An AAA Architecture Extension for Providing Differentiated Services to Mobile IP Users

Torsten Braun, Li Ru and Günther Stattenberger

Institute of Computer Science and Applied Mathematics
University of Bern
[braun|liru|stattenb]@iam.unibe.ch

Abstract

Differentiated Services (DiffServ) are not yet fully adapted and integrated with mobile environments, especially when Mobile IP [7] is used as the mobility management protocol in the Internet. When a mobile node visits a foreign network and requests services based on Service Level Agreements (SLAs), the DiffServ Internet Service Providers (ISPs) must care about how to charge the mobile user. In addition, SLAs have to be renegotiated between home / foreign links and their ISPs. Authentication, authorization and accounting (AAA) procedures must be provided. This paper proposes a concept to combine the Service Location Protocol and the Mobile IP AAA based architecture. It is independent of the availability of a foreign agent (FA) and works for IPv4 or IPv6 in a uniform manner. The architecture supports mobile telephony over packet-based IP networks without requiring GSM-like mobility management and accounting schemes.

I. Introduction

Today's Internet services are restricted to best-effort data packet transport. QoS support is essential for business and real-time applications such as Internet Telephony. As a new and attractive approach, DiffServ [2] is expected to improve QoS support in large-scale Internet backbones. Offering DiffServ to mobile nodes (MN) yields new challenges. Normally, the foreign ISP must care about how to charge the MN. This service usage in a foreign domain requires Authorization, Authentication and Accounting (AAA).

In Section 2 we review AAA concepts, describe the various system components of an AAA Server and the generic AAA architecture with a FA. Section 3 extends the AAA Architecture by introducing SLP. Section 4 discusses specific issues about AAA, such as security, resource management and accounting management. Section 5 provides a detailed description of the proposed QoS signalling protocol for Mobile IP nodes.

II. AAA Architecture

An AAA infrastructure typically consists of AAA servers that interact with each other using an AAA protocol [4]. The AAA servers authenticate users, handle authorization requests and collect accounting data. Figure 1 shows the basic AAA model.

A user wants access to a service or a resource at the foreign domain. A foreign ISP's AAA server (AAAF), which authorizes a service based on an agreement with the user home organization, may not have enough information stored locally to verify the credentials of the user. However, the AAAF is expected to be configured with enough information to verify the client identity in collaboration with external authorities (AAAH). This procedure can determine the nature of the service granted to the user.

A home domain's AAA server (AAAH) has an agreement with the user and checks whether the user is allowed to obtain the requested service or resource. This entity might have information required to authorize the user, which might not be known to the foreign ISP.

An attendant, such as a foreign agent (FA), which is an interface for the MN to the AAA server, often does not have direct access to the data needed to complete the transaction. Instead, it is expected to consult an authority (typically in the same foreign domain, e.g. AAAF) in order to request proof that the client has acceptable credentials.

A. System Components of the AAA Server

An AAA server needs several components in order to be able to handle AAA requests and supply QoS in mobile environments. With their implementation, the AAA server can inspect the contents of the request, determine what authorization is requested and choose one of the following options to further process QoS requests:

- Query and retrieve policy rules from its SLA repository.
- Forward the policy component to another AAA server for evaluation.
- Let the policy be evaluated by the resource manager.

In DiffServ environments, customers are allowed to negotiate policies which define a fixed rate or a relative share of packets that have to be transmitted by the ISP with high priority. All these policies can be put into a SLA repository which may reside on one AAA server or may be located elsewhere in the home network. Each policy should contain the following items: *user identification, password, service type, QoS parameters (rate, maximum burst, etc), source*

IP address, destination IP address, source port, destination port, duration of the request. For evaluation and enforcement, each policy also can be retrieved by user name, by password, or by other attributes.

QoS support heavily depends on the allocation of a quantifiable amount of resources between a selected destination and source. However, network provisioning becomes very difficult and complicated in highly dynamic environments where the location and the QoS requirements of the end systems may change very quickly. So, a foreign ISP's AAA server needs to have an interface with the Bandwidth Broker (BB, Resource Manager Component) to check whether the user requirement can be satisfied or supported. As a part of the DiffServ architecture, the BB is a software agent that automates the SLA negotiation and takes responsibility to allocate resources to users as requested.

