A Combination of Signalling Protocols for Future Internet Generation

Rima Tfaily Souayed, Dominique Gaïti, Guy Pujolle

A COMBINATION OF SIGNALLING PROTOCOLS FOR FUTURE INTERNET GENERATION

Rima Tfaily Souayed[1], Dominique Gaiti [2], Guy Pujolle [3]

[1] *LM2S, Université de technologies de Troyes (UTT)*
12 rue Marie Curie, BP 2060 - 10010 TROYES, France
Rima.Tfaily@utt.fr
Telephone: + 33 3 25 71 56 25
Fax: + 33 3 25 71 56 99

[2] *LM2S, UTT &LIP6, université Paris 6*
8 Rue du Capitaine Scott, 75015 Paris, France
Dominique.Gaiti@utt.fr

[3] *LIP6, Université pierre et Marie Curie – LIP6*
Guy.Pujolle@lip6.fr

Abstract:

The signalling in IP networks, particularly signalling the quality of service (QoS), has been a hot topic for many years and a lot of work has been done on end- to-end QoS signalling. The most important work remains the Resource ReServation Protocol (RSVP), developed by the Internet Engineering Task Force (IETF). RSVP, however, suffers from scalability problem in core networks. Other protocols face inter-working difficulties among domains in which different QoS solutions are deployed. Given the above, a new IETF work group (WG) termed Next Steps in Signalling (NSIS) WG was launched and is supposed to work on the requirements, architecture and protocols signalling purposes in future Internet generation. In this paper, we study some existing protocols and their infrastructures and how they can interoperate with a simplified solution for signalling in IP networks. We also propose an architecture upon which these protocols are to function.

Key words: Signalling protocols, NSIS protocol, AAA protocols, SIP protocol, and policy-based management protocols.

1. Introduction

Future Internet generation have the challenge of satisfying both end-users and network-operators. The challenge consists of providing the QoS at a high security level, while controlling and managing the mobility in a network in addition to offering an Authentication, Authorization, and Accounting (AAA) services as well as a robust and dynamic control over networks. Providing services such as QoS necessitates some signalling to describe the required service level and then reserve the corresponding resources by using the deployed resource reservation mechanisms in a network [Bru 02]. The most known QoS signalling protocol is the Resource ReServation Protocol (RSVP) [Bra 97], which serves as a starting point to determine the requirements for the simplified solution of signalling which inherited its name from "Next Steps in Signalling" (NSIS) work group (WG). We have to note, however, that a new signalling protocol should use existing QoS technologies whenever it is possible [Bru 02] [Fre 02].

Security is a very important issue in networks especially when it concerns reserving scarce resources and charging for the service(s). Users' requests for higher quality of service than that negotiated in their Service Level Agreements (SLAs) must be rejected and malicious users' capability of modifying accounting information should be rendered impossible. Evidently, users should be charged according to what they have requested and consumed in terms of QoS and resources. So, there is a need to interoperate the new signalling protocol with AAA protocols such as Diameter and Radius [Fre 02].

To offer quality of service and AAA services, it is mandatory for network administrators to regulate who has access to a given set of resources and services under certain conditions [Ren 01]. Nowadays, networks are larger and their devices are more and more complex. Therefore, deployment of the services mentioned above is critically

dependent on the use of a policy-based infrastructure that allows Internet service providers (ISPs) and consequently their administrators to regulate their network rather than configuring individual devices [Raj 99]. A policy infrastructure allows ISP intentions to be translated into differential packet treatment of network packet flows. Two well known protocols, Simple Network Management Protocol (SNMP) and Common Open Policy Service (COPS), are used for this purpose.

In this paper, first we explain briefly the policy based networking and the AAA infrastructures including the AAA services and the general NSIS framework proposed by the NSIS WG. Second, we offer a review as well as analysis of protocols mentioned above to choose the most appropriate protocols that interoperate each other with the new signalling protocol to be designed. Third, we provide some assumptions concerning this signalling protocol and propose an architecture upon which these protocols are to function. Finally, we present a conclusion of this paper and state some related perspectives.

