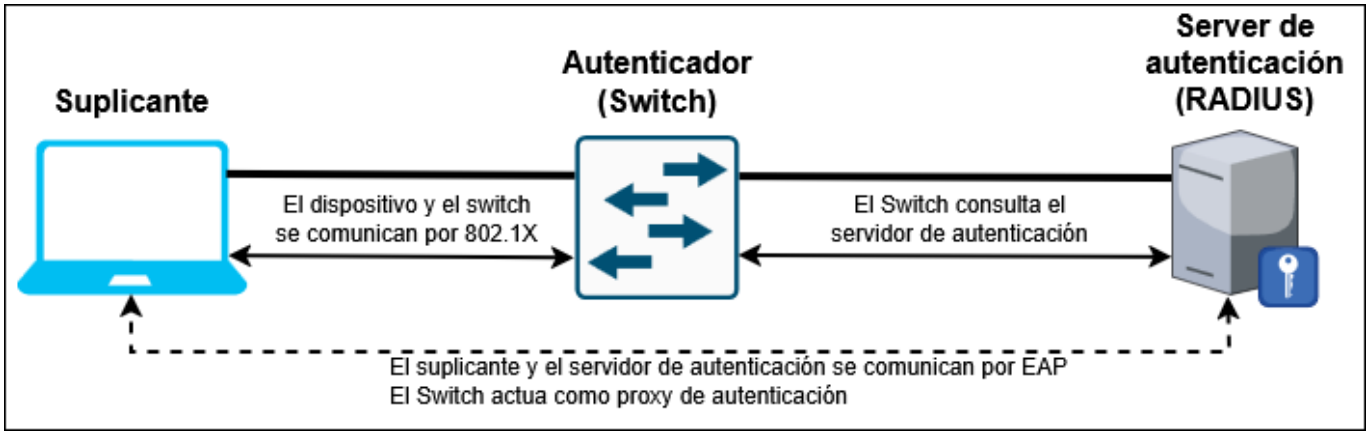
Seguridad a Nivel de Enlace

PBNAC en IEEE 802 Local Area Networks

802.1X es un estándar IEEE para control de acceso basado en puertos (PBNAC). Forma parte del grupo IEEE 802.1 de protocolos de red. Provee mecanismos de autenticación para dispositivos que se quieren conectar a una LAN o una WLAN. Los puertos del switch están bloqueados por defecto hasta que el dispositivo conectado sea autenticado correctamente en alguna entidad de seguridad de la infraestructura. La autenticación 802.1X involucra 3 partes:

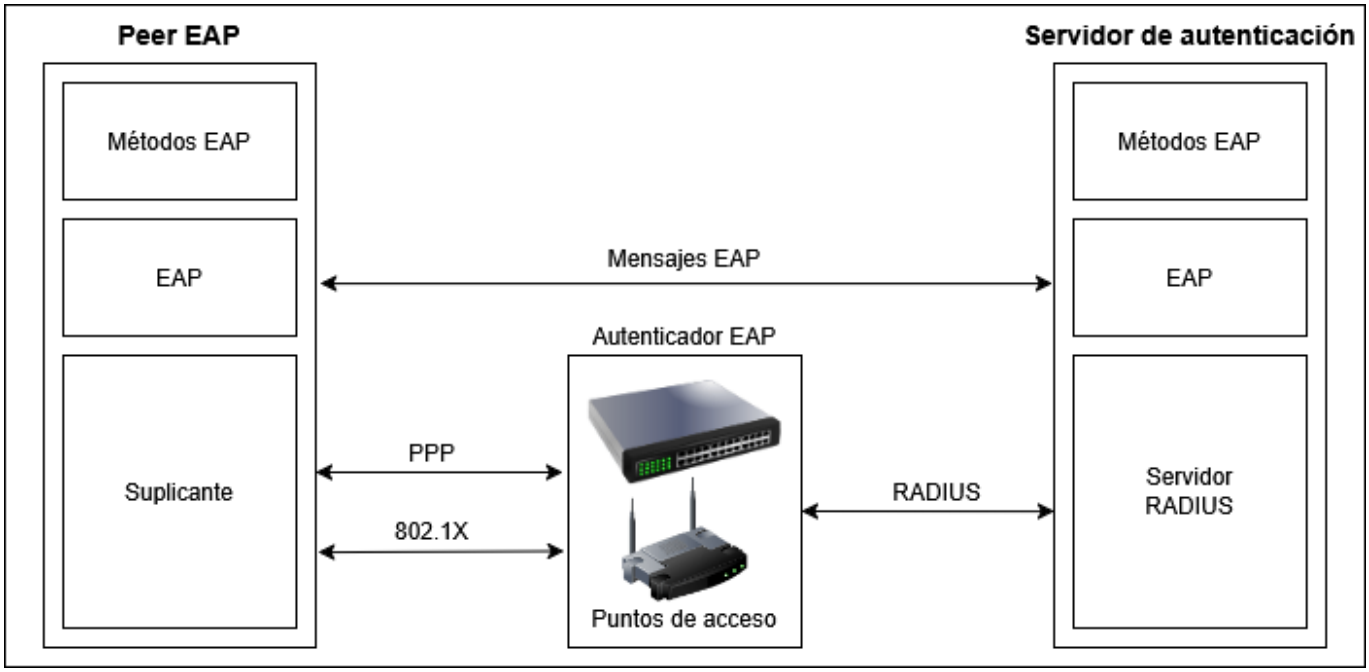
- Suplicante: Dispositivo cliente
- Autenticador: Switch o Punto de acceso
- Servidor de autenticación



Extensible Authentication Protocol (EAP)

Es un framework de autenticación de capa 2, no es un mecanismo de autenticación. Provee algunas funciones comunes y metodos de negociación de autenticación llamaods métodos EAP.

- La autenticación es proveida por el protocolo interno dentro de EAP, no por EAP
- Se usa en 802.1X entre el suplicante y el servidor de autenticación
- En EAP al suplicante se le llama peer, reflejando la idea general de que EAP podría ser usado para autenticación mutua entre entidades equivalentes.
- Facilita la implementación de entidades de autentiación intermedia o autenticadores en redes donde la gestión de usuarios está centralizada.



EAP define formatos de mensajes de autenticación genéricos

- Request
- Response
- Success
- Failure

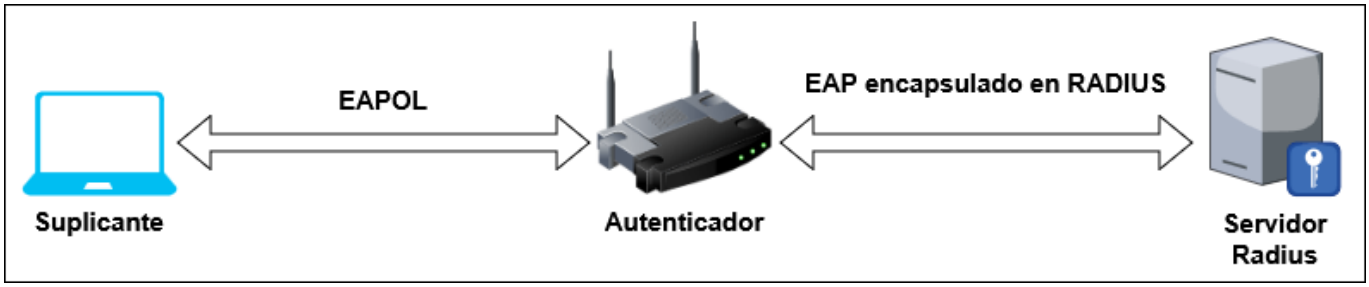
El campo “Tipo de autenticación EAP” esoecifica el mecanismo de autenticación elegido, el tipo de credenciales y como usarlas para realizar la autenticación mutua de forma segura. Hay tres tipos especiales de EAP:

- Identidad
- Notificación
- Nak

EAPOL y RADIUS

EAP normalmente funciona a nivel de enlace como Point-to-Point Protocol (PPP) o IEE802 sin requerir una IP. 802.1X define la encapsulación de EAP sobre medios IEEE802 cableados, conocidos como EAP Over LAN (EAPOL). Si el autenticador y el servidor de autenticación no están ubicados conjuntamente, los mensajes EAP deben encapsulados en otro protocolo para ser entregados al servidor de autenticación, ocurriendo lo opuesto en una dirección inversa.