Authorization may be considered as the result of evaluating a SLA. While the policy definition is typically stored in the home domain of a visiting MN, it usually depends on the availability of the resource allocation in the foreign network whether its requirements can be satisfied. Due to the multiple administrative domain nature, a mechanism to forward messages between AAA servers is needed. Generally, any of the AAA servers involved in an authorization transaction can retrieve or evaluate a policy (SLA) through an AAA protocol. This protocol is expected to be able to transport both SLA definitions and the information needed to evaluate SLAs and also to support queries for policy information.

A Network Access Server (NAS) is an interface for the MN to the AAA server, which allows access to network services to be managed on a per-user basis. The NAS may consult the AAAF in order to request proof that the client has acceptable credentials, to learn QoS and other network policies for the user via the AAA service and to apply QoS policies to the packets. A NAS may be an edge router which provides different qualities, types, or service levels to different users based on policy and identity information [6]. A NAS is like a QoS Policy Enforcement Point (PEP). Typically only the NAS knows the true dynamic session state. So, the service equipment must be able to notify its resource manager when a session terminates or the state changes in some other way. For auditing purposes, the generic server must have some form of database to store time-stamped events that occur in the AAA server. This database can be used to account for given authorizations. With the help of certificates, this database could support non-repudiation.

B. Mobile IP AAA with Foreign Agent

A client belonging to one home domain often needs resources provided by another foreign domain (Figure 1). We propose a Mobile IP AAA Architecture using the roaming pull model [9] for this case.

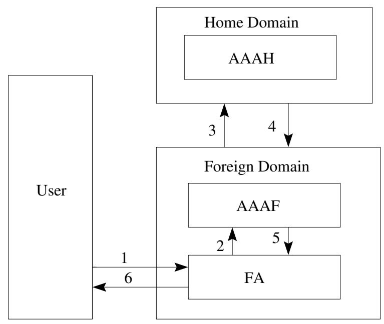

Fig. 1. AAA for Mobile IP Message Sequence in DiffServ Environment

1. The user visiting a foreign network wants to use a certain level of QoS by requesting a quantifiable amount of resources between a selected destination and itself. First, he/she needs to issue a registration request to the foreign agent (FA), which includes the authentication information. At this point the MN still has not yet gained access to the network, it can not send the requests directly to the home AAA server and because of that it doesn't have an IP address yet.
2. The FA parses this request and forwards the authentication information to the foreign Service Provider's AAA server (AAAF). At the same time it also has to keep the state for the pending registration request.
3. When the AAAF receives the registration of the MN, it checks the realm part of the NAI provided by the MN to see whether the MN belongs to its own network. The Network Access Identifier (NAI) Extension [3] is the user ID submitted by the client during authentication and has the format of username@realm. In the case of roaming, the purpose of the NAI is to uniquely identify the MN identification. Because usually the authentication information of a mobile user will typically not be validated locally, the AAAF needs to contact the appropriate external authority (AAAH) to evaluate the request by mapping the NAI to one IP address of the AAA server in the MN's home domain.
4. The AAAH looks up the corresponding policy in its SLA repository based on the user name and forwards it to the AAAF for evaluation.
5. Once the authorization has been obtained by the AAAF, it sends a query to the BB for information required to evaluate this policy and decides if it will accept a service with specific parameters. The AAAF will notify the FA about the result.
6. After a successful authorization of the MN, the service equipment should set up a policy enforcement and tell the user that the required service is available. Now, the FA is able to continue the mobile IP registration procedure without requiring further involvement of the AAA servers.