2. Policy- based networking infrastructure

Nowadays, network-operators control their networks via policies. What are these policies? And which network is called policy- based? Policies denote the unified regulations of access to network resources and services based on administrative criteria [Raj 99]. These regulations might be expressed and implemented at different levels. The network view (figure 1) is composed of different nodal views that correspond to policy objectives at various nodes. The nodal view, in turn, is composed of policy rules that are considered as atomic instructions through which various nodes are controlled. So, a policy- based networking (figure 2) is any network managed via a common set of policy definitions. Its

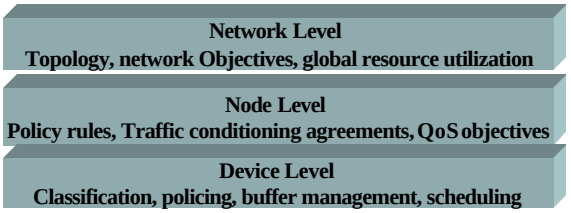

Figure 1: A Conceptual Hierarchy of Policies

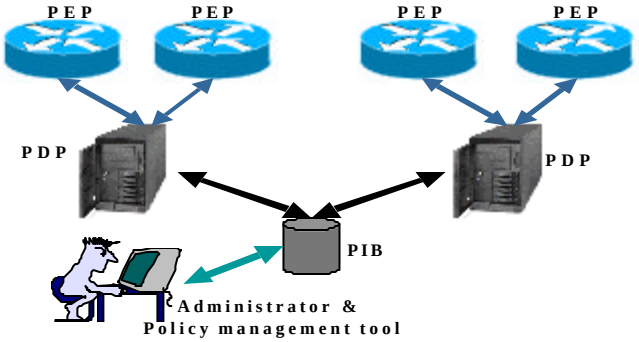

Figure 2: A policy-based Networking

management components are: a policy server(s) also called Policy Decision Point (PDP) that makes policy decisions, network nodes (PEP[1]s) that enforce policy actions, a policy repository (PR) where policies are stored and retrieved to help PDP making its decision, and a policy management tool that enables the administrator to enter the intended policies [Raj 99].

3. Authentication Authorization Accounting (AAA) infrastructure and services

The deployment of resource reservation mechanisms forces network operators to use an AAA system in order to verify users' claimed identity, determine their access rights before granting network access for them, collect information on their resource usage, calculate the corresponding price and provide fine-grained set of details for billing [Laa 00]. The AAA system is also needed to avoid fraudulent use of QoS and to manage service level agreements (SLAs) among operators. This system is also based on policies to manage AAA services but it has some problems[2] that have led us to adopt a generic AAA architecture [Ren 01] that is compatible with that of policy based described above.

4. NSIS Framework structure

[1] Policy Enforcement Point
[2] Explaining these problems is outside this paper scope

NSIS protocol, being designed, has two independent layers, an application signalling layer and a common transport signalling layer. Its WG has determined an overall framework structure [Fre 02], where we could identify three entities (figure 3): NSIS Initiator (NI), NSIS Forwarder (NF) and NSIS Responder (NR). NI entity is responsible for initiating a signalling request to reserve network resources. This signalling may be triggered by a user application, a network management entity, or other protocols. It is intercepted by NF, which- in turn- interacts with the local resource management function (RMF), and then forwards it to the next NSIS node. Reaching the NR, the signalling might interact with applications located in that node before signalling is terminated.

