Analysis of SIP, RSVP and COPS Interoperability

Csaba Király, Zsolt Pándi, Tien Van Do

Department of Telecommunications, Budapest University of Technology and Economics,
Pf. 91., 1521 Budapest, Hungary
{cskiraly, pandi, do}@hit.bme.hu
http://www.hit.bme.hu/

Abstract. The All-IP network concept with end-to-end QoS provisioning has received particular attention in 3GPP recently. The UMTS proposals, however, have not yet solved some protocol interoperability issues. This paper analyzes the IP Multimedia Subsystem from the aspect of call control, resource reservation and network policing interoperability from the viewpoint of implementations. More specifically, the experiences based on a prototype implementation of the IMS based on SIP, RSVP and COPS are analyzed and conclusions are drawn to support the standardization process, as well as future implementations. The considered architecture is general and can be applied also to fixed IP networks.

1 Introduction

Mobile communications, as well as mobile telephony, is one of the hottest areas in the networking world. The number of mobile users has grown steadily throughout the recent years, which indicates the global success of second generation mobile networks such as GSM, CDMA and TDMA. The future of mobile communications is just being defined in the framework of the 3rd Generation Partnership Project (3GPP) which organizes worldwide research on the wireless standardization. The standardization of the radio access network of Universal Mobile Telecommunications System has already been finished, but that of the core network is still in progress. In the evolving standards some trends can be perceived, which represent the intentions of the standardization body [1], [2].

At the present 3GPP is aiming at the All-IP network concept as a final target. However, one of the most serious issues that still need to be resolved is the end-to-end QoS (Quality of Service) provision. To provide QoS an appropriate networking technology must be selected with appropriate signaling protocols and mechanisms which implement the following major functions: call control, QoS architecture for resource reservation and network policing.

3GPP standards regarding the IP Multimedia Subsystem (IMS) [1], [2] define an architecture which consists of the following components.

Firstly, for call control and signaling the Session Initiation Protocol (SIP) is proposed. SIP is used in various multimedia services and originates from the IP world, that is, it incorporates concepts and design patterns characteristic of well-known protocols applied in the Internet, such as the Hypertext Transfer Protocol (HTTP) [3]. Recently the role of SIP has gained strength due to its flexibility and scalability. This protocol could be a means of implementing the Intelligent Network concept and is certainly an important step towards NGNs [4].

Secondly, as far as QoS architecture for resource reservation is regarded, the Internet Engineering Task Force (IETF) has elaborated two fundamental service architectures for QoS provisioning in IP networks: the Integrated Services (IntServ) architecture and the Differentiated Services (DiffServ) architecture ([5], [6] and [7]). DiffServ provides QoS for aggregate flows; therefore, it is primarily intended for use in the core network domain due to its scalability. On the other hand, the flow based IntServ provides QoS for each flow on a separate basis through the Resource Reservation Protocol (RSVP) at the expense of higher administrative costs; consequently, it is only suitable for the access network domain. The interworking of the two architectures has already been demonstrated by for example the ELISA and MQOS projects [8]; moreover, IETF recommendations also exist [9]. 3GPP standards propose the use of both architectures.

Finally, network policy control is inevitable in QoS provision. This is generally related to authentication, authorization and accounting (AAA), as well as resource management and call admission control. Service requests of users must be either accepted or refused based on several policy rules. Then this decision must be executed and adhered to at the appropriate network devices. The Common Open Policy Service (COPS) is a promising candidate protocol for communication on policy decisions between the so called Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) [10]. It has been defined so that it could be applied with RSVP, as well [11]. 3GPP standards propose COPS for the communication between PDPs and PEPs.

Although the functional components of the IMS and their operation have already been defined to a certain extent, the necessary interoperability of call control, resource reservation and network policing has not yet been covered. Therefore, this paper aims at the analysis of the IMS architecture focusing on service provision and protocol interoperability. To facilitate the analysis a prototype implementation was prepared. Based on the experiences gathered from the implementation important conclusions can be drawn regarding issues that still need further clarification and recommendations can be given to help the standardization process and future implementations. Moreover, as the same problems arise in fixed IP networks, our results can be applied in that context, as well.