RADIUS (Remote Access Dial-In User Service) define sus propios protocolos de transporte para comunicación entre un Autenticador y un servidor RADIUS AAA. EAP se encapsula en atributos de RADIUS.



RADIUS

Define mensajes entre el El Servidor de Acceso a la Red (NAS) y el servidor de autenticación:

- el NAS envía un Access-Request
- El server de Autenticación responde con Access-Challenge, Access-Accept o Access-Reject

Se encapsula EAP en el Access-Request y Access-Challenge de RADIUS todas las veces que sea necesario.

- EAP-Message-attribute
- El Message-Autenticator Atribute es obligatorio para paquetes RADIUS transportando EAP-message Attributes.

Radius tiene su propio protocolo de seguridad basado en una clave compartida entre los endpoints (NAS y Server RADIUS)

Seguridad de RADIUS

Las respeustas del servidor de autenticación contienen un auntenticador, las peticiones genéricas de los clientes no son autenticadas

- Authenticator = (code|id|length|requestAuth|Attributes|Shared Secret)
- RequestAuth es un nonce del NAS.

Si un paquete RADIUS transporta mensajes EAP, debe usar el atributo “Message-Authenticator” (Shared Secret, Code|ID|Length|RequestAuth|Attributes). Radius tiene su propia función key wrap para ocultar atributos confidenciales usando la clave compartida. Si un métido EAP de autenticación genera mateial de clave (Master Session Key), el Pairwise Master Key (PMK) deruvadi de MSK es enviado en un paquete Access-Accept RADIUS del server al NAS cifrado con la clave compartida.

Seguridad EAP-RADIUS

- Radius es vulnerable a ataques de diccionario.
  - Las claves compartidas tienen un tiempo de vida muy largo, muchos mensajes van en texto plano con su respectivo autenticador.
  - Se usa MD5, que es altamente vulnerable
- Otros problemas están relacionados con privacidad, spoofing, hijacking, ataques replay, ataques de negociación, antaques de suplantación, Man in the middle…
- RADIUS recomienda usar un mecanismo de autenticación bidireccional y tencnología IPSEC para

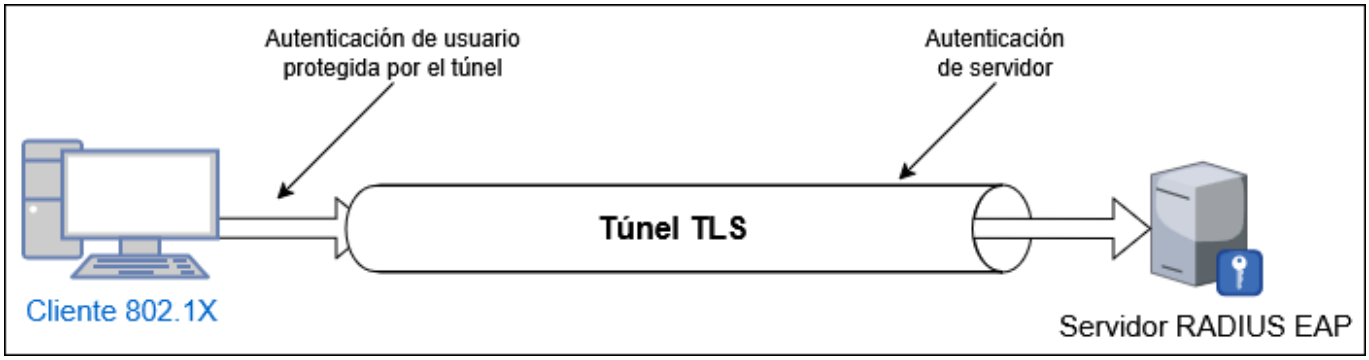
proteger la comunicación entre el NAS y el autenticador.