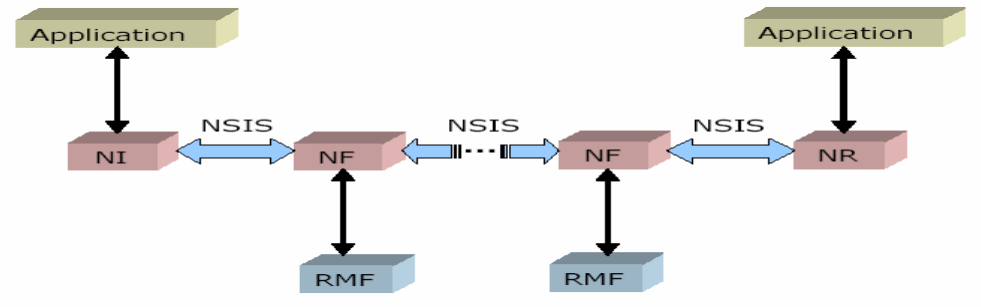

Figure 3: Basic NSIS Framework

5. Existing protocols analysis

RSVP [Bra 97] serves as a signalling protocol for applications requesting resource reservation. It is used in the Integrated Services (IntServ) approach which is a per-flow based QoS framework. RSVP negotiates an end-to-end reservation between the sender and the receiver and adopts a receiver-initiated reservation style designed for multicast environments and accommodates heterogeneous receiver service needs. RSVP is a robust protocol and allows IntServ to deliver fine-grained QoS guarantees. However, it suffers from two problems [Zho 00]. First, the fine granularity of micro- flows implies a significant routing load. Moreover, the management and maintenance of a large number of states in nodes increase flow setup time and message overhead. Second, whenever the number of flows is huge, particularly in backbone networks, routers become unable to manage these flows and to offer a separate queue for each one. This management of micro flows constitutes a considerable obstacle in term of scalability and cannot be tolerated in core networks.

RSVP includes much more functionality and complexity than it is required in some IP networks. In fact, the QoS problem, in such networks, is significantly simpler to solve. The trade-off between performance and functionality is one of the key issues here. In addition, the QoS sensitive applications do not use RSVP multicast capabilities [De M 02]. For these reasons, RSVP usage, in our framework, is limited to local access networks.

Session Initiation Protocol (SIP) is an application level control protocol [Ros 02] developed in IETF. It is used for setting up, modifying and terminating multimedia sessions and for making Internet telephony calls between two or more parties. It runs over both transport protocols: the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Studies on using Stream Control Transfer Protocol (SCTP) as the transport protocol for SIP have emerged. SIP follows the client-server paradigm. SIP system has two types of network components: user agents and network servers. User agents are end systems that initiate and accept sessions on behalf of users, while network servers provide call routing, service location and supplementary services such as redirection.

SIP is widely used by backbone providers due to its simplicity. However, it supports neither QoS services nor mobility services [Pan 98]. Hence, SIP needs to inter-operate with other protocols that support these services and exchange accounting information about user resource usage.

Radius was designed in the mid nineties to provide AAA services for dial up point to point protocol (PPP) and terminal access servers [Rig 97]. It carries authentication and authorization information between a Network Access Server (NAS), which desires to authenticate its links, and an Authentication Server. The NAS, which is a client of Radius, sends an access request to a given Radius server which would authenticate the user and return information to its client about delivering services for the Dial-in-user.

As routers and Network Access Servers have increased in complexity and density, Radius has become less useful in such large networks. The need arises for a more powerful protocol that effectively handles the problems

encountered in Radius. **Diameter** [Cal 02] is proposed by the AAA WG as an alternative to radius. Although Diameter does not use the same Protocol Data Unit (PDU) as Radius, it could sufficiently borrow from it in order to guarantee a backward compatibility. The idea is to create a Base Protocol that could be extended to allow new access methods. Diameter consists of two parts [Cal 02]: a Base Protocol and different extensions and applications. The Base Protocol is intended to provide an AAA framework for mobile hosts, NASs and roaming operations to be used by all Diameter applications. Diameter application part defines application specific functions and data units each of which is specified separately. This protocol has so far three applications [Cal 01]: NASREQ, Mobile IP and Cryptographic Message Syntax (CMS) security application which is closely connected to the Base Protocol in order to provide security to all applications. Diameter Base Protocol runs on both transport protocols: TCP and SCTP (Stream Control Transmission Protocol). SCTP is more enhanced due to the connection oriented relationship that exists among Diameter peers. It is capable of categorizing several independent streams to a single SCTP association instead of keeping all streams as independent TCP connections. Diameter connections are secured by IP Security (IPSec) and/or Transport Layer Security (TLS). It is a peer- to - peer protocol; any Diameter node could initiate a request and Diameter messages are routed according to the Network Access Identifier (NAI) of a particular user.