Obviously, the implementation of additional functions, such as authentication and accounting is also inevitable for service provision; however, these remain out of the scope of the present paper.

The rest of the paper is organized as follows. Section 2 gives a short overview of the IMS architecture, while Section 3 briefly considers some issues related to the prototype implementation. Section 4 discusses call setup signaling, then Sections 5 and 6 deal with the Policy Control Function and SIP Proxy Server entities, respectively. Section 7 analyzes the requirements for a communication protocol between these two entities and Section 8 concludes the paper.

2 Short Overview of the IMS Architecture

In this section only the most important functional entities of the IMS are covered. For a more detailed description the reader is referred to [12].

A general scenario for the application layer signaling in the IMS architecture is illustrated in Fig. 1. According to [2] the most important functional elements in the IMS are the Gateway GPRS Support Node (GGSN), the Proxy-Call Session Control Function (P-CSCF) and the User Equipment (UE). Within the P-CSCF there are two fundamental functional elements: a local SIP proxy and a Policy Control Function (PCF).

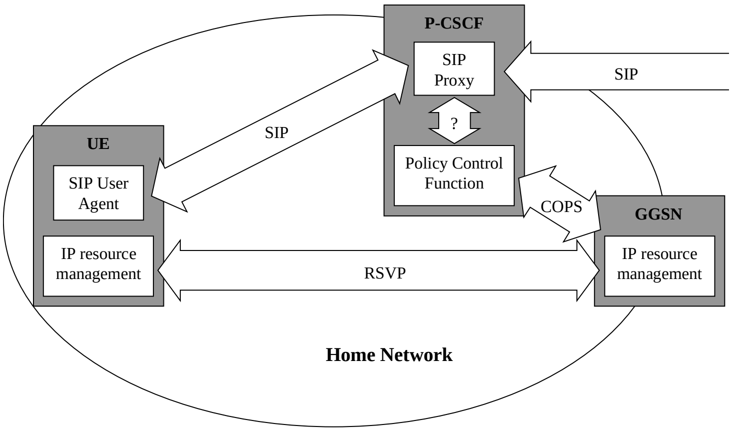

Fig. 1. Application layer signaling scenario in the IMS

[2] discusses several possible scenarios where these functional elements have different capabilities. For example UEs may support RSVP signaling or DiffServ edge functions, but they do not have to have IP bearer service management functionality at all.

Assuming a scenario where UEs are RSVP-capable, that is, RSVP signaling is end-to-end and where GGSNs are not transparent forwarders of RSVP messages (scenario 4 in Annex A of [2]) the components of the architecture must have the following functionality. The *IP resource management function in the UE* is responsible for QoS requests using a suitable protocol (e.g. RSVP), whereas the *IP resource management function in the GGSN* must contain IP policy enforcement and DiffServ edge functionality. The *PCF* in the P-CSCF communicates with the GGSN through the Go interface, which is used for transmitting policing related data and policy decisions between the two entities. COPS is proposed for use in the Go interface. The P-CSCF also contains *SIP Proxy* functionality to be able to track current SIP calls and thus make appropriate policy decisions about resource reservation requests. However, the interface between the local SIP Proxy and the PCF is still undefined in the standard.

3 Adopted Approach: Prototype Implementation

In order to be able to analyze the IMS we had to implement a SIP User Agent (UA), a SIP Proxy, and a COPS Policy Decision Point (PDP) software with the appropriate functionalities listed in Table 1. These requirements were derived from [1] and [2], and will be detailed later on. As the implementation of the GGSN a commercially available and widespread IP router was used.

In the GGSN the DiffServ functionality was not used due to the following reasons. Firstly, in the focus of interest there are the requirements for the Home Network and not the IP cloud beyond the GGSN. Moreover, [8] already demonstrated how RSVP might be used over a DiffServ domain; therefore, from our point of view it is irrelevant whether RSVP or DiffServ marking ensures QoS between GGSNs.

