

A Remote WIFI Laboratory for Engineering Education

C.J.M. Uiterwijk, R.M. Kamphuis

Hogeschool Utrecht, Faculty of Engineering, Utrecht, The Netherlands

Abstract—Continuing need for available distance learning facilities has led to the development of a remote lab facility focusing on wireless technology. In the field of engineering there is a student need of gaining experience in set-up, monitoring and maintenance of 802.11A/B/G based wireless LAN environments.

Index Terms—802.11B/G, Access network, IMS band, Network security, Radius Server, Remote laboratory, Virtual access points, WIFI, Wireless LAN

I. INTRODUCTION

A corporate enterprise of Dutch institutes of higher education and universities has been working together for some time on setting up a number of remote labs and making these facilities available for one another [1],[3]. The objective is invariably to create an access system which allows a time-lock to be reserved in order to subsequently gain unique access within this time-lock to carry out lab experiments. This way the remote object computer is monitored from one's home computer. After that objects for experimentation can be accessed. For more details see ref.[2]. During the academic year 2006/2007 a new remote lab was set up which offers students the opportunity to gain experience with wireless access networks [WIFI, 802.11B/G]. The basic assumption being that engineering students have experience with home situations in which a simple "Bridged WAP [wireless access point] is used. It is essentially only a matter of conversion from a wireless link to a wired connection. The remote lab offers three intensive experiments :

1. Simulation of a wireless 802.11 environment.
2. Setting up and testing a basic professional environment defined by a limited number of WAPs, with considerable attention to security and the wireless link.
3. The set-up of an enlarged business environment with numerous centrally managed WAPs in concept and centralized user's access points.

II. SIMULATING A WIRELESS ACCESS NETWORK

The professional set-up for a wireless network begins with the use of a tool with which, starting from a list of

demands, predictions can be made concerning the attainable coverage with a specific set-up of access points. Students are offered the RF planner 4.0 package [Colubris networks], with which a simulation is carried out for the specific environment that will be actively used in the experiments following. The student is to feed into the computer the constructive properties of walls, floors and other relevant objects in the environments, that may influence the RF behavior of signals in the IMS band [2.4 GHz]. Figure 1 shows the expected field strength for a specific configuration with three WAPs.

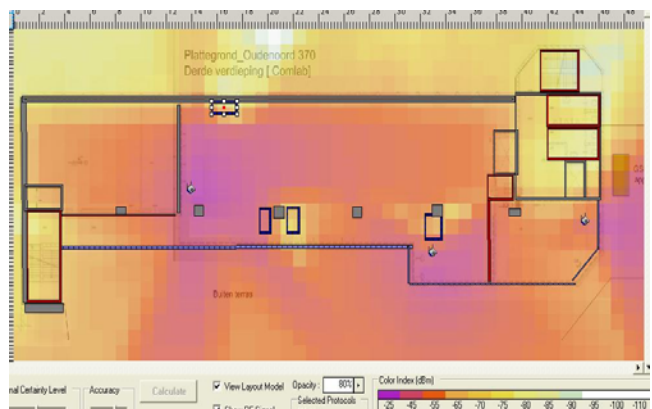


Figure 1. Simulator RF environment

When making the simulation one should also take into account that the RF signals of access points may possibly interfere with one another. In order to avoid this phenomenon an intelligent selection from available RF channels must be made.

III. AN SME ENVIRONMENT.

During this experiment the student will realize the configuration and testing of a wireless environment. Characteristics of the environment are: a limited number of own access points, rogue access points, external radiation into the business environment, the choice for optimal RF channels, access and security based on WPA-PSK. Figure 2 shows the set-up of the experiment. The object computer, controlled from a distance, is used to make a configuration of the access point via wired links. After completion contact is made with the same network by way of the WIFI-interface on the object computer for the benefit of the tests.

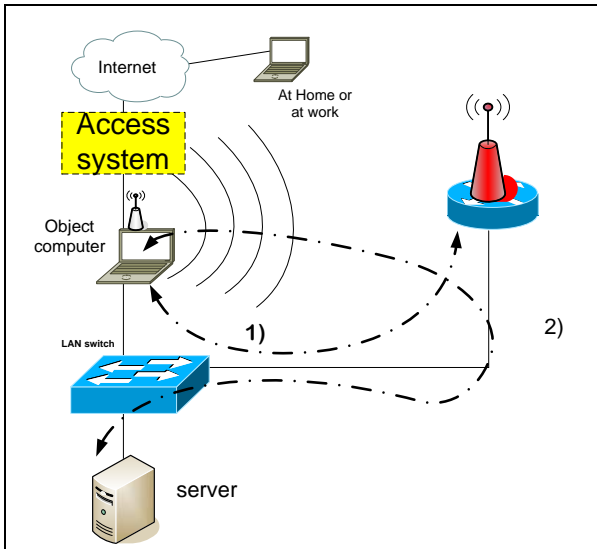


Figure 2. SME experiment

The student takes control of the object computer through which he/she is able to make a configuration of an access point (arrow 1). On the basis of information supplied by the access point on the use/usage by own and rogue access points he/she will have to select, among other things, the RF-channel used. [fig.3]