Diameter is proposed by the AAA WG as the next generation AAA protocol [Ren 01]. It is still under development and testing, but some codes are downloadable from the Internet. Unlike Radius, Diameter is used for larger networks because of its capacity to handle 2^32 requests simultaneously [Eks 00] [Mit 01]. Since it supports backward capabilities with Radius, Diameter agents are capable of acting as Radius gateways, i.e., sending Radius messages through the network without the need for any conversion. Unlike radius, Diameter does not require a shared secret among communicated peers. Its AVPs are protected by using Cryptographic Message syntax. Many mechanisms and algorithms are supported with CMS application, such as Hashing, Content Encryption, etc. Diameter is integrated with mobile IP to allow roaming for wireless network and it is designed to provide AAA framework for mobile-IP application, NAS REQuirements (NASREQ) application and ROAMing Operations (ROAMOPS) [Cal 02]. Moreover, Diameter server could send unsolicited requests and appears suitable for exchanging policies among domains. Its disadvantage is that the transport protocol over which it runs, i.e., SCTP, is not so far widely used.

COPS [Dur 00] is a request/response protocol between a PEP (policy enforcement point) and a PDP (policy decision point) for exchanging policy information and conveying decisions made by PDP (figure 6). In this client/server model, PEP sends requests to its PDP which, in turn, sends decisions back to the PEP. Upon receiving PEP requests, the policy server stores request states until they are explicitly deleted by the PEP whenever they are no longer applicable [Dur 00]. This storage allows PDP to generate, at any time, asynchronous decisions for a currently installed request state. COPS runs over TCP to assure reliable exchange of messages. It is designed to be scalable and extensible. It could support diverse PEP specific information without requiring modifications to the Base Protocol. Like Diameter, COPS relies on CMS objects to provide security and does not require any key to be distributed offline. CMS supports "Key exchanged capability" to exchange keys. COPS provides message level security for authentication, replay protection and message integrity [Eks 00] [Mit 01]. It could also reuse existing protocols such as IPSEC or TLS for security in order to authenticate and secure the channel between the PEP and the PDP.

COPS [Dur 00] is used in the market only as a policy based management protocol. It is considered acceptable as an AAA protocol according to the requirements defined in the AAA WG [Eks 00] [Mit 01]. Therefore, additions are made [Ren 01] to extend it from the client/server model to a proxy -based model supporting AAA. In our framework, we use COPS for Provisioning (COPS-PR) [Cha 01]. In addition, an extension of COPS with new client type is to be defined to assure the communication between the policy server, which is acting as NF, and the RMF entity.

SNMP [Cas 90] is a standardized protocol, designed by the IETF and used in network management. It allows the communication of management information among agents located in the network elements and a network management station, i.e., a network control center. The management information is stored in management information Base (MIB). SNMP is basically a connectionless protocol that runs over (UDP) but, now, it also runs over TCP. SNMP latest version[Cas 99] [Nat 00], SNMPV3, supports new SNMP message formats and provides more security mechanisms for messages as well as access control and remote configuration of SNMP parameters. It is also characterized by its modularity. It adopts some software engineering techniques that allow architecture scalability.

Lately, the IETF "Configuration Management with SNMP (SNMPConf)" working group studied whether SNMP could be used for policy-based configuration management [Mac 02]. Its goal was to provide a SNMP framework for both policy-based configuration management and monitoring of network. This work group believed that the SNMP framework could provide all the necessary capabilities required for configuration and monitoring. The main advantage of this approach is that traditional configuration methods could be used in combination with more powerful policy-based configuration operations. Using objects with the same name space for configuration as well as for monitoring

would facilitate error detection and recovery processes. Despite the efforts that were done to overcome SNMP disadvantages, we could not choose SNMP as a protocol for policy based management networks for many reasons. First, a MIB must still be used with SNMP over UDP along with SNMP over TCP [Mcc 99] [San 99]. As a result, the disadvantage of using a UDP would remain. Second, SNMP was successfully deployed because of its simplicity. The efforts to increase its functionalities increased also its degree of complexity. So, its stability might have been altered.

In summary, RSVP has a scalability problem [Zho 00]. Radius [Mit 01] and Diameter [Cal 02] [Cal 01] are exclusively security oriented. SIP is simple but presents adaptability difficulties in managing quality of service and mobility [Pan 98]. SNMP is successful in monitoring, but it lacks high level configuration management [McC 99]. COPS is QoS dedicated. Yet, it is open for new functionalities. As a result, none of these protocols is capable by itself of providing a secure connection, managing the QoS and the mobility and offering AAA services. There is a need to enhance some protocol functionality, make possible their interoperability and suggest or design, if necessary, a new protocol capable of doing certain functions that other protocols are not capable of.

