

Wireless networks authentication

There are three main authentication methods:

- Open authentication
- Shared authentication
- EAP authentication

Open authentication

It is the simplest of these methods. There is no verification of the user or machine. Open Authentication allows any device that places an authentication request to the access point. If no encryption is enabled, any device that knows the SSID of the WLAN can gain access into the network. The problem with this method is that the SSID can be easy to figure out even if it is not broadcasted, with passive capturing techniques.

Shared authentication

method is commonly used on individual and small business wireless LAN implementations. Both sides of the connection are given a shared key, if they match then the device is allowed onto the network.

EAP

Extensible Authentication Protocol, or EAP, is an authentication framework used in wireless networks and Point-to-Point connections. EAP is not a specific authentication mechanism. It provides some common functions and negotiation of authentication methods called EAP methods. There are about 40 different methods defined.

EAP-authentication

Local EAP is a mechanism in which the wireless LAN controller (WLC) acts as an authentication server. User credentials are stored locally on the WLC to authenticate wireless clients, which acts as a backend process in remote offices when the server goes down. User credentials can be retrieved either from the local database on the WLC or from an external LDAP server. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC are different EAP authentications supported by local EAP.

LEAP

The **Lightweight Extensible Authentication Protocol** (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys don't live long enough to be cracked).

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 that want to attach to a LAN or WLAN.

There are three parties in 802.1X authentication:

1. Supplicant - is a client device (e.g. laptop) wishing to attach to the LAN/WLAN.
2. Authenticator - is a network device, such as an Ethernet switch or wireless access point
3. Authentication server - is typically a host running software supporting the RADIUS and EAP protocols

Until the supplicant's identity has been validated and authorized, the supplicant is not allowed access through the authenticator to the protected side of the network. With 802.1X port-based authentication, the supplicant provides credentials(e.g 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 is allowed to access resources located on the protected side of the network.

Sources:

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/68583-FAQ-Wireless-Security.html>

http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

<http://blog.pluralsight.com/wireless-encryption-authentication>

http://en.wikipedia.org/wiki/IEEE_802.1X

http://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol

<http://archive.is/J5Jv>

Author : Silvia Vigašová, 409781