LANCOM Techpaper

LEPS / PPSK (private pre-shared key)

The encryption methods WPA2 and WPA3 protect data traffic in the WLAN from interception. The required passphrase is easily handled as a central key; there is no need for a RADIUS server as required for 802.1X installations.

Nevertheless, these encryption methods do have some shortcomings:

- **A single passphrase (pre-shared key, PSK) applies globally for all WLAN clients**
- **Without careful treatment, the passphrase may fall into unauthorized hands**
- **The leaked passphrase then offers attackers free access to the wireless network**

In practice this means that: If the passphrase goes missing or an employee with knowledge of the passphrase leaves the company, then the passphrase in the access point needs to be changed in the interests of security—and consequently in each and every WLAN client, too. As this is not always possible, an improvement would be to have an individual passphrase for each user in the WLAN instead of a global passphrase for all WLAN clients.

Since early 2000, LANCOM's LEPS-MAC (LANCOM Enhanced Password Security MAC) has allowed operators to avoid the insecurities of using a global passphrase. As of LCOS 10.20, LANCOM offers a further highly efficient method based on the PPSK method and called LEPS-U (LANCOM Enhanced Passphrase Security User). With LEPS-U, you have the ease of configuration of IEEE 802.11i plus passphrase, while

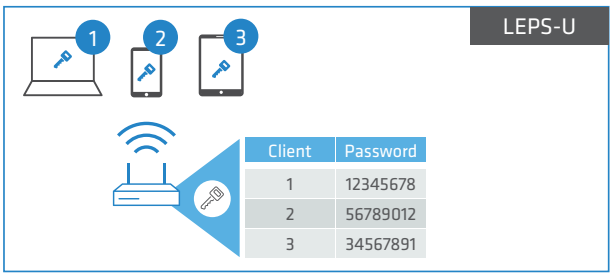
at the same time avoiding the potential security loopholes that come with global passphrases.

With LEPS-U you assign an individual WLAN password as a private pre-shared key (PPSK) for an SSID to individual users or entire groups. Using LEPS-MAC, you additionally authenticate the clients by their MAC address, which is ideal for secure corporate networks.

LANCOM Enhanced Passphrase Security User (LEPS-U)

LANCOM Enhanced Passphrase Security Users (LEPS-U) allows a set of passphrases to be configured for WPA2 (PPSK method) and assigned to individual users or groups. This avoids having one global passphrase for an SSID. Instead, there are several passphrases, which can then be distributed individually.

This is useful for onboarding devices into the network. For example, a network operator onboarding multiple WLAN devices into different areas of the network does not want to configure each individual device; instead this should be done by the users of the devices themselves. In this case, users are given a pre-shared key for the company WLAN for use with their own devices. The pre-shared key is used

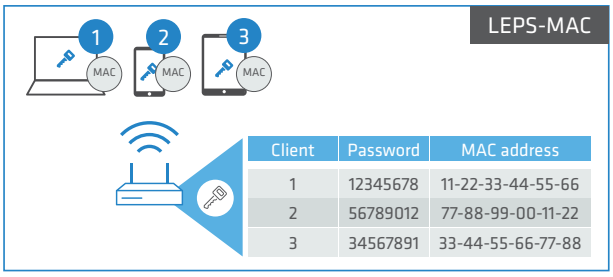


to map each user to a VLAN, which automatically assigns them to a specific network. The configuration of LEPS-U takes place on the infrastructure side only, so assuring full compatibility to third-party products.

The security issue presented by global passphrases is fundamentally remedied by LEPS-U. Each user is assigned their own individual passphrase. If a passphrase assigned to a user should get lost or an employee with knowledge of their passphrase leaves the company, then solely the passphrase of that user needs to be changed or deleted in order to close the security loophole. All other passphrases remain valid and confidential.

LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)

LEPS-MAC provides an additional column in the access control list (ACL) and it assigns an individual passphrase to each MAC address.



Authentication at the access point is only possible with the correct combination of passphrase and MAC address. This unique combination of passphrase and MAC address makes the spoofing of the MAC addresses futile—and LEPS-MAC thus shuts out a potential attack on the ACL. If WPA2 or WPA3 is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN, because knowledge of both the MAC address and the passphrase is required before encryption can be negotiated.

LEPS-MAC can be used both locally in the device and centrally managed by a RADIUS server. It works with all WLAN clients available on the market without any modification. Full compatibility to third-party products is further assured as LEPS-MAC only involves configuration in the access point (directly or indirectly by RADIUS).

Compared to LEPS-U, the administrative overhead with LEPS-MAC is slightly higher because the MAC address has to be entered for each device.

Summary

Keep full control of who is in your WLAN with private pre-shared keys (PPSK) via LEPS. With LEPS-U you assign an individual WLAN password (private PSK) for an SSID to individual clients or entire groups. Using LEPS-MAC, you additionally identify the clients by their MAC address.

LEPS combines the ease of configuration of IEEE 802.11i plus passphrase, while at the same time avoiding the potential security loopholes that come with global passphrases.