Table 1. Functional elements of the implementation

IMS function	Implementation	Remark
UE	SIP User Agent software	must support end-to-end SIP and RSVP signaling for call control and resource reservation
GGSN	Router	must contain RSVP and COPS PEP functionality
P-CSCF/SIP Proxy	SIP Proxy software	must be able to provide the COPS PDP with session data
P-CSCF/PCF	COPS PDP software	must be capable of making policy decisions based on SIP session information and a priori configuration data

During the software design and development several problems were faced regarding the interoperability issues of the applied protocols. In the rest of the paper these points will be covered. Firstly, we will overview the actions that must be taken during service provision, especially at call setup, as this is the most difficult process in the IMS. Other processes related to QoS provisioning can be handled in a fairly straightforward manner, therefore their discussion will be omitted. After discussing the call setup all the requirements derived from the functionalities listed in Table 1 will be analyzed for each system component that belongs to the service provider, except for the GGSN, as the role of this entity is adequately defined, and its implementation does not entail interoperability issues for the investigated protocols.

4 Call Setup Signaling Scenario

Due to the separation of the bearer and control planes the call setup process is a difficult process with multiple entities, which may fail due to the following reasons:

1. Either the caller or the callee is not authorized to make the call.

2. Either the caller or the callee tries to make an illegal step during call setup, for example issues a reservation request for too much resources.
3. The authorized reservation request fails due to the lack of resources (supposing that QoS assured operation mode is implemented).

Moreover, "ghost rings" must be avoided, that is, the device of the callee must not ring if the call cannot be set up for any reason. Fig. 2 demonstrates a successful call setup process until the phone of the callee begins to ring. Dark (light) background shading marks the RSVP and COPS messages associated with the media stream sent by the caller (callee).

The functional elements interact during call setup as follows:

1. A UE initiates the call setup, the UEs negotiate and agree in the media streams, the set of applicable codecs for each stream and the necessity of QoS with an SDP offer/answer pair [13] in the INVITE and 183 messages[1].
2. Both on the caller and callee side the SIP Proxies forward the SDP information to the PCFs.
3. For both users the appropriate PCF decides whether the user is authorized and which billing category the call belongs to.
4. The RSVP messages sent by UEs for each media stream arrive at the GGSN, which requests a decision using COPS from the PCF. The PCF then examines for each request if the RSVP parameters conform to the parameters negotiated via SDP. If they do, the resource allocation will be permitted, and rejected otherwise.

Finally, the UEs notice the success or failure of their RSVP requests. A request might be rejected by the PCF (due to policy reasons) or CAC at the GGSN (due to the lack of resources). Depending on the result of this preliminary negotiation the call setup may proceed by sending Ringing messages.

At the time when the presented work was in progress the current version of the SIP RFC [14] did not contain any recommendations regarding the integration of resource reservation management in the SIP protocol state machine. Neither work that was under progress in the IETF [15] nor the new proposed standard published recently [16] contained such recommendations. However, the topic was addressed in other IETF drafts [17] and [18], which were being developed continuously. The available draft version at the time of the specification of the architecture recommended the use of COMET and PRACK messages for this purpose. Hence we adhered to these specifications. However, out of these two messages the first was replaced by the UPDATE message used for the same purpose here, while the second one became a proposed standard [19]. Even though the UPDATE message replaced COMET and its function, the analysis of the architecture using COMET will not loose its relevance, as the basic functionality of the two alternatives does not differ.

As far as SDP usage is regarded, we adhered to the SDP offer/answer model of [13] (published later as an RFC [20]) and [18].

---

[1] The offer/answer can also be in 183 and PRACK when media streams are defined by the callee.

