User Service Management in Hot Spot Networks Using Policies

Idir Fodil and Vladimir Ksinant

Research and Development, 6WIND, Montigny-le-Bretonneux, France.
e-mail: {idir.fodil,vladimir.ksinant}@6wind.com

Abstract: **Advances in wireless LAN technologies based upon IEEE 802.11[1], and proliferation of portable and mobile computing led to large deployment of WLAN in corporate and in public places called Hot Spots. At the opposite of corporate places, users in public places come from different service providers, have different needs are not easy to identify. This implies user management, that offer AAA (authentication, authorization and accounting) mechanism, and Hot Spot provisioning and adaptation according to user's SLA (service level agreement). The first one is useful for user authentication, authorization and accounting and there is currently lot of solutions that are deployed and used. The second is related to providing users with their subscribed services and achieving service differentiation in the Hot Spot. This can only be achieved at the IP level by adapting Network equipment each time users arrive or leave the Hot Spot. Realizing such task in access points is not optimum, because more than one access point have to be configured and adapted. For these reasons, we propose to process user management in the access router. This management is done through the use of policy based management model (PBM) as introduced by the IETF. These policies are high level configuration tool, and are installed on the access router offering efficient user management.**

Keywords— Management, Policies,SLA, WLAN, Hot Spot, IEEE 802.11.

1. Introduction

Advances in wireless LAN technologies based upon IEEE 802.11[1], and proliferation of portable and mobile computing led to large deployment of WLAN in corporate and in public places (Hot Spot) ([3], [5], [6]). To get benefit of Hot Spot large deployment and to provide their mobile users with their contracted services, service providers (ISP, content provider, and cellular operator) maintain contractual relationship with Hot Spot operator [2]. For that, service providers must be able to manage their mobile users by:

- Providing their SLA ([9], [10], [11]) including QoS parameters.
- Rapidly solving problems when they occur.
- Achieving billing (charging) functions

Such tasks can be achieved through AAA mechanisms and WLAN provisioning and adaptation according to user's contracted SLA ([2], [4]).

A lot of solutions provide user management. Most of them do not support multiple service providers, and provide all users with same services. This is due to the fact that providing service differentiation can be achieved only at the IP level, implying access router reconfiguration for each new mobile user according to its SLA [9]. Achieving this with actual router configuration tools is very difficult and hard task because human intervention with accurate knowledge of configuration tools is needed. For these, we propose the use of policy based management approach ([11], [12], [13], [14]), which provide high level configuration mechanism, allowing dynamic router behaviour according to specified events and conditions.

In this paper, we will present solution for managing Hot Spot Networks based on the use of policies installed on WLAN access router. This solution supports multiple service providers, and allows them to provide their users with differentiated services according to their subscribed contracts (SLA). We have implemented our solution in 6WIND Router's [22], and experimented it in small platform. This solution will be used in the context of INFRADIO project [23], which aims to deploy large IPv6 WLAN in Paris6 University and ENST Paris, with advanced functionalities such as access control, filtering, authentication and quality of service.

The paper is organised as follows: In section2, we list and discuss the existing solutions for user management in Hot Spots. In section3, we detail our solution, and its implementation. In section4, we describe scenario of user access management. Finally, we conclude the paper in section 5.

2. State of the Art

In Hot spot Networks, users are mobile. They come from different ISPs, have different SLA, and execute different applications. For those reasons, one of the important management issues is related to user access management (arrival and departure of new users) in the WLAN, since a complex process is required. This process includes authentication, authorization, accounting and SLA provisioning. We detail a non exhaustive list of solutions that allow user management.

2.1. IEEE 802.1x

The first one and the most used is the IEEE 802.1x ([7], [8]) standard which defines a method for executing EAP protocol over Ethernet frames [17]. EAP has been defined as an extension to the PPP protocol, and can carry any authentication mechanism. EAP messages are exchanged between an EAP client (mobile user) and EAP server (remote authentication server), and are completely transparent to the access

point. The AP has only to maintain a trust relationship with the remote authentication server. Initially, only EAP messages can go through the AP, but when the user is successfully authenticated, the associated MAC addressed is authorized on the access point. Advantage of IEEE 802.1x is the use of EAP protocol which allows mutual authentication between Access points and users, and EAP-Key establishment between them.

The first drawback of the 802.1x standard is that users have to re-authenticate when they change access point, since EAP is used between users and access points. This can be avoided by doing context transfer between access points, but generating a big handoff delay.

