

RESACO¹ : an open and programmable multi-domain platform for cooperative and auto-configurable networks

Wajdi Louati* Klecius Cardoso* Wassef Louati* Houda Labiod** Marc Girod-Genet*
 Artur Hecker** Badii Jouaber* Djamal Zeglache*

* *GET-Institut National des Télécommunications
 9 rue Charles Fourier - 91011 EVRY, France*

** *GET-Télécom Paris; LTCI-UMR 5141 CNRS
 46 rue Barrault, 75634 Paris, France*

Abstract-- *This paper presents a set of studies and proposals related to cooperative, auto-configurable and adaptive networks. It summarizes some extensions and experiments performed within the RESACO project. The objective of this project is to propose viable architectures and tools that enable and enhance Quality-of-Service (QoS), mobility, service discovery and security aspects over multi-domain and heterogeneous networks. The proposed extensions are based on the use of programmable software-based edge routers and access points. Additional features that enable adaptability, auto-configuration and cooperation are experimented.*

Keywords: *auto-configurable, software-based router, heterogeneous networks, WiFi, GPRS/UMTS, service discovery*

1. INTRODUCTION

B3G solutions are likely to be implemented by combining existing solutions currently being developed to support adaptation, interoperability and cooperation. The main challenges are management and optimization of service access over heterogeneous access and transport networks. In addition, service offers will be personalized and based on context, according to user location, preferences and terminal capabilities. Different network and service providers will own and share these environments and possibly share their resources while protecting their conflicting business interests.

For all these reasons, new management solutions to enable cooperation are needed. The aim of the RESACO project is to analyze and propose solutions to enhance cooperation between these heterogeneous technologies and to facilitate QoS and security management and auto-configuration. The project has limited its initial scope by focusing mainly on the following:

- Inter-technology inter-working and vertical handover,
- Inter-domain security management,
- Inter-domain QoS and bandwidth management,
- Service discovery,
- Adaptive, auto-configurable and programmable access.

¹ RESACO which stands for "RESeaux Adaptatifs et COopératifs" is funded by the "Groupe des Ecoles de Télécommunication" (GET), 2003, France.

The objective of this paper is to present the analysis, test-beds and various experiments carried out throughout the first year of the project. The goal has been to assess the feasibility and the viability of different solutions for heterogeneous network cooperation.

Section II of this paper reviews and discusses WLAN and GPRS/UMTS inter-working solutions. Section III presents the feasibility of adaptive and auto-configurable network entities. These network elements include a WLAN access point and an IP/DiffServ edge router. In section IV, a security framework for a multi-domain network architecture is presented. Section V describes the integration of the service discovery and the access control architectures. Section VI concludes the paper.

2. WLAN, GPRS. AND UMTS INTERWORKING SOLUTIONS

One of the main advantages of mobile networks, such as GPRS and UMTS, resides in their sophisticated and efficient mobility management schemes. However, they are incapable of offering higher throughput to enable multimedia applications. At the opposite, WLANs technologies can offer higher throughputs but they have not been conceived to handle mobility. WLANs do not embed billing and user management policies. Even if these two technologies are continuously being improved through successive releases, it appears interesting to take advantages of both technologies according to users' needs and context. Many studies have already investigated WLANs and GPRS/UMTS inter-working and cooperation. Two main approaches, which appear to be viable, are described in ETSI and 3GPP standards. They are respectively denoted as "**tight coupling**" and "**loose coupling**" solutions.

The tight coupling approach is more suited when a unique provider owns and manages both the GPRS/UMTS and the WLAN networks. It relies on the reuse of GPRS/UMTS facilities including mobility, billing and security management. In this approach, the WLAN is connected to the GPRS/UMTS network through the Gb/Iu-ps interfaces. In this first approach, no major additional developments are needed to enhance WLAN architectures.

The loose coupling approach is a general-purpose architecture. It can be used even if different providers own the WLAN and

GPRS/UMTS networks. The WLAN is connected to the GPRS/UMTS network through the Gi interface and additional features are needed to ensure mobility, security and billing features within the WLAN segment. The interconnection with the GPRS network is achieved through the use of a *Cellular Access Gateway* (CAG). Table 1 summarizes and compares the two architectures.

