SECURITY AND DIFFERENTIATED HOTSPOT SERVICES THROUGH POLICY-BASED MANAGEMENT ARCHITECTURE

Idir FODIL and Vincent JARDIN
6WIND, Research and Development,
{Idir.fodil, Vincent.Jardin}@6wind.com

Abstract: We have studied the case of deploying services in public wireless networks based on IEEE802.11 standard. Due to low cost, easy deployment, cost effectiveness and high performance, this technology appears as a very attractive solution for providing internet access and services in public places called hotspot like airports, hotels, train stations... etc Actually, there are numerous solutions that allow user management in WLAN networks. However, most of them do not support multiple service providers and provide all users with the same level of services to Internet access. In our paper, we propose a new software management architecture for hotspot networks, which is based on policy-based management principles introduced as a result of collaboration with the IETF. Our solution enables multiple service provider support and it allows user and service differentiation in hotspot networks. It provides efficient, flexible and scalable user management solution by implementing coherent combination of AAA functions, quality of service guarantee and security assurance for hotspot operators and service providers. For policy configuration, XML schemes have been defined, offering open, easy and customizable management architecture. Moreover, since our solution is layer 2 agnostic, it can be extended to different access technologies such as DSL, PLC... This management architecture has been implemented, tested and validated on the 6WINDGate™ routers and it can easily be ported onto other software architectures and open standard platforms.

Key words: Hotspot, security, AAA, WLAN, 802.11, Policy Management, services, SLA, multiple service providers

Y. Deswarte et al. (eds.), *Security and Protection in Information Processing Systems*

1. INTRODUCTION

Today, service management remains a strong concern for both service providers and customers. Service providers are not only under pressure to sell services that are guaranteed and differentiated but also to provide "always-on" connectivity for their customers. At the same time, customers are demanding for more discerning services such as security, mobility, and quality of service (QoS). Achieving these services separately is easy as a lot of standards exist and implementations are widely available. However, combining these services at the same time remains a challenging task since there are a lot of dependencies between them, leading to instable and non performing networks. For those reasons, a higher layer of service management is strongly needed to provide both users and service providers with guaranteed consistency and efficient service deployment. To this end, we have studied the case of deploying services in public wireless networks based on IEEE802.11 standard. Due to low cost, easy deployment, cost effectiveness and high performance, this technology appears as a very attractive solution in order to provide internet access and services in public places called hotspot like airports, hotels, train stations... etc

The Wi-Fi hotspot usage is actually quite inconvenient since users have to buy a new account with each hotspot provider, and has no security assurance from the hotspot provider. It means that the actual hotspot cannot support efficiently roaming. Such inconvenience would reduce the user's interest in using the hotspot services. One solution to this problem is to push the user's existing service provider's contracts into the hotspot. This service provider can be any type of entity that offers the users certain types of services and maintains the user's accounts. These service providers may include Internet service providers, content providers, or cellular operators.

This convenience and security assurance from the existing service providers give greater interest and confidence in using the hotspot services. In such environments, where hotspot operators can have contracts with several service providers (SP), user access management appears as the most important issue to resolve. Hotspot operators must guarantee the SP a subscribed contract that includes dynamic or static bandwidth reservation and security insurance. Moreover, they must be able to provide different levels of services for both service providers and their own users. Concerning service providers, they must be able to manage their mobile customers by providing them with their subscribed contract, and by achieving service differentiation between users in the hotspot network.

This management requires a solution that allows supporting multiple service providers, securing authentication and authorization of users according to their service provider, provisioning hotspot network according

to the user service level agreement (SLA), and that allows different billing models. User management implies hotspot access equipment (router, switch...) adaptation for each new user according to his SLA. Concerning multiple service provider support, a new architecture must be built on top of the access equipment in order to provide virtual dedicated equipment for the hotspot operator and for each service provider. Actually, there are numerous solutions that allow this user management in WLAN networks. However, most of them do not support multiple service providers and provide all users with the same level of services to Internet access. This is due to the fact that these solutions are layer 2 based, and providing a scalable service level differentiation can only be achieved at IP level, which is the layer 3. For these reasons, a new management approach that allows access equipment virtualization, dynamic adaptation and reconfiguration is strongly needed.