Another drawback of 802.1x solution is that we can't differentiate users (different SLA) because the authentication is done on the access points based on the MAC layer. Moreover, access points can't dynamically select the authentication server based on user request but rather are configured to communicate with a fixed authentication server.

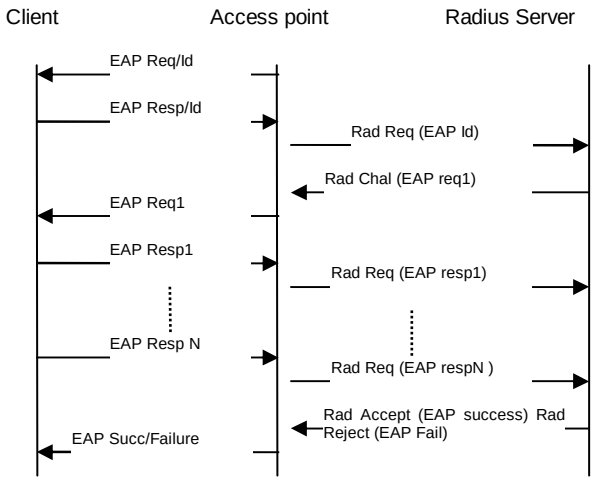

Fig. 1 IEEE 802.1x : EAP / Radius

2.2. PANA (Protocol for carrying Authentication for Access Networks)

Currently under design in the PANA working group of the IETF [19], its main purpose is to implement Network layer access authentication protocol by defining solutions that are layer2 agnostic and IPv4/IPv6 compliant. These solutions define a client-server messaging protocol that will allow authentication payload to be carried between the host/client (PaC) and an agent/server (PAA) in the access network for authentication and authorization purposes regardless of the AAA infrastructure that may (or may not) reside on the network. Since its goal is to provide Network layer secure access control by carrying authentication methods, PANA will reuse EAP protocol and its extensions.

PANA protocol brings the advantage of using EAP between users and authentication agent which can be access router or switch, avoiding user re-authentication problem of 802.1x.

Service differentiation between users and multiple provider support in Hot Spot Networks can not be achieved through PANA protocol, because of the lack of EP (enforcement point) provisioning specification in the PANA architecture and the use of EAP protocol. Some works are currently in progress in PANA working group for definition of EP provisioning (draft) methods using SNMP, COPS-PR, Diameter or Forces. More, PANA deployment may suffer from 802.1x deployment which is actually used in most of the AP (access points).

2.3. LWAPP (Lightweight access point protocol)

LWAPP is an IETF draft standard [20], which was primarily designed by company named Airespace (Wi-Fi Network Management Company). The main goal of LWAPP is to be a protocol that provides centralized management for access points in 802.11 Networks.

LWAPP idea is the following : since Access points has their own IP addresses and works as access servers, it would be more benefit if access points works as layer3 devices instead of working only as layer2 devices. Thus all access points can be controlled (managed) through a switch router or console, reducing filtering, policy processing, traffic management, authentication, and encryption needed in an access point. A generic encapsulation and transport mechanism is also provided by LWAPP to enable interoperability between LWAPP management console and LWAPP access points.

Currently LWAPP is available in an Airespace product called AireWave Director Software, but still not a real IETF standard because it has not reach consensus.

2.4. IPSec VPN Solution

The second solution completely based on IP is currently used by multiple WLAN service providers, which uses existing WLAN operator to provide wireless services to their subscribers (e.g. Boingo).

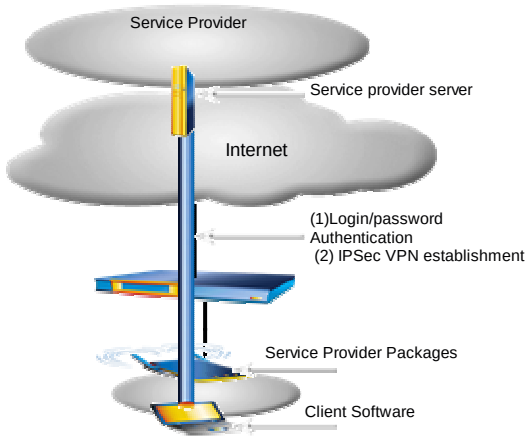

Fig.2 IPSec VPN Solution

For that, WLAN operator have to join service provider by installing "hot spot in a box" package, and mobile users have to install client software that helps them to locate service provider compatible access points. After successful authentication and authorization based on login/password, an IPSec tunnel [21] is created between client and specific server. This solution has the advantage of providing service provider with user control since all traffic go through its Network infrastructure. First drawback of this solution is that only service provider services are supported (not multiple service providers), due to the package installed on access points.