Mencanismos de autenticación basados en EAP

- EAP-TLS: Autenticación mutua durante el handshake inicial que establece el tunel tls. se requieren certificados X509 en ambos lados
- EAP-TTLS (EAP Tunneled TLS): Autenticación mutua, solo el server AAA necesita certificado X509. Normalmente la antenticación del cliente se hace usando contraseñas compartidas. .
- PEAP (Protected EAP): Similasr a EAP-TTLS. El mecanismo de autenticación del suplicante usa EAP para transportar las credenciales del cliente.
- EAP-FAST (EAP Flexible Authentication via Secure Tunneling): No es necesario el uso de clientes o certificados de servidor. Usa PAC (Protected Access Credentials) para establecer el tunel TLS. Tiene 3 fases, PAC Provisioning, TLS Tunnel stablishment y Authentication.

Autenticación a través de un túnel TLS

Los credenciales de usuario son vulnerables a ataques de diccionario. Transimir infomración dentro de un tunel TLS previene que un atacante puede acceder a dichos credenciales. El túnel TLS se establece utilizando el certificado del servidor, autenticando en un primer momento el final de la conexión. Tras eso, se usa el tunel cifrado para enviar las credenciales del cliente de forma segura.



Secure Association Protocol

El acceso puede ser denegado para un peer autenticado debido a la ausencia de autorización u otras razones. Un peer sin credenciales de acceso o que ha fallado el proceso de autenticación puede tener acceso a la red para un servicio o para una VLAN de invitados. El completar la autenticación por parte de un perr y un server eap no significa que tenga acceso inmediato a la red, una Security Asociation entre el EAP per y el Authenticator debe ser establecida con el Secure Association Protocol.

MACsec

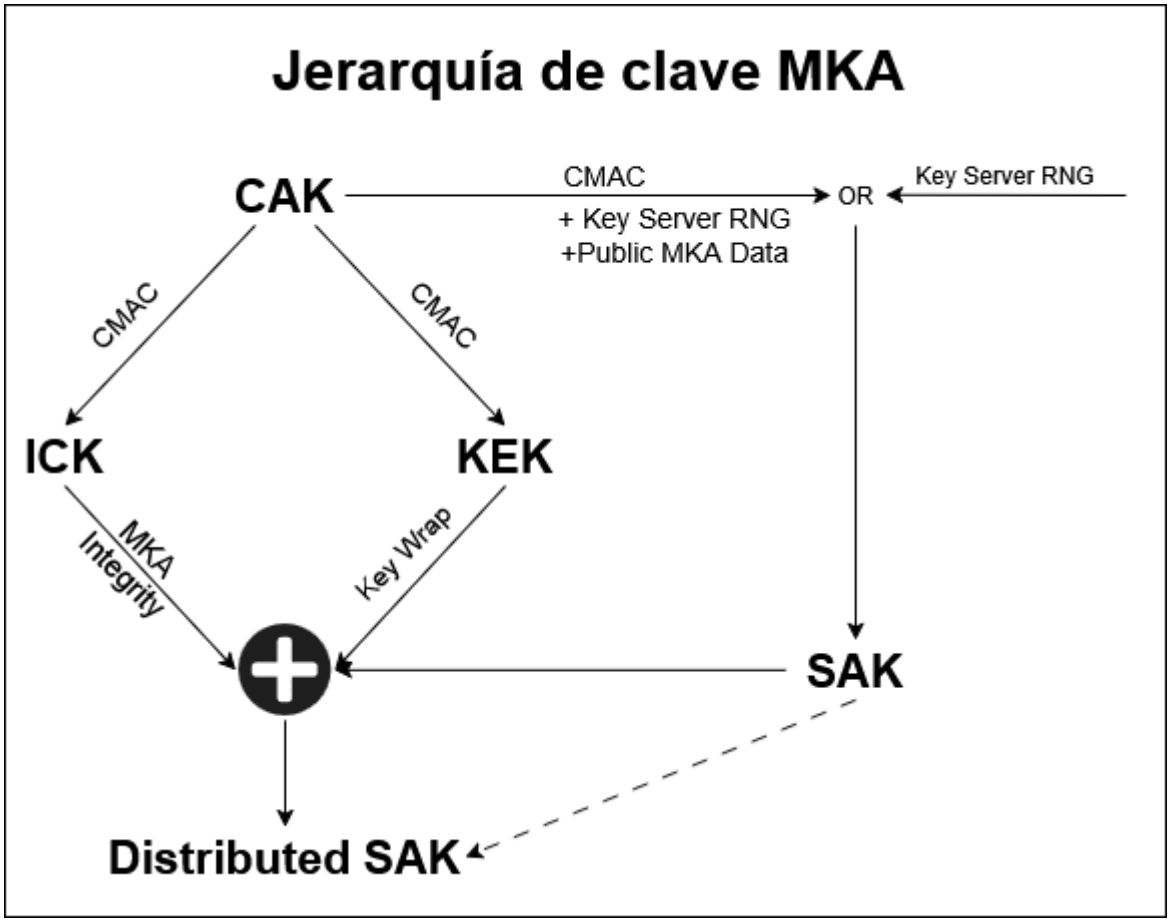
Es el cifrado de conexiones ethernet cableadas (IEEE 802.1AE). Cifrado en la capa MAC, cifrado a la velocidad del cable. MACsec garantiza lo siguiente:

