# DiffServ Management on Mobile IP Networks using COPS-PR

Edgard Jamhour, Mauro Fonseca, Andre Beller, Thiago Pereira
PUCPR, PPGIA, Imaculada Conceição 1155,
90815-901 Curitiba, Brazil
{jamhour, mauro.fonseca, a.beller, tmp}@ppgia.pucpr.br,
WWW home page: http://www.ppgia.pucpr.br/docentes.html#redes

**Abstract**. This paper describes and evaluates a framework for managing Differentiated Services (diffserv) configuration on Mobile IP-based networks. In the considered scenario, users can keep their QoS privileges while they move along through different access networks interconnected by a diffserv domain. In this case, the edge routers receive the diffserv configuration dynamically, according to the authentication events registered by the home agent during the mobile node's handoff. The proposed framework is based on the IETF standards concerning diffserv management. The device configuration is represented in terms of a diffserv PIB, which is distributed to the diffserv edge routers using the COPS-PR protocol. By exploring the COPS-PR facilities, we define an efficient strategy for updating the PIB information in the managed devices without generating excessive management traffic. We conclude that, by properly exploring the COPS-PR facilities, the latency introduced by the COPS-PR management is not significant when compared with the Mobile IP handoff latency.

## 1 Introduction

This paper describes and evaluates a framework for managing SLS assignments on Mobile IP-based networks. The Mobile Internet Protocol (MIP) is an IETF standard that defines a tunneling technique for permitting a mobile host to keep its IP address regardless its attachment point with a backbone network [1]. MIP can be employed in cellular networks technologies such as GPRS and EDGE. MIP can also be employed to provide seamless roaming between wireless local-area networks (WLANs), or even across different types of infrastructures (i.e., WLAN and cellular networks).

In the scenario considered in this paper, users can keep their QoS privileges (i.e. SLS assignments) while they move along through different access networks interconnected by a *diffserv* domain. According to the IETF terminology, a SLS

*Please use the following format when citing this chapter:*

Jamhour, E., Fonseca, M., Beller, A. and Pereira, T. 2007, in IFIP International Federation for Information Processing, Volume 229, Network Control and Engineering for QoS, Security, and Mobility, IV, ed. Gaïti, D., (Boston: Springer), pp. 187–198.

(Service Level Specification) represents a subset of a SLA (Service Level Agreement) that refers to traffic characterization and treatment [2]. In order to keep the SLS assignments of mobile nodes, the *diffserv* edge routers must receive their configuration dynamically, according to the authentication events related to the mobile node's handoff.

This paper addresses the problem of building a framework for supporting QoS provisioning in presence of mobility by exploring the IETF standards concerning *diffserv* management. The framework follows a PEP/PDP architecture, using a provisioning approach [2]. The PEP (Policy Enforcement Point) is responsible for representing a managed device and requesting the initial *diffserv* configuration from the PDP. The *diffserv* configuration is represented in terms of a *diffserv* PIB (Policy Information Base), which contains a vendor independent description of the configuration assigned to a network device [3]. The PEP is also responsible for interpreting the PIB and installing the configuration into the managed device. The PDP (Policy Decision Point) is responsible for generating the PIB with the configuration corresponding to the SLS assigned to the users. The PIB is transferred from the PDP to the PEP using the COPS-PR protocol [4].

In order to support the user's mobility, the PIB information must be updated and transferred from the PDP to the PEPs as a response of a handoff confirmation event. The COPS-PR protocol supports sending non-solicited PIB updates from the PDP to the PEP. However, an important aspect that must be addressed is how to preserve the user's QoS privileges in distinct access networks, where the network devices implement distinct QoS mechanisms and benefit from different levels of available bandwidth. This paper addressed this problem by proposing a three-layer policy model. A high level policy model (HLPM) is used for defining SLS assignments using rules that take into account the facilities in each access network. A configuration level policy model (CLPM) is used for defining the device configuration independently of the specific device capabilities. Finally, a *diffserv* PIB is generated by compiling the CLPM and by taking into account the specific device capabilities. This strategy is based on the work published on [5], but several modifications have in introduced in order to support mobility.