2.5. Web Based Approach

The last solution is a WEB browser based approach, where authentication process is carried out in the web browsers on client machines using secure https protocol between access points and users. Benefits of this solution are that no specific configurations are required on client machines, and web browsers with https support are universally available on nearly all client machines. Drawbacks of this solution are that it doesn't support multiple service providers, user re-authentication is required on each access point, and finally service differentiation can not be achieved.

2.6. Discussion

In all the above solutions, several service providers in the same WLAN are not supported, and mobile users have access to the same service levels. Since service providers sell different type of contracts to their users, differentiating them is a crucial aspect in WLAN. Allowing service differentiation can be done in IP level by user SLA provisioning and dynamical access router configuration. SLA provisioning can be done during the authentication and authorization process, but dynamic router configuration is more complex because nowadays routers are configured using CLI commands (command line interface) and monitored using SNMP.

These tools are not suitable in Hot Spot Networks where users change frequently, because users associated configurations need to be installed in access router when users arrives and removed when leaving. For that reasons, a new approach is needed to allow automated access router configuration according to provider configuration and to WLAN mobile users SLA. This approach is based upon policies which are set of events, conditions and actions. New events launch the evaluation of conditions that entail the execution of the actions.

3. Policy Based Solution

We investigate the use of policy based management approach in Hot Spot networks in order to offer service providers a solution that allow simple, flexible and scalable user management. Based on the use of policies installed on the access router by the service provider, and according to user SLA containing allowed services and QoS parameters, the access router configures itself dynamically to ensure the contracted service. In our solution, the entire authentication authorization and service level provisioning is achieved at the IP layer, by using web based approach associated to Radius authentication server [18]. For policies, each service provider can implement its own policies on the WLAN access router according to their contracts. Service provider policies are separated and we assume that no conflict can happened between them since the access router appears as dedicated router for each service provider.

We will first detail the policies implemented on the router. After, we will detail the designed router architecture for multiple service provider policies support and we will finish with detailing user access management scenario in Hot Spot Networks.

3.1. Policy Definition

RFC 3198 states that: « a policy can be defined from two perspectives : a definite goal, course or method of action to guide and determine present and future decisions … and a set of rules to administer, manage and control access to network resources » [15] . In other words, policies allow network management in terms of users, services and applications, not in device technically terms. A policy is a set of rules that command the network how to operate. Policies are based on the SLA jointly agreed between an ISP and a client. To translate the SLA into device-dependant configuration is done through policies.

Technically speaking, a policy is a set of conditions and actions. A policy may include one or more conditions, and one or more actions. If the conditions – some or all – are evaluated to true, then the totality or a part of the actions must be enforced. Conditions allow knowing when to do, whereas the actions express what to do. Note that the definition of an action does not specify how to do. The way to apply the action(s) is device dependant, and it is the mapping of the policy and the device technology. In our solution, we define policy as follows:

Policy = ***"On Event***
If conditions then apply {action1… action n}
Else apply {action1'… action n'}"

When event belonging to policy occurred, conditions are evaluated. If they are satisfied then the first list of actions is applied, else the second list of actions is applied if it exists. As event, one can quote the arrival of new user, new application launching ...etc. Conditions contain parameters related to the events such as user profile, application type and to router parameters such as time of the day, quality of service, number of users...etc.

Actions are related to services such as allowing certain type of traffic, VPN establishment, Diffserv QoS marking …etc

3.2. Router Architecture

When service provider subscribes contract with WLAN operator, a new module is instantiated on the router and called service provider block. After, the service provider installs its own policies on the access

router. These policies are received by a module named policy manager which forwards them to the associated service provider block. Policy module stores these policies in tree structure. Policy module checks if the rule can be directly applied. If it's not the case, the policy module notifies the event module that it is waiting for specified event.