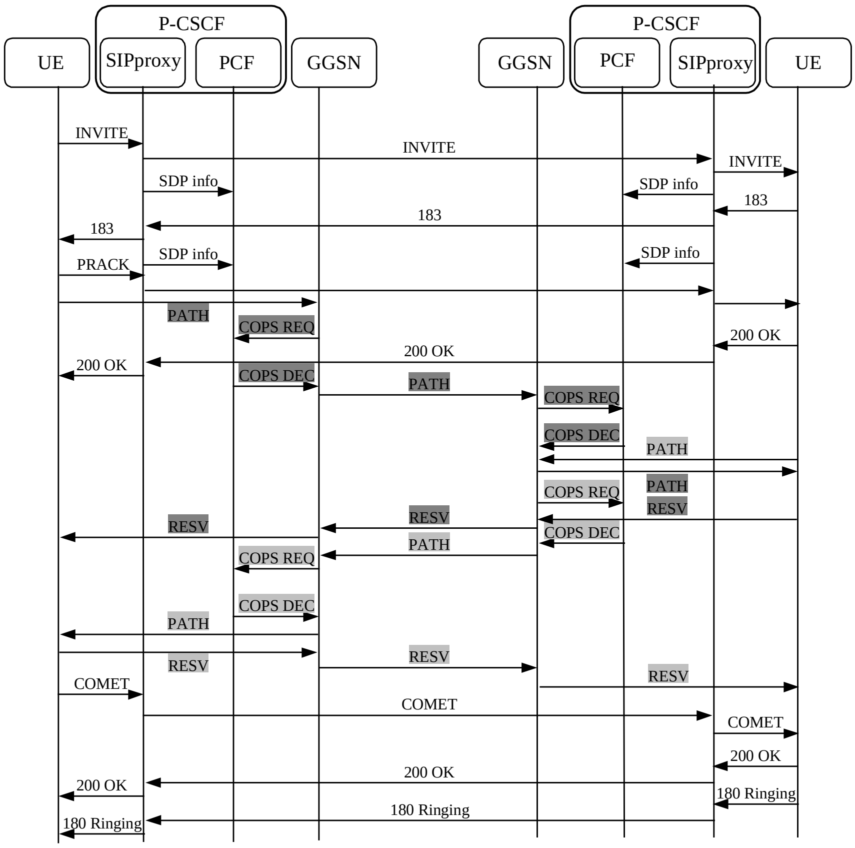

Fig. 2. Message sequence diagram of a successful call setup

5. Policy Control Function

As it was already mentioned, the PCF collects all the necessary call parameters from SIP and RSVP signaling and decides whether the resource reservation request of the user may proceed. For making the policy decision the PCF must use a Policy Information Base (PIB), that contains identification information and service contract details for each user (user profile). Moreover, the PCF must have a predefined set of decision rules, and another database describing resource requirements of different codecs in terms of RSVP parameters.

5.1 Input Information for the Decision

When defining the decision process, the starting point was the fact that the information contained in RSVP messages is insufficient for deciding whether the caller (callee) is authorized for requesting the indicated resources. Transmitting resource management related information in SDP parameters embedded in SIP messages is more conformant to the business model of service providers.

Various pieces of information might be used for authorization and accounting depending on the business model, which leads to a decision mechanism that is far more general and flexible than decision making based only on RSVP parameters. The most important features of a general decision mechanism are as follows:

- integrated management of multiple media streams used in the same session,
- distinction based on the locations of the other party (same network/foreign network),
- distinguished callers or callees (e.g. customer service, emergency calls),
- distinction between different media types (e.g. audio, video, whiteboard),
- distinction between codec performance levels (e.g. high and low quality video conference),
- constraints on the number of simultaneous calls.

It is important to note, however, that although these aspects might be involved in the decision process, some of them imply the conformance of user terminals, which cannot be controlled by the service provider. For example, SDP parameters contain the codec information, but it is not reasonable to check whether user terminals apply one of the negotiated codecs, as this would mean huge additional load for GGSNs. We do not deem the violation of this conformance requirement to be a serious business risk, as this fraud would require the modification of user terminals.

5.2 Decomposition of the Decision Process

The decision process can be decomposed to the following stages:

1. The PCF checks whether the service contract permits the call for the user according to the conditions mentioned above, and determines which billing category the call belongs to.
2. The PCF checks whether the resource reservation request is reasonable based on call parameters.