This paper is structured as follows. Section 2 reviews the concepts related to MIP and *diffserv*. Section 3 presents an overview of our framework for managing *diffserv* configuration in MIP-based networks and discusses the strategy for implementing the *diffserv* PIB updates. Section 4 presents the three-layer policy model adopted by the framework. Section 5 presents some results concerning the strategy defined in section 3. Section 6 reviews some related works, pointing the main difference of this paper with respect to other published works addressing the QoS management in mobile environments. Finally, the conclusion summarizes the main results of this work and points to future developments.

## 2 Mobile IP and Diffserv

The Mobile IP (MIP) standard [1] treats the problem that may arise when a host changes its IP address during a communication. A mobile host changes its IP address

because the IP protocol assumes that each IP network identifier is related to a specific physical network. If a mobile node (e.g. a cellular device) connects to another physical network, it must change its IP address. Changing the IP address during a communication session will require restarting any application being executed in the mobile node.

MIP solves this problem by using a tunneling technique. Each mobile host has two IP addresses. One address is related to its "home network" (where the mobile host is registered), and does not change when the host changes its position. The second address is related to a "foreign network", and changes each time the host attaches to a different physical network (refer to Fig. 1). This second address is called CoA (Care-of Address). The router attached to the mobile host at the foreign network is called "foreign agent" (FA). The router at the home network is called "home agent" (HA). The home agent is a special router, responsible for authenticating the mobile host, and keeping an internal table mapping the CoA to the home IP address of every mobile host it serves. Mobile IP specifies that is up to the mobile host the responsibility of informing the home agent that it has changed its CoA. For doing this the mobile host sends a "binding update" message to the home agent each time it changes a CoA. The message is delivered to the home agent by the foreign agent. The binding update message contains a digital signature allowing the home agent to validate the binding request. From a non-mobile host viewpoint, a mobile host is identified by its home IP address. Packets from the Internet are delivered to the mobile host through a tunnel that follows the hosts while it changes its position and attaches to different networks. Depending on the preferred implementation, this tunnel can be created between the home agent and the foreign agent, or between the home agent and the mobile host. The tunnel is created by encapsulating the incoming packets from the Internet, addressing the mobile host by its home address, with an IP header that addresses the mobile host by its Care-Of Address (CoA). If the tunnel is created only up to the foreign agent, then all the mobile hosts served by the same foreign agent can share the same CoA. If the tunnel is created up to the mobile host, than every mobile host must have their own CoA. Please refer to [1] for more details about the Mobile IP standard terminology and operation. The work described in this paper assumes all the tunnels are created between the home agent and the foreign agent (i.e., the mobile nodes share the foreign agent CoA).

The *diffserv* QoS methodology defines two main entities: the edge router and the core router [6]. The *edge router* is responsible for policing and assigning an aggregated class to the packets transmitted by the hosts. According to the *diffserv* methodology, a *core router* does not differentiate individual flows. Instead, packets are handled according to the aggregated classes assigned by the edge routers. Fig. 1 illustrates how a MIP-based network could be adapted to the *diffserv* QoS methodology. For the sake of simplicity, we have assumed that the functions of foreign agent (FA) and home agent (HA) are accumulated by the edge routers.

The IETF defines fourteen aggregated classes for the core network (i.e., expedited forwarding - EF, 12 X assured forwarding - AF and best effort - BE). An edge router is responsible for policing the traffic and assigning an aggregated class according to the SLS assigned to the mobile host. Considering the MIP scenario, the edge router configuration must be updated when the mobile host moves from a FA

domain to another. In this case, the mobile host's SLS configuration must be added to the FA in the incoming domain and removed from the FA in the previous domain.

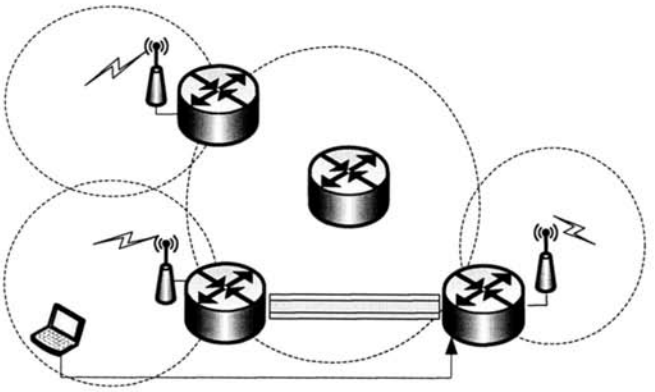

**Fig. 1.** Diffserv and MIP

## 3 Strategy for Updating the Foreign Agent Configuration

The framework described in this paper adopts the *diffserv* PIB standard for representing the distributing the edge router's configuration [3]. A PIB module is a named data structure described as a conceptual tree where the branches represent Provisioning Classes (PRCs) and the leaves represent Provisioning Instances (PRIs). The *diffserv* PIB PRCs model a Traffic Condition Block (TCB), which is formed by zero or more classifiers, meters, actions, drop algorithms, queues and (packet) schedulers.

