The Chinese University of Hong Kong
Department of Information Engineering

IERG 4841 Networking Laboratory II
Enterprise level Wireless LAN setup module
(Lab Sheet)

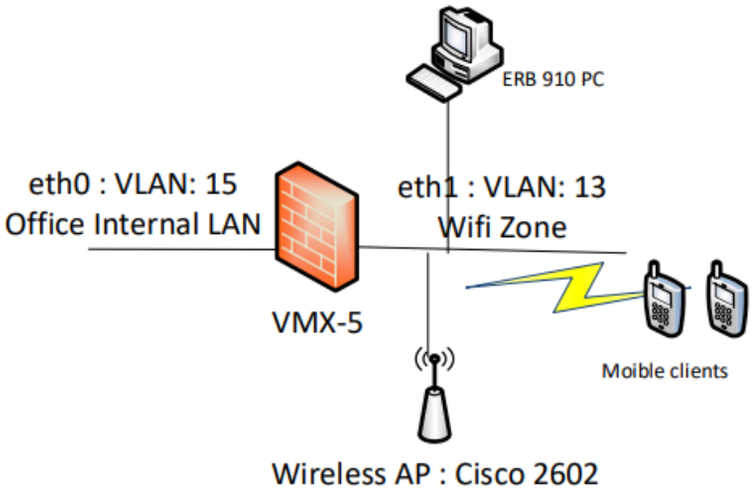
Updated at Jan 2022 By Peter S F Luk

History

Wireless LAN is an indispensable part of the network nowadays. However, the security of it is often commented by others as very weak and problematic. In this module, you will learn techniques and building blocks to build a secure enterprise-level wireless LAN.

Missions

Use the provided Cisco Aironet 2602 Access points, the host vmx-5 (centos 6) and the Rm910 PC will be used to build an enterprise wireless LAN with different level of security and authentication settings like captive web gateway, WPA, 802.1x EAP (the protocol used by the ssid : eduroam & CUHK1x) and RADIUS, etc



Setup Procedures

- Setup the basic IPv4 network structure as prelab
  - Configure VLAN13 as the wifi zone
  - Import VMX-5 from the template using the procedures stated in Lab 2 for IP forwarding and NAT for wireless clients (it should be able to reach internet). There will be two network interfaces for it. Eth0 will be connected to VLAN15 and eth1 will be connected to VLAN13
  - Configure IP forwarding, NAT and DHCP service on VMX-5 so that all clients connected to VLAN13 will be assigned an ip from it and will be able to reach internet
  - Re-reconfigure uplink of ERB910 PC to VLAN13 and make sure it can get an ip from VMX-5
- In the above diagram, please note that all the wireless LAN traffic should route and NAT via VMX-5. The web portal and radius server used in task 2 should be installed and configured on VMX-5.

Task 1 : Basic Access Point configuration

- Press and hold the MODE button while you power on the access point to reset AP to the default configuration
- Hold the MODE button until the Status LED turns amber (approximately 10 to 20 seconds), and release the button
- Configure the switch port of the Access point connected to VLAN13. The same VLAN of eth1 of VMX-5 and your client PC in Rm910 as shown in the above diagram
- Use the DHCP server in VMX-5 to assign an ip to THE Cisco Aironet 2602 Access point ethernet interface so that the client PC in Rm910 can connect to the access points for the configuration via telnet or browser (The Access point use the default IP address 10.0.0.1 the first it power up if there's no DHCP server to assign it an ip. The default login name and password for it is Cisco)
- connect to the access points using its assigned ip via telnet or web access. Create a HIDDEN SSID : wave*yourgrpno* (eg: wave1, if you are group 1, etc) and an assigned WPA pre-shared key
- If you find the AP cannot get the ip from your DHCP server, you can try to debug connect to the serial console of the AP (by pressing the button with the label AP of the DB9 switch similar to the procedures of connecting serial console of your network switch, router and ASA)

Checkpoint 1

- Use your notebook or mobile devices to connect to your access point's hidden SSID via WPA and surf the internet.
- Record down your procedures of configuration and hand in as your lab report

Special Precaution after finishing task 1

- **You must unplug your Access point after testing and never leave it turned on in the room without any attention.**

Task 2 : Configuration of a Linux based captive portal

- Download coovachilli from https://staff.ie.cuhk.edu.hk/~sfluk/4941/coova-chilli-1.3.0.tar.gz, compile and install
- Download haserl from https://staff.ie.cuhk.edu.hk/~sfluk/4941/haserl-0.9.26.tar.gz, compile and install
- Configure captive portal coovachilli on VMX-5. Refer to the reference section for the procedures.

