Wireless LAN

- Setup & Optimizing Wireless Client in Linux
- Hacking and Cracking Wireless LAN
- Setup Host Based AP (hostap) in Linux & freeBSD
- Securing & Managing Wireless LAN : Implementing 802.1x EAP-TLS PEAP-MSCHAPv2 , FreeRADIUS + dialupadmin + MySQL (FULL DEMO ☺)
- Make Deep Security with WPA2

  Wifi Protected Access = 802.1x + (TKIP or CCMP)

Wireless LAN Security

Protecting a WLAN involves three major elements:

- Authenticating the person (or device) connecting to the network so that you have a high degree of confidence that you know who or what is trying to connect.
- Authorizing the person or device to use the WLAN so that you control who has access to it.
- Protecting the data transmitted on the network so that it is safe from eavesdropping and unauthorized modification.

http://go.microsoft.com/fwlink/?LinkId=23481

Port-Based Network Authentication

- What is 802.1x ?

  “Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of *authenticating* and *authorizing* devices attached to a LAN port that has point-to-point connection characteristics, and of *preventing access* to that port in cases which the authentication and authorization fails. A port in this context is a single point of attachment to the LAN infrastructure.”

  http://standards.ieee.org/getieee802/download/802.1X-2001.pdf
  http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.html

- What is EAP ?

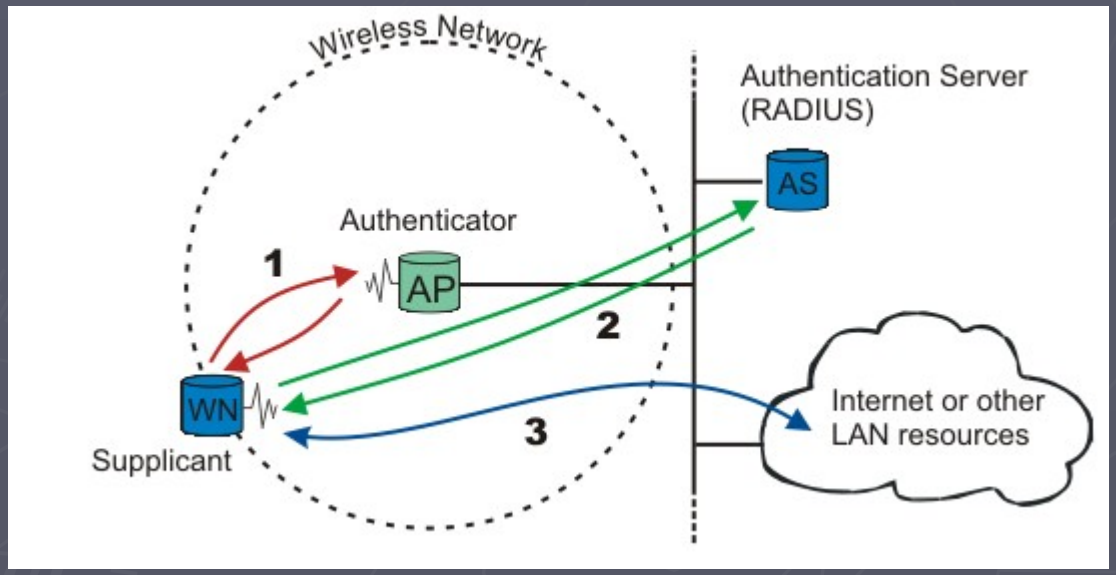
  Extensible Authentication Protocol (EAP)

