TOWARDS HOTSPOT NETWORKS MANAGEMENT USING POLICY BASED MANAGEMENT APPROACH

Idir FODIL[1,2], Vincent JARDIN[1], and Guy Pujolle[2]
[1] 6WIND, Research and Development, {Idir.fodil, Vincent.Jardin}@6wind.com; [2] LIP6, University of Paris6, { Idir.fodil, Guy.Pujolle}@lip6.fr

Abstract: This paper describes a new management architecture designed for WISPs to facilitate the implementation and management of the services they offer at the access side of the WLAN, and to manage roaming contracts between WISPs. Our architecture is based upon the policy based management principles as introduced by the IETF, combined with more intelligence at the network edge. Our policy architecture adopts an architecture that is composed of two elements: a WISP management center (MC) that deploy policies and monitors all the WLANs, and programmable access router (CPE) located in each WLAN.

Key words: WLAN, Hotspot, IEEE802.11, WISPs, Policies, PBM, Management, Services, SLA, Roaming

1. INTRODUCTION

The recent years have seen expanding advances in new access network technologies which aimed to provide users with high speed access to the internet, and ability to use their network services everywhere and every time. Among these, the IEEE802.11 [1] standard has confirmed that it is the most simple and effective technology for providing network access in public places for users equipped with wireless cards. In order to provide their users with their subscribed service levels, and to benefit from public WLANs deployment, WISPs must be able to efficiently manage their public wireless networks at the wireless side and Internet access side. The wireless management which consists in guaranteeing micro mobility, security and

quality of service in the wireless side is actually supported by significant projects in research, industry and standardization community. For the access network management, its main functionalities is to provide means for services specification and deployment, service differentiation, user access management, security guarantee and roaming management [5,6].

Numerous solutions have been proposed [12, 13, 14, 15, 16], but most of them don't address the whole access management paradigm. Some, provide AAA functionalities (authentication, authorization, accounting), others provide security, and others mobility management. Moreover, dynamic WLAN adaptation according to users SLA, service differentiation, heterogeneous network support, and roaming management are not achieved.

The first reason is that service differentiation and heterogeneous network support can not be achieved using layer 2 based solutions, because they are link layer specific and cannot provide means for identifying services. Secondly, management is distributed among access points of the WLAN, which is not optimum network management solution because more than one AP has to be configured and adapted. Thirdly, dynamic network adaptation according to users and services is very difficult and challenging task with currently available network management tools. And finally, roaming management is very complex in such environment, because multiple service provider support on hotspot network still hard task.

Unfortunately, current network management cannot provide suitable tools for achieving the above needs. This is essentially due to the fact that network management is not much automated, and need skilled staffs with accurate knowledge of the various management tools. Moreover, existing tools are closed, service specific and cannot allow new service deployment. These generates extremely complex and very difficult network management, which weighs down and slows down introduction of new services, as well as significantly increase service providers operating costs.

We investigate the use of IETF policy based management [8, 9] approach in wireless LAN networks combined with central management held by access router instead of access points. We have enhanced the IETF architecture, because it is incomplete even though it is worthy foundation, since servic e providers and users needs have not been translated into suitable policies [11], and intelligence is not distributed among network equipments. Furthermore, we focused on designing an IP level solution, because it's the only way to differentiate services and to provide independent access network support. As result, we designed a policy architecture which provides WISPs with ability to offer innovative and differentiated services to their customers, to manage them in simple easier and more cost effective way, and to have roaming contracts with other WISPs. The rest of the paper is organized as follows. Hotspot management requirements are provided in section 2. The

policy management architecture, policy specification, and implementation are detailed in section 3. And finally, conclusion, actual and future works are overviewed.

2. POLICY MANAGEMENT SOLUTION

The main objective of our policy architecture is to provide WISPs with suitable tools enabling them to efficiently manage their networks and users, and to establish and manage roaming contracts with other WISPs. Based on the use of policies installed on the access router by WISP and according to users SLA containing allowed services and QoS parameters, the access router configure itself dynamically to ensure the contracted service. For Roaming Management, according to the roaming contract (per user, or per bandwidth), WISPs can install their own policies on the router and manage their users. Policies of different WISP are separated and we assume that no conflict can happen between them since the access router appears as a dedicated router for each WISP.

2.1 Architecture

The architecture has two main components, the management Center who takes on the WISP sold SLA guarantee and the access router (CPE) linking the public WLAN to the Internet.

The Management Center: The management center is the component of the architecture related to the WISP. The Management Center is responsible for the SLA negotiation, the generation of relevant policies and the application of these policies on the access router (CPE). The management center is a set of five modules: Service Portal (SPo), customer Agreement Database (CAD), Policy Server (PS), Policy Database (PDB) and Management tool (MNT).