As shown in Fig. 2, in the *diffserv* PIB, the functional elements (classifier, meter,...) and their parameters (IP filter, token-bucket parameters,...) are represented by distinct PRCs. The "*Specific*" attribute in the functional PRCs is used for associating a functional element to its parameters by using an *Object Identifier* (OID) pointer. The functional PRCs also include the "*Next*" attribute to indicate the sequence of *diffserv* treatment for the packets (Fig. 2 illustrates a possible sequence). Fig. 3 shows an example of how the packets from a user are classified (by the IPfilter) and receives a specific policing treatment (by the Meter, TBParam and AlgDrop) and specific marking action (DSCPMark). The marking action is responsible for assigning an aggregated core class to the packets generated by the user.

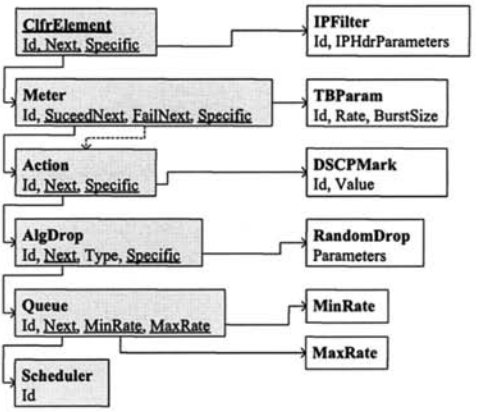


**Fig. 2.** Diffserv PIB overview

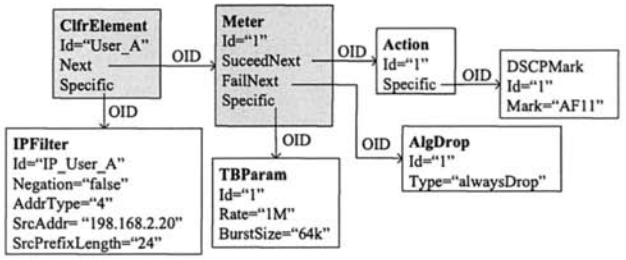


**Fig. 3.** Diffserv PIB configuration example

Considering the MIP scenario, a FA should contain the configuration of all possible mobile users that could be attached to its network. This approach, however, is understandably not practical. Therefore, the framework proposed in this paper adopts a dynamical configuration of the FAs, which is triggered by the authentication events generated by the HA. By analyzing the *diffserv* PIB structure, one observes that the configuration process can be significantly simplified if the PIB elements are classified into static and dynamic information. This approach, illustrated by Fig. 4, assumes that most users will share a small number of SLS definitions. The SLS definitions are represented by the "white PRCs" and are considered static information. The PRCs responsible for the SLS assignment (i.e., mapping a user to a SLS definition) are represented by the "dark PRCs" and are considered dynamic information. Because we have assumed that all tunnels are created between the FA and the HA, the mobile host is represented by its home address. The static information can be provisioned at the initialization of the FA. The dynamic information must be updated when mobile host moves from one FA domain to another. In this case, the FA in the incoming domain must receive the new filter

information for associating the packets generated by the mobile host to the corresponding SLS assignment. Similarly, the filter information must be removed from the FA in the previous domain.