6. Solution: architecture and interoperability among protocols

As we explained before, our objective is to unify existing incompatible signalling protocols or at least to make possible their coexistence. At the beginning, we preferred having multiple signalling protocols; each tailored to perform well its specific task instead of having a single complex protocol to perform all tasks. Yet, it is also important to avoid extremities because splitting up tasks too much complicates the interaction among the different signalling protocols. Below, we propose an architecture upon which these protocols are to function and state its assumptions.

6.1. Some assumptions and mode of operations

Our work is mainly an end-to-edge. The new signalling protocol is initiated by an end host (respectively edge node) and is terminated by an edge node (respectively end host) of a domain. Initiation and termination by core nodes are also included. We concentrate on an out-of-bound signalling in core network, i.e., the core network configuration split between signalling and data paths. In this case, signalling messages are routed through nodes which might not be in the data path. So, in end-to-edge approach, an edge node might be a proxy located on an off- path. Nothing prohibits using both in-bound and out-of-bound approaches in core networks.

In the new signalling, a sender-initiated signalling approach is used. In this approach, the sender of the data flow initiates and maintains the resource reservation used for that flow. Therefore, acknowledgements and notifications could be securely delivered to the sending node. Unlike RSVP, nodes do not have to maintain backward routing states. In a sender-initiated approach, a mobile node can initiate a reservation of its incoming flows as soon as it moves to another roaming sub-network. Otherwise, i.e., in a receiver- initiated signalling approach, a mobile node has to inform the receiver about its handover procedure for allowing it to initiate a reservation.

The new signalling protocol should be used to set up both type of resource reservation, unidirectional and bidirectional. Unidirectional resource reservation is required for media stream with no feedback, while bidirectional one is required for voice-call flow. The latter is more advantageous for mobile nodes compared to the unidirectional. In case two communicated mobile nodes change their access points, the signalling procedure, after handover, might be more efficient [Fre 02]. Using Multicast, as in RSVP, would violate the simplicity objective of the signalling protocol. As a result, this signalling would support unicast only. Other assumptions such as “Addressing” will be determined in the near future as we progress in our work. In fact, signalling messages could be addressed directly to the destination or to a closer node by neighboring signalling aware entity [Fre 02].

6.2. Framework components

Figure 4 presents a simplified “next network generation”. It is composed of an access network, which makes its own decisions concerning the QoS provisioning and a single core domain, which our work is concentrated in. In figure 4, we distinguish some important entities: an access network edge node, core network edge nodes, a QoS policy server, a Security server/AAA server, a SIP proxy, a RMF entity and a Monitoring Function entity. The nodes implement the signalling protocol with different degree of complexity depending on the location of the node i.e., edge node, interior node, etc.

In the next generation of core networks, each domain is expected to have at least two policy servers acting as a QoS policy server and a Diameter server/ AAA server. Having one policy server that acts as a QOS policy server and as

an AAA server at the same time could be a possibility. Other servers would be alternative servers. These policy servers are also NFs (Network Forwarders)[1]. Each node, i.e., router, in turn, should act simultaneously as PEP and as a Diameter client, whereas SIP proxy and other proxies should implement the signalling protocol and be diameter clients.

At boot-up time, servers and clients inform each other about the features they support. Each client establishes a connection with its server in order to communicate their capabilities such as the interface types supported. The protocol used between a PDP and its PEPs is COPS, while Diameter is used between an AAA server and its clients. We suggest studying the possibility of running COPS over Stream Control Transmission Protocol (SCTP). In case this is feasible, a node may establish only one connection with the policy server(s). Both types of policies, AAA policies and QoS policies are stored in one (or more) policy repository. Independence is a key feature among these policies. Upon user request performed by service equipment in a NAS, an AAA server requests the corresponding policies from its PR and takes the policy decision of providing the requested service.

