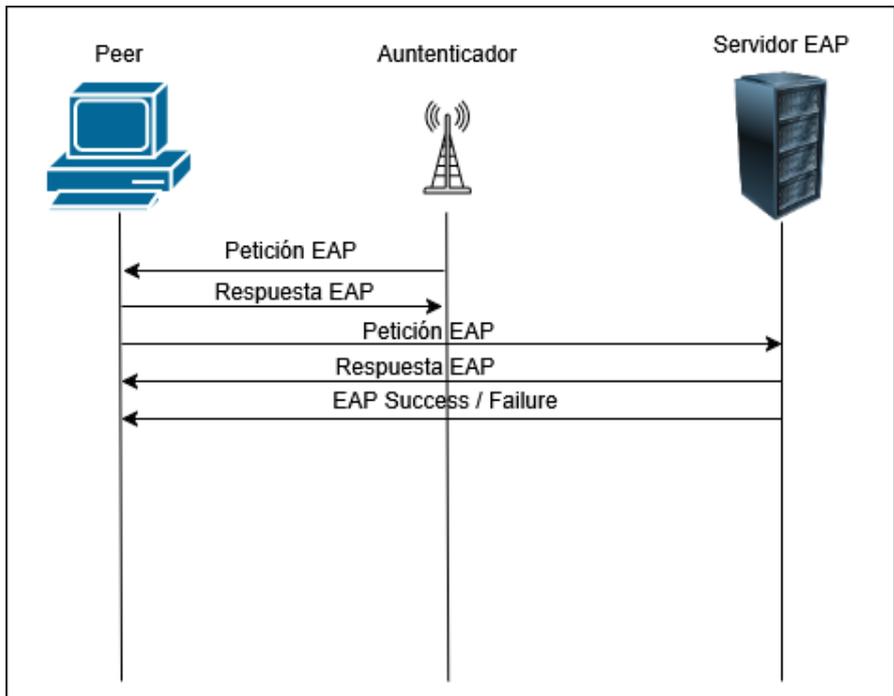
El Estándar 802.1X es un estandar para el PBNAC (Port Based Network Access Control). Provee mecanismos de autenticación para los dispositivos que se quieran conectar a la LAN o la WLAN. Los puertos del Switch están bloqueados por defecto hasta que se autentica el dispositivo conectado a este. La autenticación 802.1X involucra tres partes, un suplicante (Cliente), un autenticado (Switch/punto de acceso) y un Servidor de Autenticación.

802.1X y EAP

El Extensible Authentication Protocol (EAP) es un marco de autenticación de capa 2, no es un mecanismo de autenticación específico. Provee funciones comunes y metodos de negociación de autenticación llamados Métodos EAP.



EAP define formatos genéricos de autenticación: Request, Response, Success, Failure. El tipo de autenticación EAP especifica los mecanismos de autenticación seleccionados y el tipo de credenciales.



EAPOL y RADIUS

EAP suele correr directamente sobre la capa de enlace de datos como el protocolo Point to Point (PPP) o el IEEE 802. 802.1X define la encapsulación de EAP sobre 802, conocido como EAP over LAN (EAPOL).

Remote Access Dial-In User Service (RADIUS) se usa para sistemas centralizados de autenticación de usuarios. Define mensajes entre el Network Access Server (NAS) y el Authentication Server.

- el NAS envía un Access Request
- El Authentication Server responde con un Access Challenge, Access-Accept o Access-Reject.

EAP se encapsula en el Access-Request y Access-Challenge de RADIUS. RADIUS tiene su propio protocolo de seguridad basado en un Secreto compartido entre los extremos.

Seguridad de Radius

El servidor NAS y el RADIUS comparten la clave secreta. Las respuestas del Servidor de Autenticación contienen un autenticador, una petición genérica,

From:
<https://knoppia.net/> - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:secom:tm3

Last update: **2026/02/18 16:43**