Checkpoint 2

- Use the wifi client to connect to your access point's hidden SSID and launch the browser and it should be redirected to your webportal for a login name and password. After you entering the login name and password, your wifi client should be able to surf the internet.
- Record down your procedures of configuration and hand in as your lab report
- You need to demo this checkpoint to the tutor before proceeding to task 3

Task 3: Securing WLANs with WPA and FreeRADIUS EAP/PEAP

- Stop the linux web portal and restore the setting of Task 1 if it has any changes as the web portal setting will interfere with the setting of this task
- Build your CA and use it to generate a server certificate for your radius server. You can use easyrsa from OpenVPN (downloadable from internet or from http://staff.ie.cuhk.edu.hk/~sfluk/4941/) to do so or you can use the openssl command directly
- Compile freeradius 1.1.8 (get the freeradius source tar, the required libtool-ltdl and libtool-ltdl-devel rpms from http://staff.ie.cuhk.edu.hk/~sfluk/4941/)
- Configure your compiled radius, your Access point so that your wifi client can use the WPA + EAP-PEAP protocol (the protocol used by the ssid : eduroam &CUHK1x) to authenticate and surf the internet. Read the provided HOWTO in the reference section carefully

Checkpoint 3

- Use your wifi client to connect to your access point's hidden SSID using WPA EAP-PEAP and launch the browser and it should be able to surf the internet.
- Record down your procedures of configuration and hand in as your lab report. Moreover, in your lab report, compare the pros and cons of the web portal encryption + authentication and the WPA + EAP-PEAP encryption + authentication. If you are the IT consultant of your company, which method you would recommend to your senior management?? Discuss in your Lab report

References

- Startup Guide of Cisco Aironet 2602 https://staff.ie.cuhk.edu.hk/~sfluk/4941/2602-start.pdf
- Configuration Guide of Cisco Aironet 2602 Access Point http://staff.ie.cuhk.edu.hk/~sfluk/4941/2602-configuration.pdf
- CoovaChilli : An open source captive portal; http://www.coova.org/CoovaChilli
- EasyHotspot in Centos 6.4 + CoovaChilli 1.3.0 (please only refer to the **Install CoovaChilli section and skip other non-related part)** https://staff.ie.cuhk.edu.hk/~sfluk/4941/Easyhotspot%20in%20Centos%206.4%20CoovaChilli%201.3.0.html
- Working configuration used by IE Dept. for coovachili https://staff.ie.cuhk.edu.hk/~sfluk/4941/config.txt
- The free radius project

http://www.freeradius.org/

- Setup FreeRADIUS with EAP-PEAP
  http://staff.ie.cuhk.edu.hk/~sfluk/4941/Authentication%20Server%20%20Setting%20up%20FreeRADIUS.htm
- HOWTO: Incremental Setup of FreeRADIUS Server for EAP authentications (also teach you how to do debugging at command line using a tool : eapol_test)
  http://staff.ie.cuhk.edu.hk/~sfluk/4941/HOWTO%20%20Incremental%20Setup%20of%20FreeRADIUS%20Server%20for%20EAP%20Authentications.htm
- Paranoid Penguin - Securing WLANs with WPA and FreeRADIUS
  http://staff.ie.cuhk.edu.hk/~sfluk/ieg3841/wpa-1.htm
  http://staff.ie.cuhk.edu.hk/~sfluk/ieg3841/wpa-2.htm
- http://staff.ie.cuhk.edu.hk/~sfluk/ieg3841/wpa-3.htm