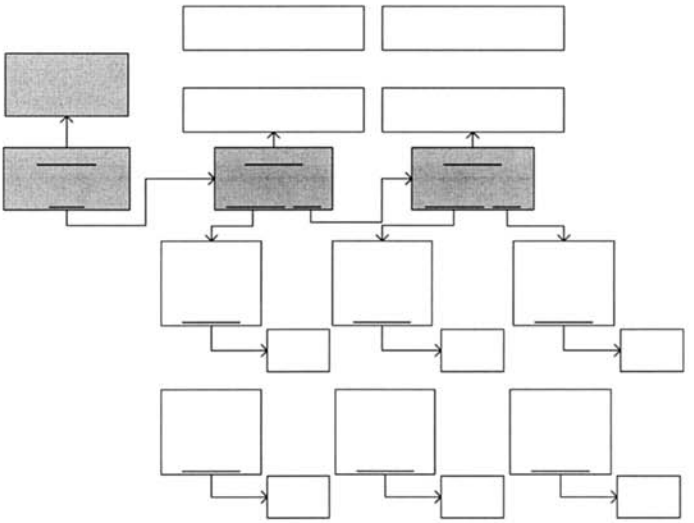

**Fig. 4.** Static and Dynamic PIB information

Fig. 5 illustrates how the PDP/PEP approach can be adapted to the MIP - *diffserv* environment. The *diffserv* routers are represented by the PEP agents. In a typical operation scenario, when the HA authenticates a binding request from a mobile host **(1)**, it sends a notification event to the PDP **(2)**. Then, by using the COPS-PR protocol, the PDP updates the configuration of the FA *diffserv* routers. In order to reduce the latency of the update process, a logical choice is to place the PDP in the same network as the HA.

The messages exchanged between the PDP and the PEPs are illustrated by Fig. 6. The first set of messages (1 to 5) corresponds to the initial provisioning process where a PEP requests the static PIB configuration. After this, the PDP sets the PIB's flag "FullState = False", informing the PEP that the subsequent DEC messages must be interpreted as updates (i.e., the PEP must not delete the previous PIB incarnation). The update process is implemented by a non-solicited decision message transmitted from the PDP to the PEP.

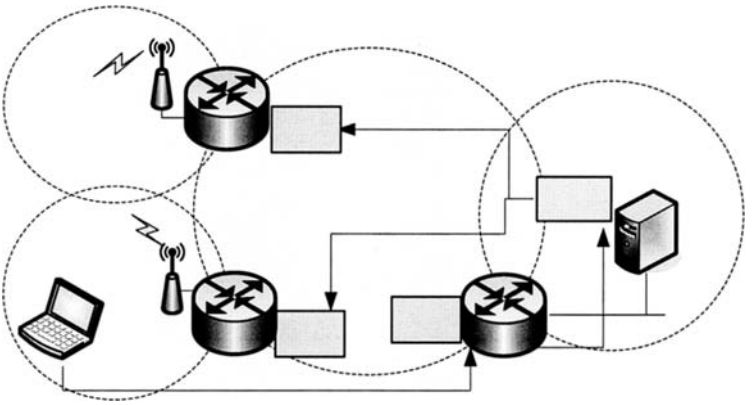

**Fig. 5.** Deployment Overview

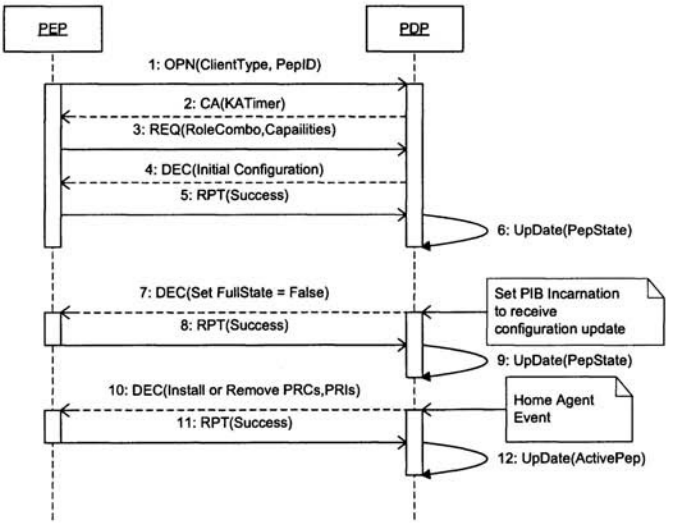


**Fig. 6.** COPS-PR messages exchange during provisioning process

## 4 Three-Layer Policy Model

An important problem that must be solved by a *diffserv* management framework is how to take into account the different QoS mechanisms implemented by the edge routers during the configuration process. An important IETF contribution for

addressing this problem is QPIM (Policy QoS Information Model) [7]. QPIM is an information model that permits to describe device independent configuration policies. By defining a model that is not-device dependent, QPIM permits to "re-use" QoS configuration, i.e., configuration policy concerning similar devices can be defined only once. QPIM configuration is expressed in terms of "policies" assigned to "device interfaces", and does not take into account business level elements, such as users, applications, and network topology. The RFC 3644 that defines QPIM, points that a complete QoS management tool should include a higher level policy model that could generate the QPIM configuration based on business goals, network topology and QoS methodology (diffserv or intserv) [6].