The Access Router (CPE): Rather than configuring and managing each access point by itself, we choose to configure access router. Like that, user's re- authentication in the same WLAN is avoided, and handoff delays are reduced. Moreover, access points provisioning and management can be done by the router allowing global view of the network and more efficient resource management. In our architecture, the CPE is the equivalent of the PEP+PDP (Policy enforcement and policy decision points) [8, 9] in the IETF architecture. The CPE is more "intelligent" than a simple PEP since it has the capability of monitoring events, keeping network states, and providing users the ability to modify their services on the fly. The CPE ensure plays the following roles:

- Enforcement of the policies sent by the PS,
- Translation of these policies in proprietary configurations,
- Auto-adaptation according to the network state,
- Reconfiguration or new PS policies solicitations,
- Response to monitoring requests sent by the PS,
- Periodic delivery of monitoring information up to the PS,
- Storage of policies sent by the PS.

2.2 Policy Specification

In order to provide policies those allow appropriate translation of WISPs and users requirements onto access router configurations, we have specified the entire service provisioning and adaptation process. Thanks to this model, we have identified two policy families: WISP Policies and Roaming Policies.

Roaming Policies: point to the subscribed roaming contracts between the WISPs. These policies contain parameters related to foreign WISP, associated roaming model, and AAA parameters. If a foreign WISP has per bandwidth roaming contract, it will insert its own policies for users and services management as described after. But, if the contract is per user, service deployment will be done only when new user connect to the hotspot and according to parameters pushed by the foreign WISP. In other words, when a roaming contract is established on per user model, users coming from foreign WISPs are treated as users of the local WISP.

WISP-Service Policies: These policies define the set of policies chosen by the WISP administrator in order to manage their own services and their users. For foreign WISPs who have per bandwidth contract, they also insert their own WISP-Services policies in order to manage their users and services. We divide these policies into service specification, service update, user access management and on-demand service policies.

- **Services Specification policies (SSP):** These policies represent the full description of service deployment methods adopted by the WISP to manage its services. Since deploying differentiated services consists in specifying IP service parameters (port, protocol, etc) and their quality of service, we divide the SSP policies in two categories: QOSP and FAP.
  - **Quality of service policies (QOSP):** These policies allow WISPs, to specify their own services according to the quality of service strategy adopted in the hotspot network. Obviously, specified strategies are tightly depending on the home WISP quality of service strategy. In case where DiffServ is applied, each service will be assigned to specific class of service (example: VoIP → EF, Web → BE) with

associated parameters. In case where Not DiffServ strategy, each service will be assigned a specific queue on the output.

- **Filtering Actions Policies (FAP):** These policies give a description of the services through filtering rules. Parameter of the filtering policies can be static (example: destination port =80) to handle known services or dynamic to handle applications such as VoIP, VoD, etc (pushed when a session is launched). The filtering rules can be either IPv6 or IPv4. In order to provide users with their guaranteed service levels, the filtering policies are applied in coordination with the quality of service policies. This is done thanks to an enhanced filtering engine which combine filtering and quality of services functionalities.

- **Service updates Policies (SMP):** In network management process, the WISP must be able to dynamically change its current services specification. For example, it may change bandwidth or services parameters. For those reasons we have defined the services updates policies which provide WISP with ability to dynamically change its current configuration. Currently, we provide means for changing Bandwidth parameters of existing service or class of service in DiffServ case. This policy is defined as follows:

  On Service update IF request= "change" then service_bandwidth ="new_rate"

- **User Access Management Policies (UAMP):** UAMP policies allow access control management of the users by specifying which types of users have access to certain services, under which conditions, and dynamic network adaptation according to the users SLA. When applying these policies, the access router adapts itself to meet the user's quality of service requirements contained in the service level agreement (SLA). There are two possible types of SLA that a WISP can sell, which led to two possible types of UAMP policies:
  - **Per service SLA:** in this SLA, users can choose one or more service among services list, and for each service specify their own quality of service parameters. For example, WISP sells VoIP, FTP, Mail, Web, VoD, and Video Conferencing. User John will buy VoIP and Mail, while Barbara buys VoD, Mail and FTP. Each service of each user has its own quality parameters. In order to give WISP with ability to manage their users and services, the UAMP policies have been defined as follows:

    On New User If (service name) and (conditions) Then Authorize service
    Else re-adaptation

    Conditions are related to quality of service parameters (available bandwidth, etc), date, time, number of currently running service sessions, etc. Re-adaptation consist in authorizing service, even when conditions are not accepted through quality of service dynamically

reconfiguration. For example, the voice over IP service is programmed using the following policy:

If (service = VoIP and VoIP available bandwidth)
Then authorize VoIP else Readapt.