	Tight Coupling	Loose Coupling
Security	Possible reuse of GPRS mechanisms (authentication and encryption)	Additional CAG for authentication based on IMSI
Billing	Reuse of GPRS billing system	Need of new billing management system
Mobility	SGSNs manage the handover	May rely on Mobile IP. Handovers can be performed by both GGSN and/or CAG
Performances	The SGSNs have to manage GPRS and WLAN data flows.	GPRS and WLAN data flows are on separate links.
Development costs	Marginal	Additional developments in the WLAN (CAG, AAA and billing system required).
Usage	Only if the GPRS provider owns the WLANs.	No restrictions

Table 1: Comparison between WLAN and GPRS/UMTS inter-working architectures

3. SOLUTIONS FOR ADAPTIVE AND AUTO-CONFIGURABLE NETWORK DEVICES

In order to evaluate, study and experiment different proposed extensions and additional features related to cooperative and adaptable networks, open and programmable network entities have been considered within the project. This has been motivated by the fact that available commercial network devices such as WLAN access points and IP routers are not sufficiently open and currently do not offer online configuration without disturbing ongoing traffic. Since within RESACO highly flexible and open solutions are sought after, software-based solutions to ensure auto-configuration and adaptability have been retained. In particular, open software based access points for WLANs and open Edge router technologies have been investigated and designed.

3.1. Open and adaptive software-based WLAN access Point

The proposed solutions for open and adaptive WLAN access points are based on extensions of the HostAP project². HostAP is an open software based framework that transforms an 802.11 WLAN card into a software access point. In order to enable end to end harmonized QoS over the wireless and the fixed transport network, the first extensions are related to QoS handling. A QoS differentiation feature is added on the radio interface part of HostAP. DiffServ routing capabilities were also added on the transport interface. A dynamic Policy Based Management framework (PBM) [2], based on the Common Open Policy Service (COPS) protocol [1], has been integrated in the open programmable access point. This PBM allows the dynamic management and configuration of both wireless and

fixed interfaces for both uplink and downlink flows. All key parameters related to resource management for both radio and fixed networks interfaces are stored into dedicated Management Information Bases (MIBs).

The overall architecture proposed for this adaptive and flexible software AP is composed of the following elements:

- HostAP framework
- Additional DiffServ capabilities at the AP and core network interface,
- Additional service differentiation capabilities on the wireless interface
- A Policy Based Management framework based on COPS

The two main components of the PBM framework are the Policy Decision Point (PDP) responsible for decision-making and the Policy Enforcement Point (PEP) responsible for applying these decisions on the managed network entities. A Policy Information Base (PIB), containing policies and rules to be applied, is attached to the PDP. The COPS protocol is used to exchange management information and decisions.

In the proposed architecture, the PDP and PEP entities are added to the AP.

- The PEP entity integrated in HostAP is responsible for enforcing the decisions concerning the management of the radio part and its dynamic bandwidth allocation.
- A second PEP entity is also integrated in the DiffServ routing module to enforce the decisions concerning DiffServ parameters and policies on the fixed network segment.
- A local PDP (LPDP) and its corresponding PIB is included in the architecture to make local decisions and minimize data exchange with the remote PDP.

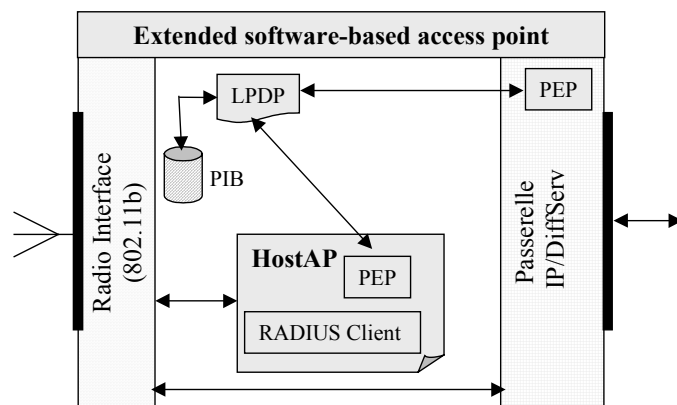


Figure 1: An extended open software-based architecture

For security handling, HostAP currently contains a RADIUS client for user authentication. Ongoing functional and performance evaluations of these security extensions will be reported in separate contributions.