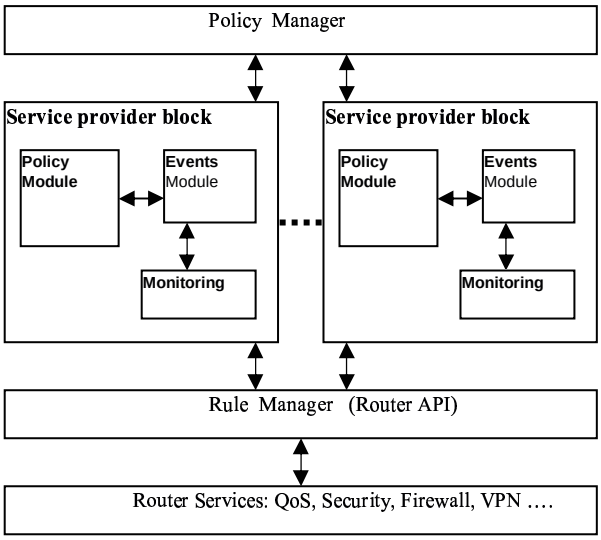

Fig.3 Policy Router Architecture

Events can be external (e.g. new user) or internal (e.g. QoS parameter) and when they occurred the events module notifies the policy module which will apply the associated policy.

To apply a policy, the policy module must send it to the Rule manager. This module will apply the policy by translating it to router rules using router API.

- Policy Manager: ensure policies reception and forwarding to the appropriate service provider block.
- Service provider block: ensure policy storage and enforcement on the router. It is composed of three parts:
  - Policy Module: ensure policies reception, storage and enforcement. It communicates with the events module to get notifications of new events.
  - Events Module: responsible of events management. It notify Policy module when new event occurred and communicate with monitoring module to supervise internal router parameters (security, QoS, filtering….)
  - Monitoring: responsible of monitoring internal router parameters (QoS, security...).
- Rule Manager: apply policies sent by the policy module. It translates them into router rules using router API.
- Router Services: gather all services provided by the router such as security, filtering, quality of service, mobility …

3.3. Policy Implementation

In this section we will detail the service provider block and more precisely the policy module which is responsible of policy reception, storage and application. Policies can be inserted using CLI (command line interface) directly or from remote machine, and WEB interface. Policies are stored in the access router in tree structure as shown in figure 4.

Policy entry object represents the root of the tree and contains Policy-St objects. Each Policy-St object represents a single policy and its structure is depicted in figure 5.

Policy Wait is an object containing the event that will launch the policy execution. This object communicates with the events modules in order to get notifications when event occurs.

Policy-Cond is the object containing the conditions (one or more) of the policy. When the event occurs, the events module sends notification to the Policy-Cond object, which will evaluate the condition in order to execute one of the two branches of the policy (Then or Else).

Action object contains the different actions that will take place when the events occurred. These actions are related to services such as web and video conference authorization, and will be translated to router rules by the rule manager. This architecture has been used for implementing policies in case of access control in Hot Spot networks

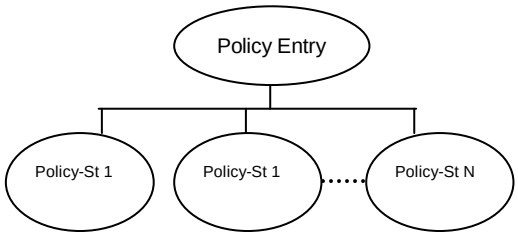

Fig. 4 Global policies structure

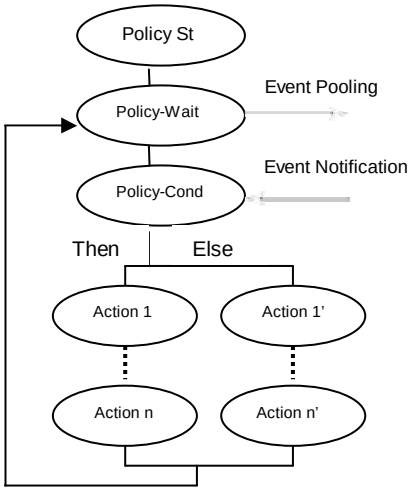

Fig.5 Policy Representation

4. Experimentation of Access Control Scenario

To illustrate the use of the policies in Hot Spot Networks for user access management, we describe a usage scenario. Since each service provider sees the access router as dedicated, we will focus in our scenario on one service provider that has contract with WLAN operator and wants to provide services to its clients.