If there is no available bandwidth for VoIP service, then the access router evaluate if it can recover bandwidth from other classes or change its configuration thanks to Readapt actions.

- **Packaged SLA:** in this SLA, services are grouped in different packages, and users can buy one among them. Each package has its specific QoS parameter. For example gold package contain VoIP, Mail and Web with 20, 20 and 20 Kbps respectively. Time connection is related to the entire service package. In this SLA, when user buys a package, he/she is given a profile. In order to manage this packages, the WISP will program its access router using the following UAMP policies: On New user If (user_profile) and (conditions) then
  Allow list of services
  Else degrade to other profile

  Conditions are related to available bandwidth on the access router, or to number of current connected users. For example, for the precedent gold package, the WISP will install
  if (user=gold) and (available bandwidth) then
  Allow Mail, VoIP, Web
  Else degrade to silver package.

  The available bandwidth provides means for checking if there are enough resources for the specified service package. For the both SLA, the UAMP policies provide means for dynamic service deployment thanks to automatic router adaptation.
- **On-Demand Service Policies (ODSP):** Materialize the value added services that a WISP may offer for its customers. For example, user may change its profile from silver to gold, in order to have better quality on voice over IP. The application of service update policies generate a modification of the associated filtering policies that have been applied for the user. These policies provide users with means for service upgrade and are pushed directly from user terminal to the access router (Web interface or some protocols). These policies have two main objectives, provide users with means for dynamically changing their requirements and allow them to configure access equipments according to their SLA which is stored in the user side (smart card). At present, we have defined the following policy

  On Update if (request="change") Then
  (user_profile = "new_profile")

This policy allows users to dynamically change their profile, thus allowing them to get more services without interruption.

2.3 Architecture Implementation

In this section, we describe the implementation of the policy management architecture on the access router. We have used the following access router functionalities: Dual stack (Ipv4 and Ipv6 support), DHCPv4/ DHCPv6 server, Radius Client, Filtering, and Quality of services. Figure 1 shows the elements of the implementation architecture.

Policy Manager: All policies defined in our architecture are described and validated using XML schemas and installed using: CLI (command line interface), an XML/HTTP connection, or a web interface directly of from remote machine. The Policy manager which is handled by the WISP administrator can receive policies from foreign WISPs when they have roaming contracts. It is responsible of validating the policies XML schemas, storing them in database, sending Add/Delete/Update messages to the appropriate WISP block. The entire policy manager has been developed using C++ language, because it provides more flexibility and scalability in implementing new services.

WISP block: When a foreign WISP establish roaming relationship according to per bandwidth model, a new module called WISP block is instantiated and created on the access router. The WISP block contains policy enforcement, policy rule tree and monitoring modules.

Policy Enforcement: It ensures the following tasks:

- After reception of the policies from the Policy Manager, it translates these policies into C++ objects and stores them in tree structure, and processes them. The policies which can be directly applied (QOS Policies) are translated to routers rules thanks to the Router Service API Module. For the others, it notifies the "event module" of the events types it is waiting for (UAM policies are launched by arrival of new users).
- Communicate with monitoring module to get local router information. For example, bandwidth use, number of users, ... etc
- Ensure keeping states about users deployed services in order to remove them when the user leaves the network.
- Periodically, or on request, it sends monitoring reports to the Policy manager.