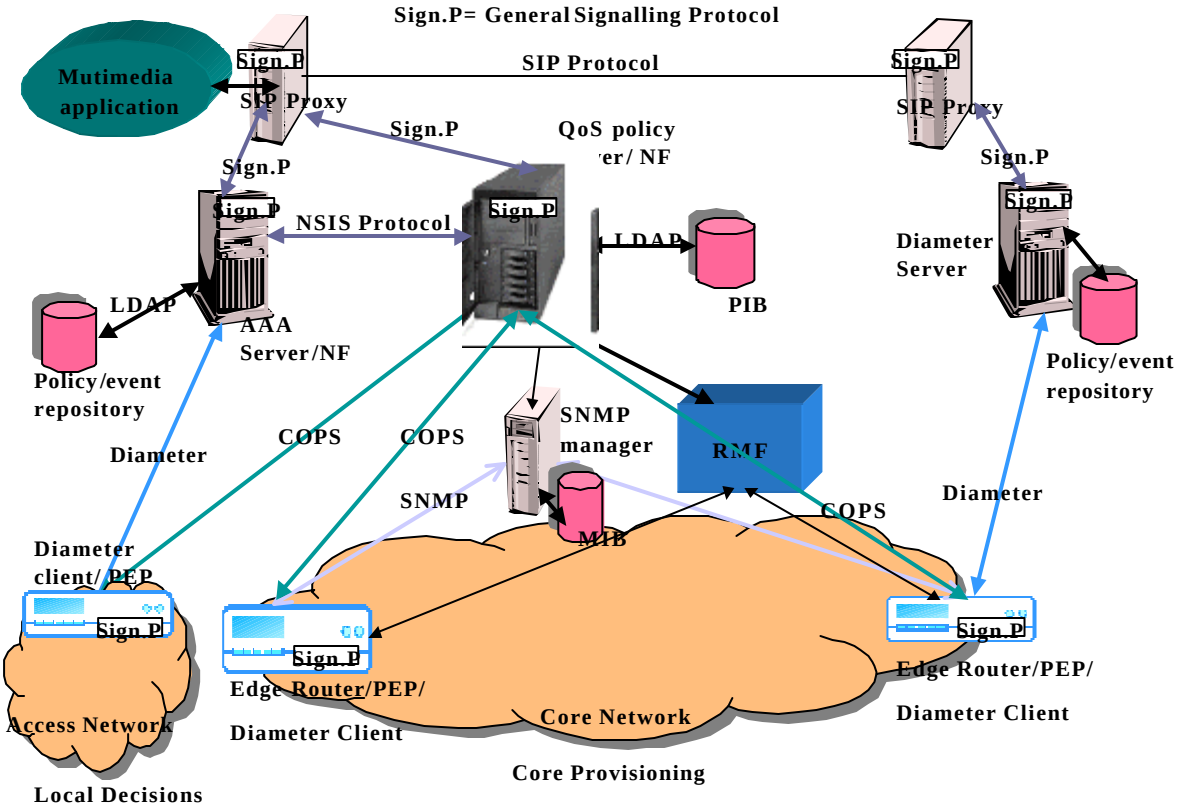

Figure 4: Next generation signalling protocol framework

6.3. Interaction among the signalling protocol and servers (SIP and policy servers)

SIP system does not support user policies and accounting and billing features. It needs to interact with a policy server in order to exchange with it some policy and accounting information. In this case, a SIP server acts as a Diameter client. When a SIP server is being notified to set up a call for a user, it first initiates a Diameter request command to its AAA policy server with all the information about the user. The AAA server, in turn, checks the request against the admission control policy database and returns a Diameter response message. If the response is approved, the caller sends a SIP INVITE message to the called user. After session establishment, the caller must send a notification to the server to start the accounting process. By receiving a termination notification call from the user or a SIP BYE message from the called user, the caller informs its server to stop the accounting.

SIP, as it is used by backbone operators, is not capable of requesting QoS. By implementing the signalling protocol, SIP can request a service quality. When a SIP server receives a user inquiry for establishing a multimedia

[1] See the Overall NSIS framework paragraph

session, it formulates a request to the QoS policy server. This request may be conveyed via the signalling protocol (see figure 5). As SIP interacts with Diameter, the QoS policy server checks SIP request against its admission control policy database and sends back a response message. In order to minimize session setup time, a SIP server must contact the two policy servers simultaneously (figures 4, 5). These policy servers should negotiate before generating a coherent response(s). In case a QoS request for a given user is rejected, the AAA server should be notified. The AAA server should also be notified about the agreed QoS level for a given user. The two policy servers could communicate via signalling protocol messages.