In our paper, we propose a new software management architecture for hotspot networks, which is based on policy-based management principles introduced as a result of collaboration with the IETF. Our solution enables multiple service provider support and it allows user and service differentiation in hotspot networks. It provides efficient, flexible and scalable user management solution by implementing coherent combination of AAA functions, quality of service guarantee and security assurance for hotspot operators and service providers. For policy configuration, some XML schemes have been defined, offering open, easy and customizable management architecture. Moreover, since our solution is layer 2 agnostic, it can be extended to different access technologies such as DSL, PLC... This management architecture has been implemented, tested and validated on the 6WINDGate™ routers and it can easily be ported onto other software architectures and open standard platforms.

The paper is organized as follows: in section 2, we describe hotspot networks, services and their requirements; in section 3, we list and discuss the existing solutions; in section 4, we describe our policy based solution and its implementation on 6WINDGate routers; in section 5, we describe a use-case scenario of access management in hotspot network with multiple service providers; finally, we conclude this paper in section 6 and some future works are presented.

2. HOTSPOTS OVERVIEW

Initially, WLAN was seen as a potential threat to existing network services for both wireless operators and Internet service providers[24]. But, with the growing deployment of hotspot networks, both have taken more positive view and created new business opportunities by including hotspot

networks as complement to their existing offerings. To cater to this demand and to capitalize on their customer relationship, a number of fixed network operators are investing in public hotspots to which they give access to their own DSL subscribers. Now mobile operators are moving to incorporate Wi-Fi access into their service offers.

To provide attractive hotspot services with user security assurance, convenience and always the same level of services, it is mandatory that the customers use the same login ID in all these places. To achieve this goal, a customer relationship must be established between hotspot operators and service providers, and between service providers themselves. This includes marketing, customer service, billing and collection, providing secure access, and account management.

Stronger encryption of the wireless traffic is required to prevent eavesdropping and to secure authentication, especially when business users are accessing company networks from a hotspot. Moreover, business users in particular will require more guarantees about their quality of service to justify higher prices. Last but not least, more varied billing strategies must been supported like free access, prepaid access for a certain amount of time or volume, pay per use period and differential fees for higher bandwidth. Finally, roaming and multiple service providers must be supported in all hotspot networks, which always achieve the best services and the required connections.

To get benefit from this new business model, networks services and architectures, the following requirements must been satisfied:

- Multiple service provider support.
- Secured Authentication, Authorization and Accounting (billing models).
- Quality of service assurance
  - Static: some service providers may pay for fixed bandwidth in some hotspot networks, because they are deployed in places that attract lot of people. In these cases, the quality of service is guaranteed per service and it is the service provider responsibility to ensure per user quality of service guarantees.
  - Dynamic: in other places, which are less frequented, service providers may pay for bandwidth only when their customers use the hotspot. In this case, the hotspot operator must be able to ensure the quality of service for the user.
- Dynamic User management according to profiles, authorized times, and network resources.
  - Achieving user's SLA.
  - Service differentiation between users.
  - Rapidly solving problems when they occur.

In the next section, we will detail the existing solutions for hotspot networks, and we will discuss their advantages and drawbacks concerning the above requirements.

3. EXISTING SOLUTIONS

In the hotspot networks, users are mobile. They come from different ISPs, have different SLA, and execute different applications. For those reasons, one of the important management issue 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 allows user management.

3.1 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 (AP). 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. The advantage of IEEE 802.1x is the use of EAP protocol which allows mutual authentication between access points and users, as 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 users (different SLA) cannot be differentiated 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.

3.2 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 layer 2 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 that can be access router or switch, avoiding user re-authentication problem of 802.1x. Service differentiation between users and multiple provider support in hotspot networks cannot be achieved through PANA protocol, because of the lack of EP (enforcement point) provisioning specification in the PANA architecture and the use of the 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. Moreover, PANA deployment may suffer from 802.1x deployment that is actually used in most of the APs (access points).

3.3 LWAPP (LightWeight Access Point Protocol)

LWAPP is an IETF draft standard [20], which was primarily designed by a 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 an access point has its own IP address and works as an access server, it would be more benefitable if the access point worked as a layer 3 device instead of working only as layer 2 device. Thus all the access points can be controlled (managed) through a level 3 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 the LWAPP access points.

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

3.4 IPSec VPN Solution

The second solution completely based on IP is currently used by multiple hotspot service providers, which use existing hotspot operator to provide wireless services to their subscribers (e.g. Boingo). With intend to provide this scalable level 3 service, the hotspot operators have to join some service providers by installing "hotspot 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 a specific IPSec server.