3.2. Open and adaptive software-based edge router

The rapid evolution of network management techniques and policies and the rapid increase of exchanged data volumes and

² Jouni Malinen, <http://hostap.epitest.fi/>

service diversity, require more and more flexible and high performance network devices. In Next Generation Networks (NGN), edge routers will play a key role in internetworking, managing and controlling of data flows. Software-based routers are attractive solutions that can offer both high flexibility and performance. Recently, many extensible frameworks have been proposed to improve software-based routers [3][7].

Within the RESACO project, architectural extensions are proposed to enable more flexibility and dynamic configuration. The proposed architecture is based on the IETF **ForCES** (Forwarding and Control Element Separation) [8] architecture proposed for NGN programmable networks. This architecture defines three interdependent functional blocks (management plane, control plane and forwarding plane) connected by standard interfaces.

Extensions to enable dynamic adaptation of the data plane are achieved through the use of the *SMP Click* modular language [9]. Moreover, standard interfaces defined by the Network Processing Forum (NPF) [10] have been implemented to provide and manage interactions between the different planes.

In this architecture, each Network Element (NE) is defined as a set of logical entities. Two types of NEs are specified: the control element (CE) operating at the control plane and the forwarding element (FE) operating at the forwarding plane. Control Elements include control functions (routing and signaling) while Forwarding Elements perform packet-processing functions.

The plane separation approach and the ForCES architecture are combined in the proposed architecture to achieve the desired flexibility and performance. The proposed solution is implemented using the high performance *SMP Click* software language for the forwarding plane. *SMP Click* is a flexible software tool for creating configurable and extensible routers. It is derived from the Click modular router, providing both flexibility and high performance on multi-purpose multiprocessor platforms. A Click router is built by assembling software components into a directed graph. Each component (or element) represents a unit of router processing (such as packet classification, queuing, scheduling, etc).

In order to achieve run time extensions on the Click router, we can dynamically update the router configuration, by adding, modifying or removing router components or parameters. With these actions, it is possible to automate runtime configuration processes and make the router auto-configurable (using rules).

4. MULTI-DOMAIN SECURITY AND QOS MANAGEMENT

Networks can share their resources and offer the best possible QoS for users according to their location and needs. Security functions enable user and network authentication and authorization. Service Level Agreements (SLAs) can be established between network owners and users to establish agreements on QoS and security to define specific strategies concerning QoS, billing and mobility management.

The DiffServ framework is particularly suitable to be a common policy for QoS handling over multi-domain cooperative networks. Policy Based Management strategies can be used in order to automate decision-making and facilitate network cooperation and information exchange. Within RESACO, an inter-domain QoS management framework based on the use of DIAMETER[11] and COPS has been adopted. As described previously, COPS entities have been integrated into an open software-based access point and an open software-based edge router. A Policy decision point (PDP) is embedded within the introduced Bandwidth Brokers (BB) [12] defined in each domain to achieve inter domain cooperation. The BB is a software agent that performs SLA/SLS negotiation and allocates resources on a per-flow basis. This BB can manage intra-domain and inter-domain DiffServ QoS negotiation.

Communications between BB's require the use of secure communication channels to ensure privacy and integrity. DIAMETER fulfills these security requirements. Assuming the existence of AAA servers in each domain, RESACO extended DIAMETER with DiffServ features to provide security and achieve QoS control. New DIAMETER commands and AVP (attribute-value-pairs) are defined to transfer QoS related control parameters.