- Integridad de los datos sin conexión
- Autenticidad de los datos de origen
- Confidencialidad

- Protección contra replay
- Limita la naturaleza y extensión de los ataques de denegación de servicio.

Definiciones MACsec

- Secure Connectivity Association (CA): Relacion de seguridad establecida y mantenida por protocolos clave de acuerdo (MKA), que compone un subset de puntos de awcceso a servicio completamente conectados en estaciones conectadas a una sola LAN.
    - Secure Connectivity Association Key (CAK): Clave secreta poseida por los miembros de la CA
    - Secure Connectivity Assiciation Key Name (CKN): Texto que identifica un CAK
    - CAK y CKN son derivados del material ram del keyring que el método EAP inyectó en el suplicante y auntenticador.
    - Cada CA tiene un key server elegido dinámicamente.
    - Un key server perteneciente a varias CA con peers en el mismo segmento puede crear un grupo CA.
- Secure Association (SA): Relación de seguridad que provee garantías de seguridad para los marcos transmitidos de un miembro de la CA a otro.
    - Cada SA está soportado por una sola secret key o un solo set de claves donde la operación utilizada para proteger un marco necesita más de una clave.
    - SA es unidireccional.
- Secure Association Key (SAK): La clave secreta usada por una SA.
- Secure channel (SC): Un SC es soportado por una secuencia de SAs, permitiendo el uso periódico de claves nuevas sin terminar la relación.
- MACsec Key Agreement (MKA): Protocolo IEEE802.1X. Puede descubrir miembros ya autenticados en una CA conectadas a la misma lan. Puede confirmar la posesión mutua de CAK para probar autenticación mutua pasada. Asegura que los datos protegidos por MACsec no tienen retraso.
    - Usa marcos EAPOL-MKA para el intercambio de información
    - Asegura transporte multipoint-to-multipoint completamente distribuido.
    - Si no se implementa un MKA, mACsec puede seguir siendo usado para cifrar datos si los peer finales estan configurados de forma estática.



- Mensaje de Codigo de autenticación con cibrado basado en ASES (CMAC)
- CAK es el PMK que el Server de Autenticación entrega al Autenticador en RADIUS Access-Accept.
- Durante el diálogo EAP entre métodos equivalentes en el server de autenticación y el suplicante, este último obtiene el MSK y deriva el PMK (CAK)
- Es estándar tambien cosidera la posibilidad de la configuración manual de CAK y CKN en ambos extremos del enlace.

Seguridad de LAN Inalámbricas IEEE 802.11i