  A flexible protocol used to carry arbitrary authentication information over PPP

  It used by supplicant and authenticator to communicate

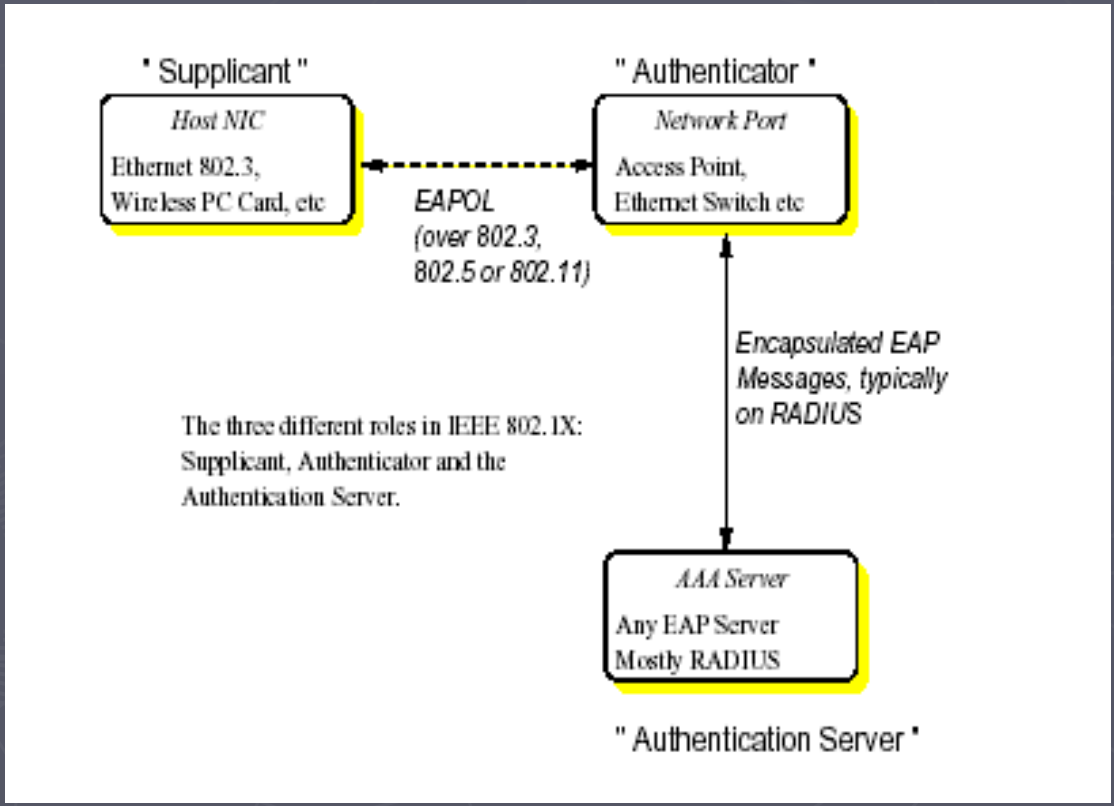
  http://www.ietf.org/rfc/rfc3748.txt

- It requires entitie(s) to play three roles in the authentication process: that of an **supplicant**, an **authenticator** and an **authentication server**



http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.html

The authenticator (Access Point) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information



EAP authentication methods

- EAP-MD5
- EAP–TLS
- EAP-Tunneled TLS (TTLS)
- EAP-Protected EAP (PEAP)
- EAP-Lightweight EAP (LEAP)
- EAP-MSCHAPv2
- PEAP-MSCHAPv2

- ***EAP-MD5***

  MD5-Challenge requires sername/password and is equivalent to the PPP CHAP protocol [RFC1994]. This method does not provide dictionary attack resistance, mutual authentication or key derivation and has therefore little use in a wireless authentication enviroment.

  http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.

- ***EAP-Transport Layer Security (EAP-TLS)***

  It uses public key certificates to authenticate both the wireless clients and the RADIUS servers by establishing an encrypted TLS session between the two. Provides mutual authentication, negotiation of the encryption method, and encrypted key determination between the client and the authenticator

  http://www.ietf.org/rfc/rfc2716.txt

  http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.

- ***EAP-TTLS***

  Sets up a encrypted TLS-tunnel for safe transport of authentication data. Within the TLS tunnel, (any) other authentication methods may be used. Developed by Funk Software and Meetinghouse and is currently an IETF draft.

  http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.

- ***EAP-Protected EAP (PEAP)***

  Uses, as EAP-TTLS, an encrypted TLS-tunnel. Supplicant certificates for both EAP-TTLS and EAP-PEAP are optional, but server (AS) certificates are required. Developed by Microsoft, Cisco and RSA Security and is currently an IETF draft.

  http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.

- ***EAP-MSCHAPv2***

  Requires username/password and is basically an EAP encapsulation of MS-CHAP-v2 [RFC2759]. Usually used inside of a PEAP encrypted tunnel. Developed by Microsoft and is currently an IETF draft.

  http://www.gnist.org/%7Elars/courses/04thales/8021X-HOWTO.

- ***PEAP-MSCHAPv2***

  Combination of Protected EAP (PEAP) and EAP-MSCHAPv2

RADIUS (Authentication Server)

- Remote Authentication Dial-In User Service (RADIUS) http://www.ietf.org/rfc/rfc2865.txt
- the "de-facto" back-end authentication server used in 802.1X.
- AAA (Authentication, Authorization and Accounting) Support
- FreeRADIUS is a fully GPL'ed implemented RADIUS server

  http://www.freeradius.org