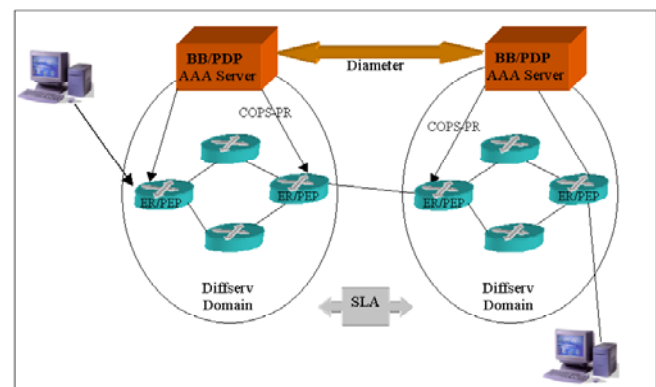


Figure 2: Inter-domain QoS and DiffServ Management

5. SERVICE DISCOVERY WITH CONTEXT-AWARE ADAPTATION AND COOPERATION

The purpose of a service discovery protocol (SDP) in RESACO is to enable users, applications or terminals to locate, find necessary information on local neighboring services, notify the offered services, and to use available services within the ambient infrastructure composed of the interconnection of several heterogeneous multi-services and multi-providers' networks (2G, 3G, IEEE 802.11, Bluetooth).

Service discovery is very challenging because of the heterogeneity and the dynamicity of related networks. It allows the homogenisation of the offered services and to enable automatic service discovery in a multi-domain context.

Existing service discovery protocols for wireless networks are usually classified in two categories: proactive (or push-based) and reactive (or pull-based) SDPs. A proactive SDP uses a broadcast mechanism, where each node unsolicitedly advertises the services it can offer to the rest of the nodes in the network. This push-based strategy is used in IEEE802.11 WLAN and HiperLAN. In case of reactive SDPs, each node queries other

nodes for the services it requires. This approach is used in Bluetooth networks. A problem with proactive SDPs is large bandwidth requirement for message broadcasts. In addition, there is a potential for long latency in discovering services, especially when nodes take turns in sending broadcast messages as in IEEE802.11 LAN. Reactive SDPs suffer from bandwidth overhead (but less than that for proactive SDPs) and long latency (longer than that for proactive SDPs) to find the required services.

In this work, we propose an architecture, where users can detect wireless network services, negotiate with the identified service providers about price and service features, select the best service, and finally configure their devices according to the selected service. The architecture is based on UPnP (Universal Plug and Play) [13] and takes into account user profiles and ambient features of the traversed environments fulfilling adaptation and cooperation goals between the cooperative networks. UPnP is a distributed open networking architecture aiming to provide an easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks; it enables seamless proximity networking for data and control transfers and automatic discovery for a breadth of device categories. UPnP mainly uses Web and IP protocols such as TCP/IP, UDP, HTTP and XML.

We assume that the code required to execute the available services does not exist on the user side until a need for this service is noticed; this latter obviously depends on the geographic location. Therefore, leaving the service zone imply the release of the software resources and the associated configuration.

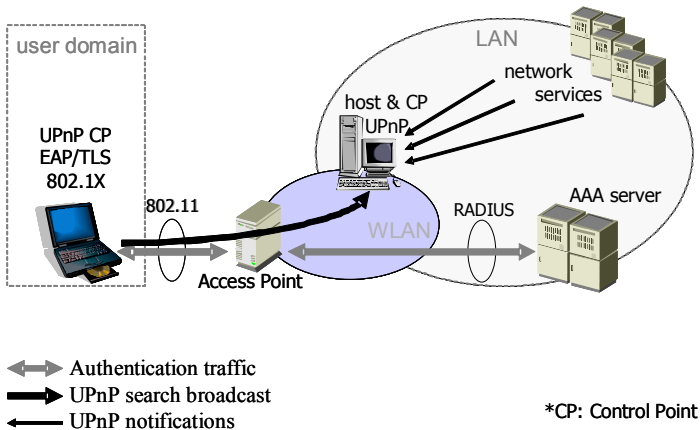


Figure 3: Service discovery and IEEE 802.1X access control RESACO architecture for a local domain

The service discovery procedure is executed once the access control finishes successfully. In RESACO it is necessary to integrate the access control and service discovery phases. This integration seems essential because the services proposed to users depend on their profiles and contexts and on the security policy. An AAA server represents a well-known interface used to access such information. Moreover, since the user authentication method is also part of user's profile; both procedures can rely on common authorization bases.