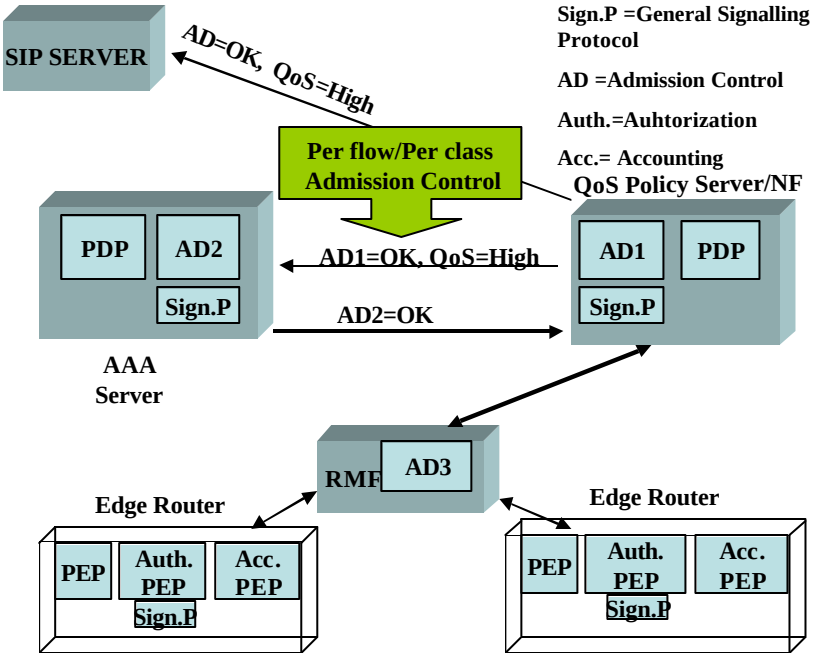

Figure 5: Policy servers' communication

6.4. Signalling protocol interaction with the Resource Management Function

The signalling protocol serves to convey signalling information. It is not involved in reserving resources. Yet, it interacts with resource reservation mechanisms. The RMF entity is charged with resource provisioning according to user SLSs, providing feedback information to the NF about resource availability, topology, configuration, etc. It could, via monitoring capabilities, detect and notify the NF about a SLS violation. The RMF entity helps admission control entity of the QoS policy server to take a decision about accepting or rejecting a given user request at a given time. This admission is per- flow. It may be also per- class, i.e., per- class of service. The NF-RMF interface should allow the negotiation of dynamic SLS parameters. Such negotiation will lead to reconfigure some nodes. The negotiation protocol used for this interface will most probably be an extension of COPS. Finally, standardizing the future Internet generation protocol implies also the standardization of both the SLS parameters and the NF- RMF interface.

6.5. QoS technology in core networks

One of the main objectives is to use the existing QoS technologies whenever possible. As DiffServ is being implemented by most operators, we suggest using it in the future core networks. It is important to keep in mind that DiffServ needs, like other existed IP solutions [De M 02], some improvements. We believe that DiffServ needs a simple signalling protocol and it might benefit from the one being designed.

7. Conclusion and perspectives

In this paper, we analyzed the existing signalling protocols (such as RSVP) and policy-based management protocols (such as COPS and Diameter). We chose the most appropriate protocols with which the signalling protocol needs to interoperate for maintaining simplicity, scalability, and speed. We investigated thoroughly one part of the solution to signalling information. The solution is composed of protocols for core networks: COPS for provisioning the QoS, Diameter for accounting, SNMP for monitoring, RSVP for local access networks, SIP (placed at edges of access networks) for multimedia session and a protocol for signalling QoS and non QoS information. We also proposed an architecture upon which the above protocols are to function. Such architecture allows a separation between resource provisioning as well as management on one hand and resource reservation signalling as well as admission control on the other hand. The above framework along with its protocols will provide a certain level of security for connections as well as delivering AAA services in addition to providing a relatively good quality of service and dynamic control of networks.