III. Integration of SLP and the AAA Architecture

The main drawback in the Mobile IP AAA architecture described above is that it depends on the existence of a FA: A FA is not always available in foreign network environments. Sometimes the MN uses some other automatic configuration mechanisms to get a new IP address such as IPv6 stateless address autoconfiguration [8] or DHCP. However, valid IP addresses are also network resources. If any MN is allowed to get an IP address by automatic address configuration, it can do anything at will. This has a tremendous impact on the network security. So we need to make some specific restrictions on methods of obtaining an IP address. Therefore, it is necessary to further develop an AAA architecture which is working in a uniform manner for IPv4/IPv6 no matter whether the FA exists or not. In order to solve these problems we integrate the Service Location Protocol (SLP) [5] into our architecture.

SLP simplifies the discovery and selection of network services such as printers etc. There are three components involved in SLP: User Agents (UAs) acquire service handlers for user applications; Service Agents (SAs) advertise service handlers; Directory Agents (DA) collect service handlers in a local network. The signalling procedures are illustrated in Figure 2.

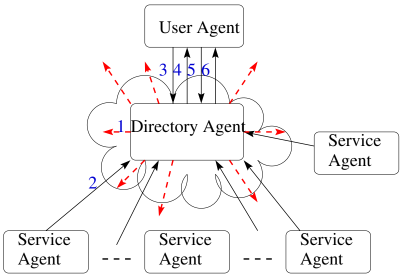

Fig. 2. Message Sequence in SLP

1. The DA periodically multicasts DA advertisements to indicate the presence of a DA to all SAs and UAs.
2. The SAs advertise themselves by registering with a DA. The registration information includes a list of all the keywords and attribute-value pairs that describe their service. Registration information also includes a lifetime after which the service information is removed by the DA. Explicit deregistration can also remove service information. The DA should return an acknowledgement on receipt of a registration or deregistration message.
3. When a client application requests a type of service, the user agent will send an attribute request to the DA to find out the characteristics of a particular service.
4. The DA sends an attribute reply which gives a list of available services matching the requested information.
5. The client chooses one, the UA sends a service request to notify the DA of its choice and acquires a service handler (i.e., service addresses and access information).
6. The DA sends a service reply to the user agent to provide the service handler.

Finally, the client application can communicate directly with the SA, they no longer need the DA's assistance.

In order to make the Mobile IP AAA architecture independent of the FA, we further make an extension by deploying SLP as shown in Figure 3. A MN can search any service agent which is available in a foreign domain (such as FA, DHCP server, printer etc.) via SLP according to the user's requirements.

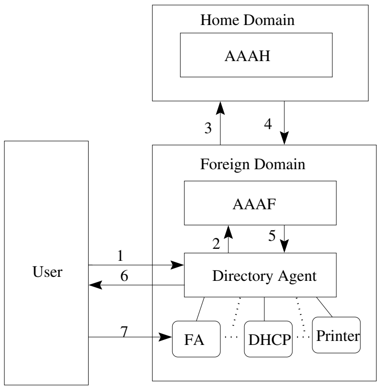

Fig. 3. Message Sequence in SLP capable AAA Architecture

1. The FA and DHCP advertise themselves by registering with a Directory Agent (DA), which periodically multicasts DA advertisements on behalf of them. Note that it is required to disable in advance the stateless autoconfiguration in IPv6 routers. Once the MN receives a DA advertisement, it will send an attribute request to obtain an IP address, which includes the authentication information.
2. The DA acts like a watchman having the responsibility of authentication. In particular, it must make sure that only valid mobile users can freely use resources / services and leave the other malicious users outside. Before the DA answers the query of the mobile user, it first needs to check whether the identity of the mobile user is valid. Then, the authentication phase begins. In order to accelerate this procedure, the DA should have a database about the valid visitors. This information can be dynamically learned via the AAA service. When the DA receives an attribute request, it checks its user database to see whether there has been a record of this user according to the username part of the NAI provided by MN. If it is not available, the DA is expected to forward authentication and NAI information to the local AAA server.
3. The AAAF first checks the realm part of the NAI to see whether the mobile user belongs to its own network. If the user is a visitor, it contacts the external AAAH to further verify the user identity.