The advantage of this layer 3 solution for the service provider it that it controls the traffic of its customers since all its traffic goes through its network infrastructure. However the main drawback of this solution is that only the services of a single service provider are supported (not multiple service providers), due to the routes through the IPSec tunnel and due to the packages installed on access points.

3.5 Discussion

In all the above solutions, several service providers in the same hotspot are not supported, there is no guarantee of the quality of service and the mobile users have access to the same level of services. Since service providers sell different types of contracts to their users, differentiating them is a crucial aspect in the hotspots. Service differentiation can be done in IP level (layer 3) by provisioning the SLAs of the users and by configuring dynamically the access routers. SLA provisioning can be done during the authentication and authorization process. But dynamic router configuration is more complex because nowadays routers are provisioned using their CLI (Command Line Interface) and they are monitored using SNMP. These tools are not suitable for the hotspot networks where the users roam frequently, because the associated configurations of the users need to be installed into its access router when a user arrives and they need to be removed when he leaves. For that reason, a new approach is needed to allow automated configuration of the access routers according to the service provider needs, the hotspot configuration and the SLA of the roaming users. This approach is based on policies that are some sets of events, some conditions and their related actions. The new events launch the evaluation of some conditions that entail the execution of the actions.

4. POLICY BASED SOLUTION

The requirements, which are related to user and network management in hotspot with multiple service provider environments, can be easily achieved separately. But providing a solution, which meets all the requirements, remains very difficult, since it involves some new network management architectures. For these reasons, we investigate the use of policy based management approach in hotspot networks in order to offer the hotspot operators and service providers a solution that allows 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 a Radius authentication server [18]. About policies, hotspot operators and service providers can implement their own policies on the hotspot access router according to their contracts. Policies are separated and we assume that no conflict can happen between them since the access router appears as a dedicated router for each service provider. We will first detail the policies implemented on the router. Then we will detail the design of the architecture of the router for multiple policies of many service providers and we will finish with a description of the management of the user accesses into the hotspot networks.

One important point to note is that hotspot operators implement their own policies for managing their user services. Therefore hotspot operators can be seen as a service provider.

4.1 Policy Specification

All policies defined in our solution are described and validated using XML schemas and installed using the two following: CLI (Command Line Interface), Web interface directly or from a remote administration machine.

Policies from our solution are grouped in 2 families: operator policies and customer policies. All policies are defined using an XML scheme.

4.1.1 Operator policies

They constitute the set of hotspot operator and service provider requirements. These policies are handled only by the hotspot operator. There are 2 types of operator policies.

- **Contract policies:** point to the subscribed contract between service providers and hotspot operator. These policies contain parameters related

to service provider name, associated bandwidth on the Hotspot, and AAA information.

- **bandwidth policies :** There are two types of bandwidth policies, depending on the contract between service provider and hotspot operator.
  - **Static bandwidth policies :** These policies enable service providers and hotspot operator to specify services and their associated bandwidth. The hotspot operator and the service providers are able to manage their own bandwidth by dividing it between their services and by allowing borrowing between them.
  - **Dynamic bandwidth policies:** a service provider can subscribe a contract with a hotspot operator specifying dynamic bandwidth reservation. This reservation is done according to parameters pushed by the SP when a new user connects to the hotspot. These parameters are carried by the authentication protocol.