However, for our design to fully function, the operators need to adopt and deploy it. To help doing so, standardisation of the signalled QoS parameters and the interface between the Resource Management Function and the Network Forwarder should be accomplished. Once these requirements are achieved, signalling and providing end-to-end QoS would be easier. Upon accomplishing the signalling protocol structure, an optimization work will follow in order to maintain simplicity, scalability, and fast signalling in addition to avoiding function redundancy especially in core networks. We will try to extend and enhance COPS functionalities due to its extensibility feature and to study the interaction between resource signalling and mobility protocols, during path updating.

8. References:

[Bra 97] Braden R. et al.: Resource ReServation Protocol (RSVP); IETF RFC 2205, September 1997.

[Bru 02] Brunner M.: Requirements for QoS Signaling Protocols; IETF, Internet Draft, work in progress, draft-ietf-nsis-req-02.txt, May 2002.

[Cal 02] Calhoun Pat R. et al.: Diameter Base Protocol; IETF, Internet Draft, work in progress, draft-ietf-aaa-diameter-11.txt, June 2002.

[Cal 01] Calhoun Pat R. et al.: Diameter Framework Document; IETF, Internet Draft, draft-ietf-aaa-diameter-framework-01.txt, March 2001.

[Cas 99] Case J. et al.: Introduction to version 3 of the Internet- standard Network Management Framework; IETF RFC 2570, April 1999.

[Cas 90] Case J. et al.: A Simple Network Management Protocol (SNMP); IETF RFC 1157, May 1990.

[Cha 01] Chan K. et al.: COPS Usage for Policy Provisioning (COPS-PR); IETF RFC 3084, March 2001.

[De M 02] De Meer H. et al.: Analysis of Existing QoS Solutions; IETF, Internet Draft, work in progress, draft-demeer-nsis-analysis-02.txt, June 2002.

[Dur 00] Durham D. et al.: The COPS (Common Open Policy Service) Protocol; IETF RFC 2748, January 2000.

[Eks 00] Ekstein R. et al.: AAA protocols: Comparison between Radius, Diameter and COPS; IETF, Internet Draft, draft-ekstein-aaa-protcomp-00.txt, April 2000.

[Fre 02] Freytsis I. et al.: Next Step in Signaling: Framework; IETF, Internet Draft, work in progress, draft-ietf-nsis-fw-00.txt, October 2002.

[Laa 00] Laat C. et al.: Generic AAA Architecture; IETF RFC 2903, August 2000.

[Mac 02] Macfaden M. et al.: Configuration Networks and Devices with SNMP; IETF SNMPCONF WG, Internet Draft, draft-ietf-snmpconf-bcp-09.txt, June 2002.

[McC 99] McCloghrie K. et al.: A Comparison of Policy Provisioning Protocols; IETF, Internet Draft, draft-Kzm-policy-protcomp-00.txt, October 1999.

[Mit 01] Mitton D. et al.: Authentication, Authorization, and Accounting: Protocol Evaluation; IETF RFC 3127, June 2001.

[Nat 00] Natale B.: Comparison of SNMPV3 against AAA Network Access Requirements; IETF, Internet Draft, draft-natale-aaa-snmpv3-comp-00.txt, June 2000.

[Pan 98] Pan P. et al.: Diameter: Policy and Accounting Extension for SIP; IETF, Internet Draft, draft-pan-diameter-sip-01.txt, November 1998.

[Raj 99] Rajan R. et al.: A policy Framework for Integrated and Differentiated Services in the Internet; IEEE Network, September/October 1999.

[Ren 01] Rensing C. et al.: A survey on AAA Mechanisms, Protocols, and Architectures and a policy-based Approach beyond: A^x; ETH-E-Collection, http://e-collection.ethbib.ethz.ch, 2001.

[Rig 97] Rigney C. et al.: Remote Authentication Dial-In User Service (RADIUS); IEFT, RFC 2138, April 1997.

[Ros 02] Rosenberg J. et al.: SIP: Session Initiation Protocol; IETF RFC 3261, June 2002.

[San 99] Sanchez L. et al.: Evaluation of COPS/PIB and SNMP/MIB Approaches for Configuration Management of IP-based Networks, IETF, Internet Draft, draft-ops-mumble-cong_management-03.txt, October 1999.

[Zho 00] Zhoa W. et al.: Internet Quality of Service: an Overview; http://citeseer.nj.nec.com/zhao00internal.html, February 2000.