4. QoS specifications are typically located in the home AAA server, which may be indexed by username, password etc. Therefore, the home AAA server checks the validity of the user identity based on the confidential information, then gives a proper response to the foreign AAA server. Of course, it needs to forward the SLA policy in its positive reply to the foreign domain in order to facilitate the later authorization, minimize latency and avoid too frequent control message exchange when the mobile user micro-moves between different subnets in the same ISP domain.
5. If the foreign AAA server receives a positive reply from the home AAA server, it will store the SLA specification to establish a customer record in its database. Meanwhile it will inform the DA about the authentication result.
6. When the DA is informed that this user is valid, it will immediately add the user information to its user records database. This is because at a later time, when this user wants to use the various network services, the DA must be able to assure his/her identity by directly checking the database, so that the time-consuming authentication is not necessary any more. Now, the DA can send an attribute reply which gives a list of the available services which can allocate an IP address, such as a FA or DHCP.
7. The client agent on a mobile computer chooses one service automatically or manually, gets a service handler from the DA, then contacts a FA or DHCP to get an IP address. From each SA's viewpoint, it must contact the AAAF to further authenticate the user's identity for more security. Finally, the MN will issue a registration request to require access to the network.

IV. Security Requirements

Nodes in two separate administrative domains often must take additional steps to verify the identity of their communication partners or alternatively to guarantee the privacy of the data making up the communication. The security associations needed between different entities (Figure 4) will be of central importance in the design of a suitable AAA infrastructure for Mobile IP [10].

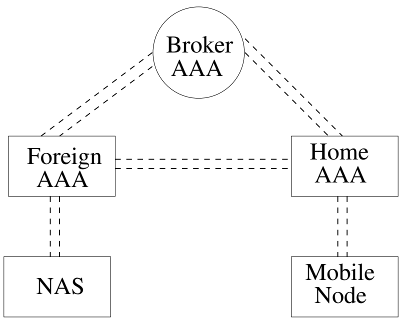

Fig. 4. Mobile IP AAA Trust Model

First, it is natural to assume that the client has a security association with the AAAH, since that is roughly what it means for the client to belong to the home domain. Second, the requirement that the AAA servers in foreign and home domains have to share a bilateral security association will cause a quadratic growth of the number of trust relationships, as the number of AAA authorities increases. At the same time one can not expect that the network that one MN visits has established a security association with the node's home domain a priori. For scalability, the AAA Broker (AAAB), acting as a mutually trusted third party entity, establishes secure associations with a large number of administrative domain AAA servers. Otherwise, they could not rely on the authentication results, authorizations, or even the accounting data which might be exchanged between them. Finally, it is clear that the NAS can naturally share a security association with the AAAF. This is necessary for the model to work because the NAS has to know whether it is permissible to allocate the local resources to the client. Since the MN's credentials have to remain unforgeable, intervening nodes (e.g., either the routers or the AAAF) must not be able to access any secret information which may enable them to reconstruct and reuse the credentials. Meanwhile, when AAA Servers communicate through intermediate AAA servers, such as brokers, it may be necessary that a part of the payload is encrypted between the originator and the target AAA server.

V. Mobile IP Node Negotiation Procedure for DiffServ

In order to achieve a complete impression on how exactly our extended AAA architecture works and how various components interact with each other to establish Differentiated Services for a mobile IP node, this section will give a more detailed description of the message sequence shown in Figure 5.

A. Initial Foreign Network Access

1. In order to obtain a temporary connectivity, IP address, subnet mask, default router, DNS server and other informations are required. When one MN receives a DA advertisement, it will send an attribute request to obtain an IP address. Because the foreign ISP needs to assure that he/she will pay for the connectivity, the user has to send some confidential information such as username, password, ID etc. to identify himself/herself. This information should be encrypted with the AAAH's public key and appended as an option extension to every attribute request message sent to the DA (Figure 6). These authentication information tends to be valid for a long period, is difficult to forge and has a strong authentication process to establish the owner's identity. It can be considered as a passport to identify the owner. Meanwhile in order to map the home domain and facilitate the later distribution of the shared key between AAAF and