Thus, we propose an AAA-based access control and a service discovery procedure which manipulate access control data. The

standard IEEE 802.1X is applied [14]. In order to guarantee a reliable access control for the two entities (the user and the network), we propose to use a mutual authentication method like e.g. EAP/TLS (Extensible Authentication Protocol/Transport Layer Security) [15,16] for network port access control. For 802.11 networks, this resolves the currently existing flaws in the provided WEP-based (Wired Equivalent Privacy) shared key authentication. The needed architecture consists of at least one central EAP/TLS-capable RADIUS-server and several RADIUS [17] and 802.1X capable APs. In a first phase the user connects to the network which it discovers by means standardized in IEEE 802.11. The access control is carried out by the access point which blocks any access of the user until the AAA server allows the opening of the port. The AP opens the associated communication port, creates the dynamic WEP keys and sends them to the terminal signed and encrypted by the session key. The received WEP-keys are installed in the network adapter and the WEP encryption is activated on the link. Once the port is opened, UPnP is used between the network and the user to discover services. In order to minimize the number of messages for discovery purposes related to each connection/disconnection, we introduce an additional logical entity which gathers information on the available services. These information can be static (e.g. configuration) or gathered gradually by the use of UPnP between the network services and this new entity. This logical entity is typically physically installed on the AP.

In a preliminary phase (see Figure 3) host&CP UPnP gathers information on all available services in the network (network services). To be identified by the server AAA (AAA server), the user follows the methods defined in standards IEEE 802.1X (EAPOL) and EAP/TLS. If the connection is accepted by the AAA server and the EAP/TLS user client, a 802.11 link is established through the access point with certain properties found in the user profile (session delay, maximum bandwidth, etc.). The user can execute his UPnP control point (UPnP CP) and thus contacts host & CP UPnP. This latter requests the AAA database which contains all the open sessions to find the identity of the respective user. Host & CP UPnP checks the user profile and thus obtains a list of personalized services the user is authorized to use. It then merges this list with its local list of available services and transfers the result to the user in its response. Then, Host & CP UPnP informs the user of any change in its service base by using UPnP notifications.

We used the open source Intel UPnP implementation and Software development kit (SDK) for Linux [18]. We validated the integration of access control and service discovery architectures in a local domain. The platform is operational. Performance measurements study will be carried out to evaluate the required delays for service discovery and service negotiation by considering scalability and user roaming through several remote networks.

Besides, service discovery mechanisms depend heavily on the adaptation offered in all the networks which is mainly based on the context definition.

Context-awareness is a characteristic that becomes important in the case of cooperation between networks. It can be defined as the capacity of a system to discover and use contextual information such as the localization of the user, the date and the

hour, the proximity of other users and devices, the possibilities of connection to one or more networks, the available bandwidth, etc. These data intervene in the choice of the network or the execution of network services as well as application services. The modeling of a context can be based on the policies. The model of information of context containing policies is designed starting from a model of the IETF called PCIM (Policy Core Information Model) and of its extensions. The concept of context corresponds to several points of views including user context, peripheral context, network context and application context.

The architecture that handles adaptation and cooperation structure that we suggest within the framework of RESACO will be based on COPS architecture deployed for QoS management.