4.1.2 Client Policies

They define a set of rules chosen by the service provider administrator

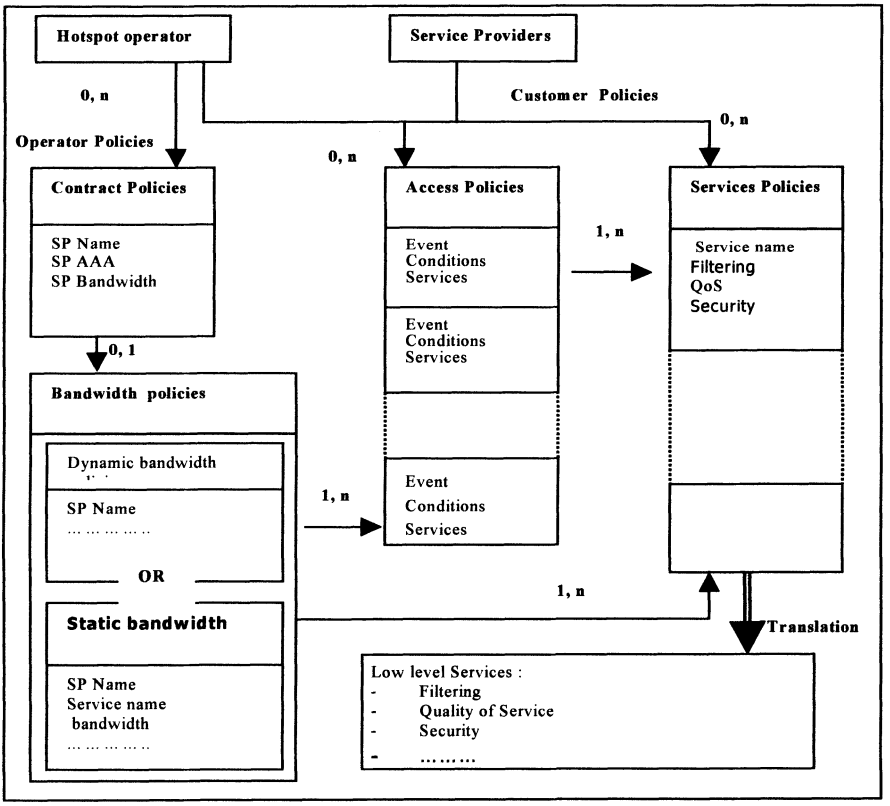

Fig1. Hotspot Policy Specification

and the hotspot administrator in order to manage the client's accesses to the network and to provide them with their subscribed SLA. Two subtypes of policies exist:

- **Access-policies:** materialize the added value that a SP and hotspot operator may offer to their customers. These policies allow dynamic service deployment by providing an admission control mechanism according to the profiles of the users, the number of users on the network, the time, the date and many other parameters. For example, an access control based on the number of users into the network, can be installed in the access equipment using these policies.
- **Service policies:** provide low level service specifications that need to be installed on the access equipment (in our case : the router). This specification gathers quality of service, filtering, security and other parameters.

4.2 Policy Implementation

When a service provider subscribes a contract with a hotspot operator, a new module is instantiated into the router.

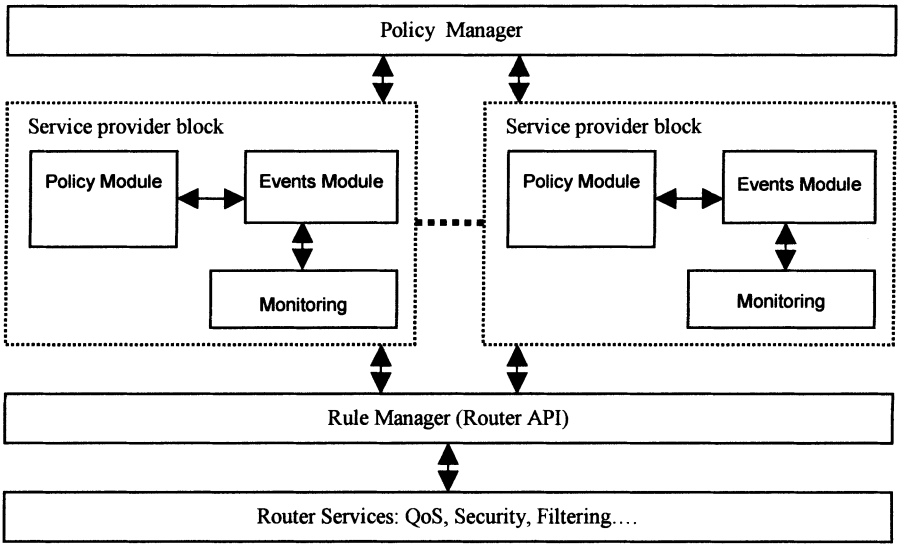

Fig2. Hotspot Policy Architecture

This module is called service provider block. After, the service provider installs its 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.

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 …

This architecture has been used for implementing policies in case of access control in Hot Spot networks