4.1. Platform

The platform as shown in figure 6 is composed of:

- Service provider Radius Server: contains authorized customers and their contracts (SLA).
- 6WINDGate Router: programmed with policies to dynamically react when new users arrive on the Hot Spot or when new applications are involved such as VoIP, VoD ...etc. The router is basically closed and only flows authorized by the ISP can pass through after authentication. For this, the router embarks a Web Portal and a radius client that will be used for user authentication and SLA provisioning.
- Hot Spot network: composed of one access point, and 6WINDGate router.
- Mobile computers equipped with Wireless LAN cards.
- All the components of the platform are IPv4/IPv6 capable.

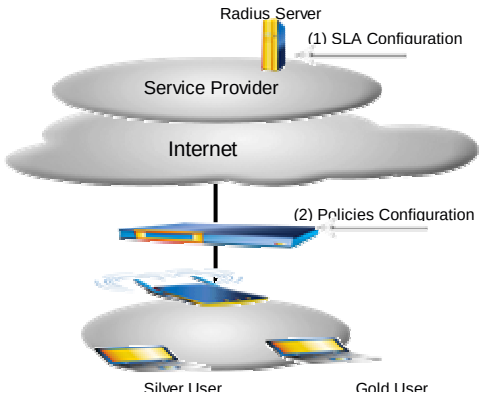

Fig.6 Platform Testbed

We define two customers that have subscribed at service provider1. The first one has a gold contract which allows him to access Web services and to make video conferences. The second one has a silver contract and can only access to Web Services. To provide better quality of service on the Hot Spot, ISP1 authorizes only 1 video conference session

4.2. Configuration

- Radius Server: configured with two customer profiles: silver and gold. For each customer, a login, password and user SLA is associated.
  - Gold customer: authorized to access Web service with 20Kbit/s and VoIP service with 30Kbit/s for infinite time.
  - Silver customer: authorized to access Web service with 10Kbit/s and for only one hour.
- Policy configuration: following policies have been installed on the access router.

On New user
If (User Gold and Max_Gold=0) then apply action 1,2
Else apply action 2
Action 1: authorize video conference service.
Action 2: Authorize Web service.

The policy installed on the access router allow gold user to access to Web and video conference service if there is no gold user before. Either, Gold user have only access to Web Service. Concerning silver user, they have only access to Web Service.

According to the user SLA, gold user is authorized to use WEB and video conference services with 20Kbit/s and 30kbits/s respectively with infinite connection time, while silver user is only authorized to use Web with 12kbit/s with one hour time connection.

4.3. How does it work?

Initially, only DNS requests go through the access router and all the other flows are forbidden. This is done by setting firewall rules in 6WINDGate router.

When user arrives at the Hot Spot, he/she obtains an IPv4/IPv6 address using stateless or statefull configuration mechanism. Statefull mechanism is achieved through DHCPv4 server, and DHCPv6 server located in the access router. IPv6 Stateless mechanism is realized thanks to router advertisement messages sent by access router.

When the user activate Internet browser, automatically the web page embarked in the router is displayed. The user must then insert its login, password and ISP name. Once this information validated, the router sends request to the radius server to authenticate the user. The Radius server responds with accepts or reject.

If the user is authorized then the Radius response contains its SLA including authorized traffic, associated bandwidth and authorized time. Once the router receives these SLA, policies are translated into router rules, allowing user to access its contracted services.

For authorized traffic and associated bandwidth, and according to user IP address, firewall and quality of service rules are created and installed on the access router.

Concerning time management, the router associates for each user time to live equal to the authorized time connection provided by the Radius server. When this time is reached, the user is disconnected by the access router. For detecting user disconnection, we use a novel mechanism based on traffic monitoring. A timeout threshold = 5 minutes is associated to each user, and if no traffic is passed through the access router during this time, the user is disconnected and associated router rules removed. After what, if the user wants to reconnect, a new authentication procedure must be done.

User connection duration is calculated based on the time of the last packet sent by the user, thus ensuring granularity of one second, because. Once user disconnects itself or is disconnected by the access router, an accounting message is sent to the Radius server containing time connection duration for billing purposes, and all the associated router rules are removed. The entire process of user management using policies is depicted in figure 7.

