Chapter 5

Conclusions

In these few years, the security holes of wireless LANs have become a high priority issue that need to be resolved as soon as possible. Although the IEEE organization had published the 802.1x standard in 2001 and proposed a brand new specification 802.11i draft for the future use, it could require additional equipments (servers), more computations, or protocol replacement. Our Round-Robin key management, shown in this article, is very simple scheme for host authentication and WEP group key management. It has the following advantages:

- The simple methodology takes very limited extra-effort, and no additional equipments needed. Only firmware updated is required.

- Instead of protocol replacement, it is the extension of conventional IEEE

802.11. That provides a great capability in compliance with current vast IEEE 802.11 device.

- It can easily and rapidly revoke those unwelcome hosts from accessing the wireless network.
- Seamlessly and periodically key updated skips the possible weakness of WEP (RC4) protocol.
- Minimize the same key used, even the pre-shared secret key is only used in authentication phrase.
- Both AP and station can verify each other according to its individual key.

Finally, we believe the Round-Robin key management is very simple, efficient, and more trusty than IEEE 802.11. It will be pretty fit for small or home office (SOHO) environment.