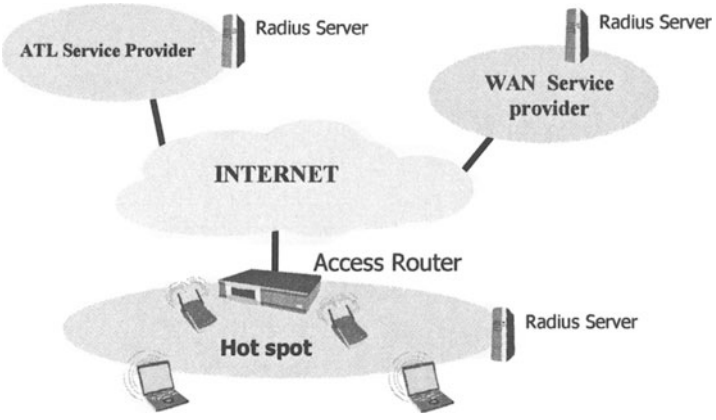

Fig3. Hotspot user management platform

5. ACCESS CONTROL SCENARIO

To illustrate the use of our policy-based solution for user access management in hotspot networks with multiple service providers, we describe a usage scenario. This scenario may be summarized as follows: A hotspot operator called "HSP" have an Internet access of 2Mbps. HSP wants to provide internet access to its own customers and reserve for these 500Kps. Two service providers subscribe contracts with HSP. The first one "ATL" buys a static bandwidth of 500Kbps. The second one "WAN" buys a dynamic bandwidth.

5.1 Access router Configuration with Policies

The policies are installed in the 6WINDGate Access router in order to dynamically react when new users arrive on the Hotspot. The router is basically closed and only flows authorized by the service providers or by the hotspot operator can pass through after authentication. The following policies are installed into the router.

- **Operator Policies:** HSP configure the access router with the following policies
  - Contract policies

```
<sp-information> <sp-name name ="HSP"/>
<sp-aaa server="10.16.0.142" secret="testing123" port="1812"/>
<sp-bandwidth rate="500kbps"/> </sp-information>
<sp-information><sp-name name ="ATL"/>
<sp-aaa server="192.17.52.36" secret="testing123" port="1812"/>
<sp-bandwidth rate="500kbps"/> </sp-information>
<sp-information><sp-name name ="WAN"/>
<sp-aaa server="192.36.96.52" secret="testing123" port="1812"/>
</sp-information>
```

  - Bandwidth Policies
    - Static bandwidth

```
<sp-bandwidth><sp-name name ="ATL"/> <service name ="web" bandwidth= "380kbps"/>
<service name ="ftp" bandwidth= "120kbps"/> </sp-bandwidth>
```

    - Dynamic bandwidth

```
<sp-bandwidth><sp-name name="WAN"/>
<sp-reservation = "dynamic"/> <sp-bandwidth/>
```

- Customer Policies
- Hotspot operator: HSP want to provide only Internet access for a maximum number of 15 users. All users have the same profile which is "guest". The following access and services policies are installed in the access router:

```
<access-policy> <sp-name name ="HSP"/>
 <policy-ident number ="1"/>
 <event type ="new-user"/>
 <conditions>
  <and>
   <type-condition          profile = "guest"/>
   <usernumber profile ="guest" maximum="15"/>
  </and>
  <then>
  <service name = "web">
  </then>
</access-policy>
```

```
<service>
 <service-name name ="web"/>
  <actions>
   <action-ident      number ="1"/>
   <action-type       type ="filtering"/>
   <action-todo       do = "allow"/>
   <action-ipversion  ver ="4"/>
   <action-protocol   pro ="6"/>
   <ipsource          ipsrc ="host"/>
   <portsource        portsrc ="any"/>
   <ipdesttination    ipdest="any"/>
   <portdestination portdest ="80"/>
 </actions>
</service>
```

- ATL: ATL have two types of users: gold, and silver. Gold users can access to web, and FTP. Silver users can access only to web services. Moreover, only 5 gold users have access simultaneously to the WEB and FTP services.

```
<access-policy>
  <sp-name name ="ATL"/>
  <policy-ident number ="1"/>
  <event type ="new-user"/>
  <conditions>
  <and>
    <type-condition profile = "gold"/>
    <usernumber profile="gold" maximum="5"/>
  </and>
  <then> <service name = "web">
    <service name = "ftp"> </then>
  <else>
    <service name = "web">
  </else>
</access-policy>
```

```
<service>
  <service-name name ="web"/>
  <actions>
    <action-ident number ="1"/>
    <action-type       type ="filtering"/>
    <action-todo       do = "allow"/>
    <action-ipversion  ver ="4"/>
    <action-protocol   pro ="6"/>
    <ipsource          ipsrc ="host"/>
    <portsource        portsrc ="any"/>
    <ipdesttination    ipdest="any"/>
    <portdestination portdest ="80"/>

    <action-ident      number ="2"/>
    <action-type   type ="filtering"/>
    <action-todo   do = "allow"/>
    <action-ipversion  ver ="4"/>
    <action-protocol   pro ="6"/>
    <ipsource          ipsrc ="host"/>
    <portsource        portsrc ="any"/>
    <ipdesttination    ipdest="any"/>
    <portdestination portdest ="21"/>
  </actions>
</service>
```

- WAN: WAN also have two types of users: gold, and silver. Gold users can access to WEB, and FTP. Silver users can access only to web services.