In other to address these problems, this paper proposes a tree-layer model illustrated in Fig. 7. The model is based on a previous publication [5], but some modifications have been introduced in order to adapt the framework to the MIP scenario, as explained in section 3. The explanation in the remaining of this section follows the numbers in Fig. 7.

According with the strategy defined by the framework, an administrator defines a library of QPIM actions **(1)** corresponding to the SLS's that will be assigned to the users. In the high-level policy model (HLPM) **(2)**, the administrator writes the business goals assigning SLSs (i.e., QPIM actions) to the customers in the managed environment. The HLPM extends the IETF PCIM/PCIMe model and supports the semantic: "*User(s) accessing (an) Application(s) in (a) remote Server(s), from (an) access Network(s) receives a specific Service Level*". Users, Applications and Network elements in a HLPM policy are expressed in terms of CIM objects **(3)** (see [2] for CIM and PCIM definitions). By using CIM associations, the HLPM defines also protocol and topology information, by assigning Users and Servers to IP addresses and Applications to protocols and transport layer ports.

The Translation Process **(4)** converts the high-level information into configuration policies, which are device independent (i.e. the configuration translates the desired QoS effect without specific mechanisms details, such as scheduler type or drop algorithm). For example, "*The traffic with IPsrc=210.0.0.5 and port=21 receives BW=25%*". The configuration-level policy model (CLPM) **(5)** is defined as a combination of PCIM/PCIMe and QPIM classes in order to support the representation of both elements in a device configuration: traffic identification (conditions) and traffic treatment (actions). Conditions are described in terms of IP header packet filters and actions are described in terms of QoS mechanisms, such as schedulers and drop algorithms. The CLPM includes also the mapping between the configuration policies and the device interface roles. This mapping is deduces from the topology information extracted from the HLPM. Both high-level and configuration model classes, as well as the translation process, are detailed in [5].

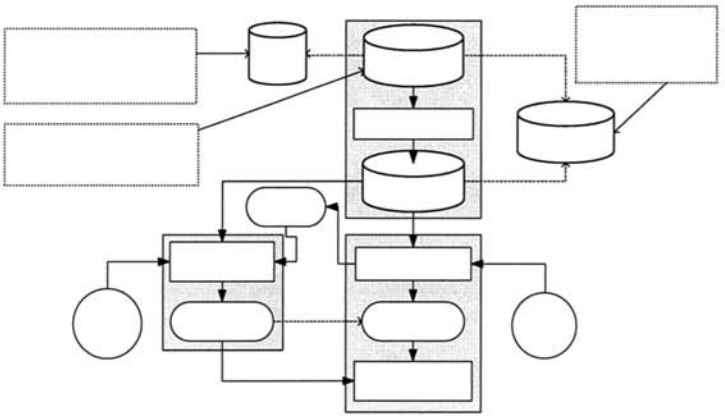

**Fig. 7.** Framework Overview

In the decision process **(6)**, the configuration policies are transformed to *diffserv* PIB instances **(7)**. This process is executed when the PDP receives a COPS-PR request message (REQ) **(5)** from the PEP asking for provisioning configuration. The REQ message includes two set of information that is used as input parameters in the decision process: (i) *RoleCombination*, which are labels associated to the managed device interfaces; (ii) *DeviceCapabilities*, describing the specific QoS mechanisms supported by the managed device. First the PDP uses *RoleCombination* for selecting the relevant policies for the managed device interface and second, the PDP converts the configuration policies into provisioning instances of the *diffserv* PIB, according to the set of *DeviceCapabilities*. The PIB information is generated from the QPIM configuration by a transformation process that takes into account the capabilities (i.e. supported QoS mechanisms) of the managed device.