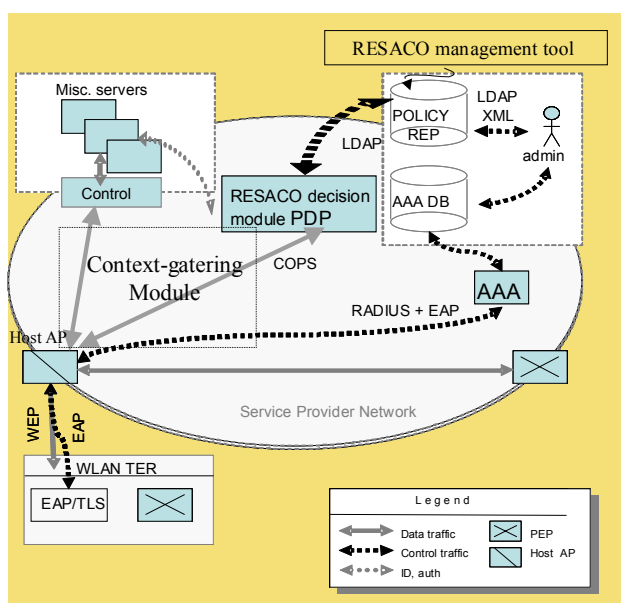


Figure 4: Context-based adaptation RESACO architecture

As illustrated on Figure 4, in the case of a local network with a PDP and several PEPs, the context management system architecture is composed of four entities: policy management tool, policy repository, PDP and PEPs. In order to make access points programmable, intelligent and active, we install a PEP in each access point which includes a module of collection of information related to the contexts cited above. Thus, we offer a dynamic adaptation to a complex environment's changes following the policies that will be defined. Those will be based on the contract signed between the service provider and the user as well as on the rules established by the administrator of the network.

6. CONCLUSION

The objective of the RESACO project is to explore, analyze and experiment with different scenarios for open, cooperative and adaptive networks in the field of mobile and wireless networks. The project partners have already set up different platforms. Ongoing experiments are dealing with resource

allocation, QoS, service discovery and security aspects. Integration actions are currently taking place and some promising results motivate future extensions that will consider mobility management as well as service discovery features and associated end-to-end QoS guarantees.

REFERENCES

- [1] J. Boyle, et al, "The COPS (Common Open Policy Service) Protocol", RFC 2748, IETF, Jan. 2000.
- [2] D. C. Verma, "Policy-Based Networking Architecture and Algorithms", New Riders Publishing, (Indianapolis, Indiana), Nov. 2000.
- [3] D. Decasper, Z. Dittia, G. Parulkar and B. Plattner; "Router Plugins: "A Software Architecture for Next Generation Routers"; Proc. ACM SIGCOMM 1998.
- [4] XORP: "Extensible Open Router Platform". <http://www.xorp.org/>.
- [5] Y. Gottlieb and L. Peterson, "A comparative study of extensible routers" OpenArch'02, June 2002.
- [6] O.I. Lepe, J. García, "A Performance Model of a PC Based IP Software Router", IEEE ICC 2002, Volume: 2, pp. 1230-1235.
- [7] Benjie Chen and Robert Morris, "Flexible Control of Parallelism in a Multiprocessor PC Router", Proceedings of the 2001 USENIX Annual Technical Conference (USENIX '01), pages 333 - 346, June, 2001.
- [8] R. Dantu, T. Anderson, R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework", work in progress, IETF draft; January 2004.
- [9] E. Kohler, R. Morris, B. Chen, J. Jannotti, and M. F. Kaashoek. "The Click modular router". ACM Transactions on Computer Systems, 18(3): 263-297, Aug. 2000.
- [10] "Network Processing Forum", <http://www.npforum.org/>
- [11] Calhoun P., Loughney J., Guttman E., Zorn G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.
- [12] Neilson R., Wheeler J., Reichmeyer F., Hares S.: "A Discussion of Bandwidth Broker Requirements for Internet2 Qbone Deployment. Internet2 Qbone", BB advisory Council, August 1999.
- [13] <http://www.upnp.org>, UPnP Forum, UPnP Device Architecture, http://www.upnp.org/download/UPnPDA10_20000613.htm.
- [14] L.M.S.C of the IEEE Computer Society, "Port-Based Network Access Control", IEEE Standard 802.1X, June 2001.
- [15] Blunk, L., Vollbrecht, J., "Extensible Authentication Protocol (EAP)", RFC 2284, IETF, March 1998.
- [16] Aboba, B., Simon, D., "EAP/TLS Authentication Protocol", RFC 2716, IETF, October 1999.
- [17] Rigney, C., Willens, S., Rubens, A., Simpson W., "Remote Authentication Dial-In User Service (RADIUS)", RFC 2865, IETF, June 2000.
- [18] www.intel.com/labs/connectivity/upnp/index.htm