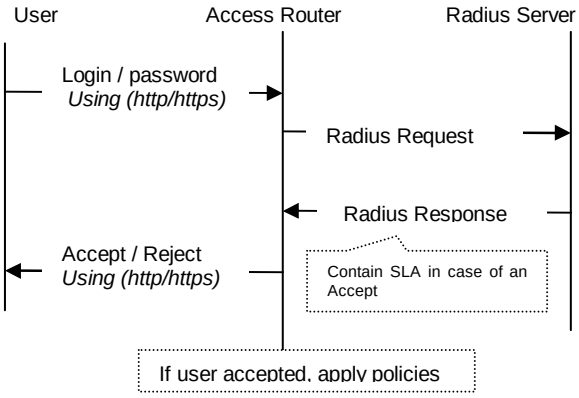

Fig.7 User access management

5. Conclusion and work in progress

In this paper, we have presented a solution that allow service providers to get benefits from the large deployment of wireless public LAN, by differentiating services offered to their customers. This solution is based on the use of policies in access routers, which offers high level configuration tool and provide dynamic router behaviour according to service provider criteria and users contracted services. Moreover, multiple service providers are achieved through modular router architecture. Because of the IP based, our solution can work over different air interfaces, across wireless LAN cards from different vendors, and does not require any modification to layer2 protocol. This solution has been successfully implemented and tested in 6windgate router, and we are currently working on the deployment of this solution at large scale in the INFRADIO project.

REFERENCES

[1] IEEE. 802.11b/d3.0 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, August 1999.

[2] Junbiao Zhang and al, “Virtual Operator based AAA in Wireless LAN Hot Spots with Ad-hoc Networking Support”, Mobile Computing and Communications Review, Volume 6, Number3.

[3] Terry Schmidt and Anthony Townsend, “Why WI-FI Wants to be free”, Communications of the ACM, Vol. 46, N° 5, May 2003.

[4] Joseph W. Graham II, *"Authenticating Public Access networking"*, SIGUCCS’02, November 20-23, 2002, Providence, Rhode Island, USA.

[5] Upkar Varshney and Ron Vetter, “Emerging Mobile and Wireless Networks”, Communications of the ACM, Vol. 43, N°. 6, June 2000.

[6] Rajeswari Malladi and Dharma P. Agrawal, ”Current and Future Applications of Mobile and Wireless Networks”, Communications of the ACM, Vol. 45, N°. 10, October 2002.

[7] IEEE Daft P802.1X/D11: Standard for Port based Network Access Control, LAN MAN Standards Committee of the IEEE Computer Society, March 27, 2001.

[8] Pekka Nikander, “Authorization and charging in public WLANs using FreeBSD and 802.1x”, USENIX annual technical conference, June 10-15 2002.

[9] Jim Martin, and Arne Nilson, “On Service Level Agreements for IP Networks”, IEEE Infocom Conference, June 2002.

[10] S. Salsano et al., “Definition and usage of SLS in the AQUILA Consortium”, Internet Draft, November 2000.

[11] Bob Moore, Ed Ellesson, John Strassner, and Andrea Westerinen, “RFC 3060: Policy Core Information Model – version 1 Specification”. IETF, February 2001.

[12] J Jason, L Rafalow, and E Vyncke, “IPsec Configuration Policy Model”, Internet draft, November 2001.

[13] Y Snir, Y Ramberg, J Strassner, R Cohen, and B Moore, “Policy QoS Information Model”, Internet draft, November 2001. [1]

[14] Raj Yvatkar, Dimitrios Pendarakis, and Rocj Guerin, “ RFC 2753: A Framework for Policy-Based Admission Control”. IETF, Informational, January 2000.

[15] A.Westrinen and al, “RFC 3198: Terminology for Policy Based Management ”, IETF, November 2001.

[16] David Kosiur,”Understanding Policy-Based Networking”. Wiley Computer Publishing, 2001.

[17] L. Blunk and J. Vollbrecht, “RFC 2284: PPP Extensible Authentication Protocol (EAP)”. IETF,March 1998.

[18] C. Rigney, S. Willens, A.Rubens, and W. Simpson, “RFC 2865: Remote Authentication Dial in User Service (Radius)”, IETF, June 2000.

[19] Alper E. Yegin, Yoshihiro Ohba, Reinaldo Penno, George Tsirtsis ,and Cliff Wang, “ Protocol for Carrying Authentication for Network Access (PANA) Requirements”, Internet Draft , June 2003.

[20] P. Kalhoun and al., “Light Weight Access Point Protocol”, Internet Draft, June 2003.

[21] S.Kent, and R. Atkinson, “ RFC 2401: Security Architecture for the Internet Protocol”,IETF, November 1998.

[22] www.6wind.com

[23] INFRADIO Project : http://rp.lip6.fr/infradio/