In order to support mobility, the initial PIB provisioning generated by the REQ event **(5)** does not contain the filter definitions. Instead, it contains only the actions corresponding to the SLSs supported in a specific access network represented by the PEP. The filter definitions are generated as a response to a mobility event (i.e., an authentication event generated by the home agent [1]). An authentication event has two effects: First, it removes the corresponding filters entries from the PEP representing the previous network the user were registered. Second, it adds new filter entries to the PEP representing the new network the user has registered. A PIB can be partially updated by adding or removing PRIDs, which correspond to specific PIB information represented by unique identifies (OIDs).

Finally, the distribution process **(8)** consists in transmitting the *diffserv* PIB PRIDs using the COPS-PR protocol.

## 5 Evaluation

In order to evaluate the strategies discussed in Section IV, we have implemented the prototype illustrated in Fig. 5 and 7. Both, the PDP and the PEP have been implemented in Java and are hosted by an Intel Pentium IV, 1.5 GHz PC, running a Linux operating system. The Mobile IP software corresponding to the mobile host, foreign agent and home agent is based on the free code available on [8]. The code was modified in order to generate a notification event to the PDP when a binding update request is confirmed by the home agent.

As illustrated in Fig. 5, the same Linux host plays the role of *diffserv* router, mobile IP foreign agent and PEP. The diffserv mechanisms are implemented by using the "*linux traffic control*" facilities available on the Linux platform. Similarly, the host that implements the home agent also accumulates the role of *diffserv* router. The PDP is implemented on an independent machine, and communicates with the home agent through a socket interface. In the evaluation scenario, the MIP tunnel is created only between the home agent and the foreign agent. Tests have been implemented in order to evaluate the latency introduced by the diffserv PIB update process. Table 1 presents a summary of the average delay measured for the most important events related to the handoff process. The table results must be considered for comparison purposes only, since we have considered only a single hop between the FA and the HA, and Ethernet links of 10 Mbps for connecting the routers.

The messages in Table 1 have been captured at the home agent network. The only exception is the MIP advertisement messages, which have been captured at the mobile host. One observes that the total latency introduced from the moment the mobile node has its registration confirmed (4) to the moment the PEP reports that the PIB update have been installed into the device (6) is about 0.31 seconds. The most important latency is introduced by the MIP messages. According to the MIP standard [1], each mobile IP advertisement message has a lifetime field that defines for how long a foreign agent route must considered "active" in the absence of new advertisement messages. After a link layer handoff, the mobile host must wait for the previous foreign agent route lifetime expiration before starting the registration in the incoming network. The latency of 3.40 seconds between the handoff event and the registration request event is the result of a lifetime of 3 seconds (the default value in the MIP package implementation [8]). Considering that the lifetime field in the mobile IP advertisement messages is an integer number of seconds, the minimum expected lifetime is 1 second. The MIP standard defines that the mobile advertisement messages must be transmitted in intervals of 1/3 of the defined lifetime.

**Table 1.** Average time between the events related to the Mobile's IP handoff process

| Event | Elapsed Time [s] | Message Size [bytes] |
|---|---|---|
| 1. Network Layer Handoff | 0.00 | - |
| 2. Third Mobile IP Advertisement Message | 3.21 | 67 |
| 3. Mobile Registration Request (at HA) | 3.40 | 236 |
| 4. Mobile Registration Reply (at HA) | 3.42 | 275 |
| 5. COPS Decision (DEC) Message | 3.49 | 538 |
| 6. COPS Report State (RPT) Message | 3.73 | 90 |

## 6 Related Works

There are a growing number of significant works relating QoS management of mobile users. Generally speaking, these works can be classified into two major groups: those addressing micro-mobility and those addressing macro-mobility. Micro-mobility and macro-mobility are defined as changes of access point association (attachment) while a session is in progress. Micro-mobility is the simplest form of mobility. The subscriber is moving within a single domain, where, usually, mobility is handled at the link layer level. Macro-mobility involves moving between two domains, where the link layer facilities are not sufficient for keeping a transparent session to the subscriber. The work in this paper can be classified as addressing the Macro-mobility issue only.