MAC address	SSID	Status	Channel	Signal	Noise	SNR	Info
00:13:f7:58:b3:b7	Wifi_d2xx	Ok	6	-60	-95	35	ESS WEP
00:03:52:f4:c5:b0	WIFI_CN1250	Ok	10	-56	-95	39	ESS WEP
00:03:52:f4:c5:b1	WIFI_cn1250_GUESTS	Ok	10	-92	-95	3	ESS WEP
00:0f:66:57:4b:8f	bats	Ok	11	-83	-95	12	ESS
00:03:52:db:c7:41	Flexlab_LOL	Ok	12	-50	-95	45	ESS WEP
00:03:52:db:c7:42	Student_LOL	Ok	12	-49	-95	46	ESS WEP
00:0f:b5:7c:0a:1a	NETGEAR1	quiet for 2 min	11	-84	-95	11	ESS WEP
00:1a:70:4e:b2:ea	thedude	Ok	11	-83	-95	12	ESS WEP
00:03:52:db:56:12	Student_LOL	Ok	1	-54	-95	41	ESS WEP

Figure 3. Signal strengths of available WAPs

Other items to be configured are: the SSID of the access point and the WPA-PSK key used. In this case the key known to the user has a double function: access provision and traffic encryption. In the configuration here aimed at the WAP has a number of functions namely: Router, NAT-translation and DHCP server for the wireless environment. After having taken the required configuration steps the connection of the object computer with the switch is brought “down”. Then the wireless link may be activated from the object computer (arrow 2). When a correct configuration of all system components has been made a connection with the server can be built up through the wireless link.

IV. THE CORPORATE BUSINESS ENVIRONMENT

With the large Corporate networks many access points are being used. The configuration to be realized outside the functions as defined in the SME environment will be more complex. There will also be large numbers of active

users. Therefore it is important to streamline the monitoring by way of a method of centralized control of both access points and user’s credentials. More likely than not users will not get access on the basis of a known “key”, but instead they will be authenticated by their own account-password combination. The authentication is made by a radius server. The basic concept [fig.4] as presented for configuration and testing, will now contain a CONTROLLER that centrally monitors the ACCESS POINTS .

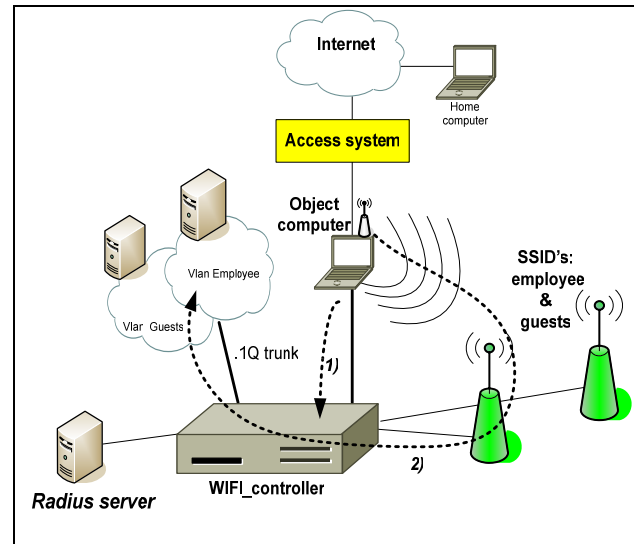


Figure 4. Corporate network set-up

Here a number of virtual access points will be simulated by the access points by way of transmitting several SSIDs, for example, SSID: EMPLOYEE and an SSID: Guest. This opens up the possibility to create different user groups with different network privileges. To this effect an SSID is linked to a so-called VSC (Virtual Service Community). A VSC is a logical group within a WLAN access point. To users every VSC will seem to correspond with a separate access point. The WiFi controller used will allow a maximum of 16 VSCs. A VSC can then be linked to a VLAN. By establishing a trunked connection between the WiFi-controller and a switch the various groups may be granted different rights to the network. In figure 4 this is indicated with VLAN Employee and VLAN guests. Both groups are in different VLANs and have different privileges within the network. In this corporate business environment NAT-translation and DHCP play a part as well.

The controller’s configuration is done from the object computer (arrow 1). After that the wireless link can be activated from the object computer (arrow 2). When a correct system configuration has been made a connection can be established by way of the wireless link. The nature of the connection depends on the user’s VSC.

V. CONCLUSIONS

The experiments fill the need for an environment in which experience with the configuration of a WiFi - network can be gained from a distance. That there is such a need is largely explained by the fact that many students combine their training with a job. As a result these students are only in the institute one day a week. For this

group the possibility to make use of the system from home is the perfect solution.

There is a growing need for qualified wireless network engineers. The experiments support the training of this group.

REFERENCES

- [1] Bedaux, van Gastel, Koreneef, Loonen, Uiterwijk: "Linking together reservation systems and remote labs, proceeding of the REV congress, June 2006, Maribor, Slovenia
- [2] Kees Uiterwijk, "Flexlab, affordable facilities for technical assignments in higher education, accessible at any time any place", 11th International Conference on Technology supported learning & training, On-line Educa Congress, November 29 – December 2, 2005, Berlin.
- [3] J.Bedaux, M.Wensink: Linking reservation systems for remote labs:Interface description and implementation experiences, REV Congress, Porto, Portugal, June 2007.
- [4] URL: <http://www.flexlab.nl/> Flexlab design
- [5] URL: <http://www.labsonline.nl/> Labs on line.

AUTHORS

C.J.M. Uiterwijk is a lecturer at the Hogeschool Utrecht, Faculty of Engineering, Institute for Electrical Engineering, Media technology and security Engineering, Oudenoord 370, 3513 EX Utrecht, (e-mail: kees.uiterwijk@hu.nl).

R.M. Kamphuis., is a lecturer at the Hogeschool Utrecht, Faculty of Engineering, Institute for Informatics, Oudenoord 370 3513 EX Utrecht, (e-mail: rein.kamphuis@hu.nl)

Manuscript received 01 August 2007. This work was supported by Colubris Networks



Published as submitted by the author(s).