The first stage can be carried out based on the contents of the SDP offer/answer and the user profile, and a so-called RSVP Envelope can be determined for each direction of each media stream, which describes the maximal allowed resource reservation. When the COPS request arrives later on[2] and the final decision has to be made, this

[2] If the PRACK message carries SDP information, the COPS REQ might arrive at the PCF earlier than the SDP information forwarded by the SIP proxy due to the independence of paths taken by SIP and RSVP messages. In this case, the decision must be postponed until SDP information arrives.

RSVP Envelope, which in fact contains the necessary information in a contracted form, will provide the boundaries for the comparison.

This two-stage process simplifies the definition of decision rules, and, although unsupported by COPS, facilitates pushing decision information to the GGSN, resulting in a reduced call setup time. Even though this two-stage process is not equivalent to a single decision made when all the necessary information is available, it is still flexible enough to support adequate differentiation.

5.3 RSVP Envelopes

Annex C of [2] demonstrates through an example how to determine the amount of resources that the user is allowed to reserve, that is, the RSVP Envelope. This is intended to prohibit unauthorized resource reservations. The envelope may introduce constraints on the following parameters based on the SDP description:

- FilterSpec parameters:
  - source IP address
  - destination IP address
  - protocol ID
  - destination port(s)
- FlowSpec parameters:
  - mean rate (r)
  - peak rate (p)
  - bucket depth (b)
  - minimum policed unit (m)
  - maximum packet size (M)

Determining the IP addresses based on the SDP description guarantees that the reservation can only be accepted between the caller and the callee. Port numbers depend on media type and the applied transport protocol according to [21], and this RFC only requires that they could be determined by an algorithm using the number contained in the SDP parameters. The PCF, therefore, must be aware of these media and transport dependent calculation methods, as well.

FlowSpec parameters can be calculated based on the set of codecs determined by SDP request and answer. The SDP information only describes the set of codecs supported by both parties, not the currently applied codec. In addition to this, the applied codec may be selected arbitrarily from this set, and can be changed during the call; consequently, the envelope must fit all of the indicated codecs. The RSVP parameters necessary for an appropriate reservation can be determined for each codec based on their parameters like frame size and frame duration. From the aspect of implementation it is more straightforward to store RSVP parameters associated with each codec in the PCF database. The envelope can then be calculated by finding the maximum (r, p, b, M) and the minimum (m) of the RSVP parameters associated with the codecs in the set.

This calculation method might significantly overestimate real resource use (consider the case when the set of codecs contains a G.711 and a GSM FR codec, and all users apply the latter), but the user will have no interest in issuing a too large reservation request if it costs more money. However, if accounting is based on the media type (like telephone quality audio) and not on the actual codec in use, the only reason why a user should choose a lower bandwidth codec is the slightly higher probability of the successful reservation.[3]

6 SIP Proxy Server

The SIP proxy is primarily applied in the PCF to extract SIP session and SDP codec data from SIP call flows. This additional function is a relatively simple extension of the standardized SIP proxy function set.

[15] defines two types of SIP proxy server behavior, namely transaction stateful and transaction stateless proxies. The former should track transaction state (but not necessarily call state) whereas the latter does not keep state information. Since SIP and SDP specifications have been changing rapidly during the last year, we recommend the use of a stateless proxy for the following reasons:

- The proxy does not generate SIP messages, so the SIP signaling can be end-to-end.
- A stateless proxy can simply forward messages without following transactions and dependencies between messages, thus implementation and future adoption according to the non-final standard is more easy.
- Better scalability can be achieved with the stateless design.