5.2 Radius Server Configuration

In the radius server configurations of the hotspot operator and the two service providers, we have added attributes in the parameters related to users. In the three radius servers, we have added the two following attributes for each user:

- POL_PROFILE: specify the user profile (guest: for HSP, gold or silver for ATL, and gold or silver for WAN).
- POL_TIME: for each user we have added an authorized time connection (Guest users are authorized for 20 minutes, ATL: gold users for infinite time and silver users for 3 hours, WAN: gold users for infinite time and Silver users for 1 hours).

Since WAN has a dynamic bandwidth subscription, we have added bandwidth attributes for each user in the radius server of WAN

- POL_SERVICE: WEB or FTP
- POL_BANDWIDTH: 20Kbps for Web and 15kbps for FTP.

5.3 How does it work?

- **Bandwidth reservation:** in the access router, the service provider ATL has a class of service of 500kbps which is divided into two classes: web class with 380kbps and ftp class with 120 kbps. HSP a class of service of 500kbps which is reserved for internet access for HSP customers. The 1MBps remaining bandwidth is used by HSP for its own services, its contract with WAN and for possible new contracts with other service providers.
- **Filtering:** Initially, only DNS request can go through the access router and all other flows are forbidden. This is done by setting firewall rules in the 6WINDGate router.
- **Authentication and authorization of users:** Authentication is done using the https protocol combined with radius protocol. This is achieved thanks to web portal and radius client embedded in the access router. The benefits of this solution are that no specific configuration is required on the machines of the users. Moreover the web browsers, which support the HTTPS protocol, are universally available. In this web portal, HSP, WAN and ATL appears offering the user possibility to choice its service provider.
  - When new user arrives at the hotspot, 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 activates Internet browser, automatically the web portal embarked in the router is displayed. The user must then insert its login, password and choice its service provider. Once this information is validated, the router sends a request to the radius server to authenticate him. The radius server responds with accept or reject.

- **Service deployment:** according to service provider, and radius response containing the user's SLA, the policies installed in the router are dynamically translated into router rules allowing users to access its contracted services. These rules are based on the policies and the IP address of the user
- **Time management:** Users are automatically disconnected from the network when their authorized time duration expired. Associated filtering and quality of service rules are dynamically deleted.
- **Data volume management:** If users are allowed to certain amount of traffic volume, we install with the filtering rules traffic conditioners. These conditioners are automatically removed when the data volume is reached and dynamically filtering rules are also removed.
- **Accounting:** Once the user is disconnected by itself or by the access router, an accounting message is sent to the radius server containing time connection duration and also data volume.

6. CONCLUSION AND FUTURE WORKS

In this paper, a new network management architecture for hotspot network has been overviewed. The lack of solutions that allow multiple service provider support, service guarantee per user and per SP, and service differentiation led us to propose this architecture. Our solution allows service providers and hotspot operators to get benefit from the large deployment of public Wireless LAN. This solution is based on the use of policies in access router, which provide high level configuration tool and dynamic router behavior according to service providers criteria and users contracted services. Secured Authentication and authorization, dynamic service deployment, quality of service guarantee and different billing schemas are managed in one way offering thus simple, flexible and scalable tool for both hotspot operators and service providers. Because of the IP based, our solution can work over different air interfaces, across wireless LAN cards from different vendors and it does not require any modification to layer2. Moreover, it can be extended to different access technologies such as PLC, DSL...

We are currently working on the deployment of this solution in the context of INFRADIO project [22]. It is a RNRT project that aims to deploy a large IPv6 WLAN into the Paris6 University and the ENST Paris. Another work we will investigate is related to the study of combining IPSec security protocol with our solution in order to provide hotspot Security.

7. 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.

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

[23]Charny, B. (2002c). Want Wi-Fi? Verizon takes it home. *CNET News.com*, October 9.

[24]A.Mahler and C.Steinfield The Evolving Hot Spot Market for Broadband Access "ITU Telecom World 2003 Forum panel on Technologies for Broadband, Geneva, October 2003"