While the work in this paper adopts a provisioning approach, some works address the QoS issue by proposing a signaling protocol for providing QoS on demand. The authors in [9] propose a new signaling protocol allowing mobile users to contact a differentiated bandwidth broker for QoS negotiation. The work presented in [10] proposes a mobility-aware QoS signaling architecture that integrates resource management with mobility management to provide the necessary QoS on demand in mobile wireless networks. It is based on a domain resource manager concept and support anticipated handover with pre-reservation of resources before the mobile node is attached to the new access point.

Our proposal adopts the *diffserv* QoS methodology. There are some proposals adopting a combination of *intserv* (Integrated Service) and *diffserv* methodologies. For example, to negotiate *QoS* specification in macro mobility, [11] proposes an end-to-end QoS provisioning architecture, combining both *diffserv* and *intserv* QoS methodologies. The BRAIN European project [12] and its successor the MIND [13] project proposed an access network that provides seamless mobility and QoS for different applications, ranging from best effort services to services with hard QoS requirements, such as IP telephony. The BRAIN QoS architecture is based on the *intserv* and *diffserv* architectures. The fundamental concept is to use *intserv* parameters and RSVP signaling to communicate application requirements to the connecting network, and to provide the actual service differentiation with the diffserv scheme. Extensions to the basic architecture have been designed to enable enhanced support for mobility and QoS, although lacking a SLA support.

## 7 Conclusion

This paper has presented framework for supporting the diffserv configuration in mobile IP based networks. The proposal is based on IETF standards, concerning diffserv configuration, where the most important elements are the PIB *diffserv* and the COPS-PR protocol. Our study shows that both, the PIB and COPS-PR offer enough flexibility for addressing the mobility problem without introducing new protocols or modification on the existing standards. Our work has proposed a strategy for updating the *diffserv* configuration by exploring the PIB structure, where the QoS action mechanisms are provisioned at the initialization of the *diffserv* edge routers and the filter definitions (i.e., SLS assignments) are updated dynamically as a response to the registration confirmation event generated by the home agent. The strategy is very simple to implement and introduce a relatively low latency in the configuration process, when compared with the latency introduced by the MIP handoff process. Future works will evaluate the strategy considering larger environments in order to estimate possible bottlenecks related to the PDP performance.

## References

1. Perkins C (1996), ed, "IP Mobility Support", IETF RFC 2002.
2. Schnizlein J, Strassner J, Scherling M, Quinn B, Herzog S, Huynh A, Carlson M, Perry J, Waldbusser S (2001) "Terminology for Policy-Based Management", IETF RFC 3198.
3. Chan K, Sahita R, Hahn S, McCloghrie K (2003) "Differentiated Services Quality of Service Policy Information Base", IETF RFC 3317.
4. Chan K, Seligson J, Durham D, Gai S, McCloghrie K, Herzog S, Reichmeyer F, Yavatkar R, Smith A (2001) "COPS Usage for Policy Provisioning (COPS-PR)", IETF RFC 3084.
5. Beller A, Jamhour E, Pellenz M (2004) "Defining Reusable Business-Level QoS Policies for DiffServ", Proceedings of Distributed Systems Operations and Management WorkShop, pp 40-51.
6. Blake S, Black D, Carlson M (1998) "An Architecture for Differentiated Services", IETF RFC 2475.
7. Snir Y, Ramberg Y, Strassner J, Cohen R, Moore B (2003) "Policy Quality of Service (QoS) Information Model", IETF RFC 3644.
8. Andersson B, Malinen J, Forsberg D, Kari H, Hautio J, Mustonen K, Weckström T, "Dynamics Mobile IP", http://dynamics.sourceforge.net/.
9. Braun T, Stattenberger G (2001) "Providing Differentiated Services to Mobile IP Users", The 26th Annual IEEE Conference on Local Computer Networks (LCN'2001), Tampa, USA.
10. Bless R, Zitterbart M, Hillebrand J, Prehofer C (2003) "Quality-of-Service Signaling in Wireless IP-based Mobile Networks", VTC2003-Fall, Orlando, FL, USA.
11. Pack S, Choi Y (2001) "An End-to-End QoS Provisioning Architecture in Mobile Network", in Proc. International Symposium on Communications and Information Technologies (ISCIT) 2001, Chiangmai, Tailand.
12. IST-1999-10050 BRAIN, Broadband Radio Access for IP-based Networks, www.istbrain.org.
13. IST-2000-28584 MIND, Mobile IP-based Network Developments, www.ist-mind.org.