However, there are some counterarguments to consider:

- The proxy can only perform syntactic check on SIP messages, but it cannot force the correct order of SIP messages. This check can be implemented in the PCF but it violates our goal to separate responsibilities, since the PCF itself does not take part in SIP signaling.
- The proxy can not filter out repeated (retransmitted) SIP messages. Retransmitted SIP messages, however, should be identical, so in case of repeated SIP messages the stateless proxy sends repeated messages to the PCF as well, which can easily be recognized.
- The stateless proxy cannot support advanced functions like forking proxy mode. This restriction can be relaxed if necessary, since another general-purpose SIP Proxy can be chained after the stateless proxy.
- Implementing a SIP authentication scheme stronger than “HTTP Basic” authentication can be complicated.

A stateful proxy does not have these problems, however, its implementation and maintenance requires far more efforts than that of a stateless proxy, due to the fact that changes in SIP and SDP standards must be followed.

---

[3] Unfortunately, some RSVP implementations do not support the modification of RSVP reservation parameters without teardown, which, in fact, forces the users to issue larger reservation requests in order to ensure that during the call they will be able to change to a codec that needs more resources without loosing the QoS guarantee.

7 Protocol between the SIP Proxy and the PCF

As it was previously noted, the communication protocol between the PCF and the SIP Proxy is not yet standardized, therefore we had to elaborate its details. In this paper we restrict ourselves to review some considerations and decisions without describing the protocol syntax.

The PCF has to receive enough information from the SIP Proxy to

- identify the user,
- recognize protocol messages belonging to the same session,
- calculate RSVP Envelopes based on media and codec information in the SDP offer/answer pair,
- couple COPS requests with the corresponding RSVP Envelope.

7.1 Protocol Messages and Statefulness of the SIP Proxy

Assuming that the SIP Proxy is stateless, it cannot gather information about the INVITE transaction or call state, thus a message must be sent to the PCF every time a SIP message contains any information necessary for the decision. These SIP messages are INVITE, 183, PRACK, COMET, 200 messages for call setup and BYE, CANCEL for ending the session.

When communicating with the PCF the protocol messages sent by the SIP proxy must contain data from the *to*, *from*, *call-id*, and *cseq* fields of the SIP message to facilitate user and call identification and authentication. At the same time, RSVP Envelope calculation requires the transmission of SDP body copied from the SIP message, as well. The latter provides enough information also to match COPS requests and RSVP Envelopes. To extract this information from the forwarded SIP messages the SIP Proxy has to do only minimal processing on SIP messages and it can handle SDP data transparently, which may simplify the proxy implementation even further.

A stateful proxy, on the other hand, may gather all the SIP and SDP information necessary for the decision and forward it in a single message. However, this delays the decision process significantly, as the PCF can only consult the PIB when it receives the message from the SIP Proxy. Therefore, it is advantageous to forward different pieces of information as soon as they become available.

7.2 Transport Protocol

The transport protocol used for the transmission of the Proxy-PCF protocol messages must be reliable and it should be non-blocking to allow for the easy implementation of a stateless proxy. A persistent connection should be set up between the SIP Proxy and the PCF, thus the TCP protocol is a straightforward choice for this purpose. If, however, the Proxy and the PCF entities are co-located in the same network device, or they are components of the same software, then any other means of non-blocking and reliable data transfer might be suitable.

7.3 Enhancements via Feedback

The protocol messages mentioned so far are all uni-directional (the SIP Proxy notifies the PCF). We think that all the necessary functionality can be implemented with this uni-directional protocol, although bi-directional communication would facilitate:

- the modification of SDP and SIP parameters in view of the user profile,
- user notification via SIP in the following cases:
  - The SIP session could be ended in case of an RSVP error, which is of particular importance if the error is between the UE and the GGSN, and the UE loses the connection with the GGSN (which may happen in mobile networks).
  - Authentication parameters could be forwarded to the UE.
  - Information calculated from the user profile and the SDP could be forwarded to the UE.
  - If the authentication fails the UE could be notified instantly, as opposed to the present situation, where it will only be notified about rejected PATH messages. (The latter results in superfluous delay, unnecessarily reserved resources and the fact that the other end will also begin to set up the RSVP session.)

Nevertheless, those opting for utilizing the advantages of bidirectional communication must be aware of the fact, that interacting in the SIP session this way breaks the end-to-end nature of SIP signaling and it is not conformant to the current SIP standard.