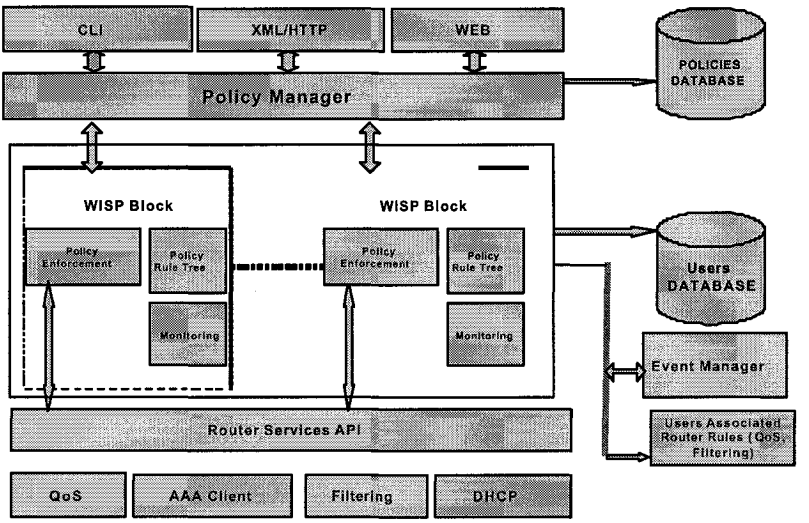

Figure 1. Access Router Implementation

Monitoring: The Monitoring module provides the policy enforcement a global view about all local router parameters and states. Currently, we can monitor quality of service, filtering, and date and Time parameters. In addition, monitoring provide very important information for achieving billing. These information concern amounts of data volume per IP address, last time an IP packet go through the router, etc. The Monitoring module can be acceded using XML requests, or simple function calls. All the monitoring information is sent to the policy enforcement point or can be directly sent to the Policy Server (PS). In addition, the PS can access directly to the monitoring module by sending XML requests.

Router Policy Tree: Policies are translated from XML schemas and stored in tree structure. This tree is of complexity equal to 1, because when new event is launched, the associated set of policies is directly retrieved without searching the entire tree.

Users Database: This database contains information about connected users such as profile, IP address, team and others. It is used by the policy manager module, and also by the WISP Administrator in order to have statistic information.

Event Manager: This module is responsible of managing events such as arrival of new users, new application request, or other events. This module interacts with existing modules such as authentication, web server, and CLI. Moreover, this module allows adding new functionalities on the policy

manager such as other authentication mechanisms or new events. For the event manager we have used the C language.

Users Associated Router Rules: This file contains indexes of actual router rules deployed for each user. The index size is low because it contains only single information per user. This file allows removing or updating services for users.

Router Services API: We have designed these API for the following three reasons:

- Provide single and simple way to use router services
- Offer means for dynamically updating router rules.

The API services are of two types: Functions calls and XML requests. The XML request support has been added in order to provide PDP or other advanced equipment with ability to directly monitor the access router, and changes its configuration without requiring other router modules.

Filtering Module: The Filtering Module called PFM is an engine that allows filtering and quality of service deployment at the same time. It works as follows:

- Output interface: implementation of quality of service queuing disciplines. We specify queues parameters (bandwidth, priority, borrow...) and scheduling algorithms (CBQ, WFQ...).
- Input interface: specification of filtering rules, based on IP packet fields such as version, protocol, port...

Quality of Service Module: This module provides traffic conditioning elements such as droppers, markers, shapers... It allows for example traffic limiting for services or users.

3. CONCLUSION

In this paper, new network management architecture for roaming and service management in hotspot networks has been detailed. The lack of solutions that allow multiple service provider support, service guarantee and service differentiation led us to propose this architecture. Our solution allows WISPs to get benefits from the large deployment of public WLANs, by differentiating services offered to their customers, efficient and simple architecture. Moreover, since access network is managed by the access routers, we can extend its functionalities to manage access points and to interact with wireless management solutions. For example, access router may control radio resources, and allow or deny new users that try to associate in busy or congested access points. This approach is currently subject of lot of works in IEEE and IETF [16]. Compared to the classical IETF PBM architecture, our solution offer two major improvements: (1) A

Further abstraction level has been added providing the administrator with the possibility to deploy services without having to know which device parameters to configure. (2) A distribute management model where more intelligence is pushed toward the access equipments (access networks). Furthermore, 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 layer 2 protocols.

4. REFERENCES

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

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

[3] 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.

[4] 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"

[5] Donald M. Fye, "Evolution of WLAN Roaming Services", CDG WLAN Technical Forum, Dallas, Texas, October 2, 2003

[6] Michael Kende, "WLAN challenges and opportunities", National Summit on Broadband Deployment , April 28, 2003

[7] Idir Fodil and Vladimir Ksinant "User Service Management in Hotspot network using Policies", European Wireless 2004, the fifth European wireless Conference, February 24-27 2004, Barcelona, Spain

[8] A.Westrinen and al, "RFC 3198: Terminology for Policy Based Management ", IETF, November 2001.

[9] David Kosiur,"Understanding Policy-Based Networking". Wiley Computer Publishing, 2001.

[10] Raouf Boutaba and Jin Xiao, " Network Management State of the Art", WCC, IFIP World Computer Congress, August 2002.

[11] O.Corre, I.Fodil, V.Ksinant and G.Pujolle, " An Architecture for Access Network Management with Policies", MMNS 2003, 6th IFIP/IEEE Conference on Network Management, September 2003.

[12] 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.

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

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

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

[16] IETF CapWap Working Group, http://www.ietf.org/html.charters/capwap-charter.html