8 Conclusions

This paper aimed at the analysis of the IP Multimedia Subsystem of third generation mobile networks from the aspect of call control, resource reservation and network policing protocol interoperability issues related to service provisioning.

The investigation was carried out through discussing some considerations based on a prototype implementation of the IMS developed by the authors beforehand. We analyzed several implementation options for the two most important functional entities of the system, the Policy Control Function and the SIP Proxy.

We proposed a two-stage decision process at the PCF, which simplifies the definition of decision rules, while remains flexible at the same time. We also showed that a stateless SIP Proxy capable of communicating with the PCF is easy to implement and that any existing proxies can be enhanced with this function via proxy chaining. Finally, we overviewed the necessary characteristics of a candidate protocol between these two functional entities.

Although the aim was to analyze the IMS of UMTS, the results presented in this paper are general enough to be applied for service provisioning in fixed IP networks, as well.

9 Acknowledgements

This work was supported by NOKIA Hungary. The authors would like to express their gratitude to György Wolfner of NOKIA for the valuable discussions. We would like to thank also Dóra Erős of NOKIA for her continous support during the course of this work.

References

1. 3GPP TS 23.228 (V5.5.0): IP Multimedia Subsystem (IMS). June 2002
2. 3GPP TS 23.207 (V5.4.0): End-to-End QoS Concept and Architecture. June 2002
3. Schulzrinne, H., Rosenberg, J.: The Session Initiation Protocol: Internet Centric Signaling. IEEE Communications Magazine, October 2000, p. 134
4. Canal, G., Cuda, A.: Why SIP will Pave the way towards NGN. In Proceedings of the 7 th ITU International Conference on Intelligence in Networks, October 2001
5. Braden, R. et al.: Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification. RFC 2205, September 1997
6. Herzog, S.: RSVP Extensions for Policy Control. RFC 2750, January 2000
7. Blake, S. et al.: An Architecture for Differentiated Service, RFC 2475, January 2000
8. Detti, A. et al.: Supporting RSVP in a Differentiated Service Domain: an Architectural Framework and a Scalability Analysis. International Conference on Communications, Vancouver (Canada), June 1999
9. Bernet, Y. et al.: A Framework for Integrated Services Operation over Diffserv Networks. RFC 2998, November 2000
10. Durham, D. et al.: The COPS (Common Open Policy Service) Protocol. RFC 2748, January 2000
11. Herzog, S. et al.: COPS Usage for RSVP. RFC 2749, January 2000
12. Lin, Y., Pang, A., Haung, Y., Chlamtac, I.: An All-IP Approach for UMTS Third-Generation Mobile Networks. IEEE Network, vol. 16, no. 5, September 2002
13. Rosenberg, J. et al.: An Offer/Answer Model with SDP. draft-rosenberg-mmusic-sdp-offer-answer-00 (formerly RFC2543 Appendix B), October 2001
14. Handley, M. et al.: SIP: Session Initiation Protocol. RFC 2543, March 1999
15. Handley, M. et al.: SIP: Session Initiation Protocol. draft-ietf-sip-rfc2543bis-05, October 2001
16. Rosenberg, J. et al.: SIP: Session Initiation Protocol. RFC 3261 (formerly draft-ietf-sip-rfc2543bis-09), June 2002
17. Camarillo, G. et al.: Integration of Resource Management and SIP. draft-ietf-sip-manyfolks-resource-02, February 2001
18. Johnston, A. et al.: SIP Call Flow Examples. draft-ietf-sip-call-flows-05, June 2001
19. Rosenberg, J. et al.: Reliability of Provisional Responses in the Session Initiation Protocol (SIP). RFC 3262, June 2002
20. Rosenberg, J. et al.: An Offer/Answer Model with the Session Description Protocol (SDP). RFC 3264 (formerly draft-rosenberg-mmusic-sdp-offer-answer-00), June 2002
21. Handley, M. et al.: SDP: Session Description Protocol. RFC 2327, April 1998