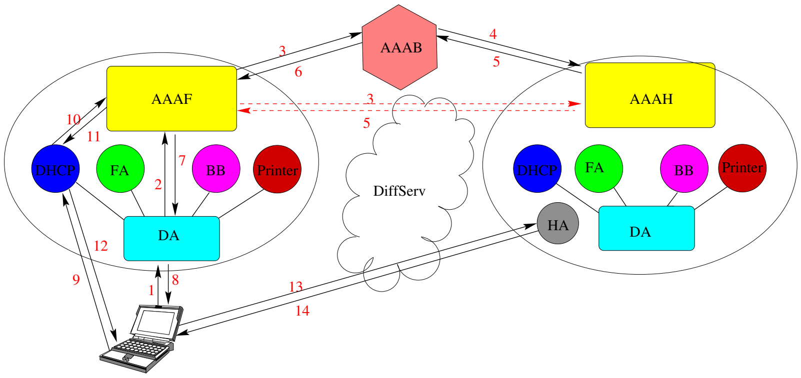

Fig. 5. Message Sequence in Negotiation Procedure

MN, the MN's NAI extension and its public key also should be included.

Type=1111	Length	Security Parameter Index
Confidential Information		

Fig. 6. An Authentication Option Extension in Attribute Request Message

2. The DA checks its user database to see whether there is a record of this user according to the username part of NAI. If it is not available, the DA is expected to forward the authentication data, NAI and MN's public key information to the local AAA server.
3. The AAAF is also required to have two tables in addition to the SLA repository with the native customers.
- One is a visiting record table about all MNs who are visiting this foreign domain. Each item in this table should contain the following information: *the username part of NAI, account number and shared key which is produced by the AAAF for the valid user, MN's public key and the SLA specifications*. The item has a lifetime which should be setup appropriately by the network operator.
- The other table is a security association table about all foreign domains with which this AAAF has established security associations. Each item in this table should contain the following information: *foreign domain name, IP address of AAAF, IP address of AAAH, shared key*.

Usually, when a mobile user moves into a new domain, at the beginning the AAA has no corresponding record to verify him/her. So it will contact the appropriate external AAA server (AAAH). By reading the realm portion of the NAI, AAAF can determine whether or where the information should be forwarded. The basic operation is as follows:

- The AAAF first checks the realm part of NAI to see whether the mobile user belongs to its own network. This is for the case when the mobile user micro-moves around in different subnets of the same administrative domain. If the user is a native customer, it will directly decrypt the authentication option with its own private key and check the validity of the user in its SLA repository.
- If the mobile user is a visitor, the AAA should check its visiting record table according to the username of NAI in order to see whether a record about this mobile user already exists or not. If his/her record is available, this user has been authenticated before and he/she certainly is a valid user.
- If this is not the case, the mobile user is a newcomer. Then, the AAAF needs to further check the security association table to see whether a security association has already been existing between the local AAA server and the AAA server of the home domain indicated by the NAI of the mobile user.
- If so, the AAA server directly sends the authentication option extension of the IP packet to the AAA server in the home domain (AAAH). The AAAH uses its private key to decrypt the authentication information (e.g. user name and password) and checks the validity of the user identity in its SLA repository. For valid users, the AAAH gives a copy of the SLA specification which needs to be encrypted with the shared keys between AAAF and AAAH. Here, the security association is assumed to be a trust relationship by which the AAA server in the foreign domain can make sure the AAAH will definitely pay for the service on behalf of those mobile users who belong to it.
- Otherwise, support from the AAAB is required. If the AAAF has an interface to the AAAB, it can send the authentication option extension and NAI extension of the IP packet to the AAAB.

4. The AAAB checks the realm part of NAI to see whether it can map this domain name into an IP address of an AAA server. If it is not available, then the AAA broker has to reject the service to the MN in the foreign network by giving a negative response to the AAAF. Otherwise, the AAA broker needs to send an inquiry message including this authentication option extension to the AAAH in order to require a copy of the authorization message from the home domain.

5. The AAAH is responsible for storing all user names and SLA specifications about the mobile users who belong to this home domain. So, when the AAAH receives the inquiry message from the AAAB, it will decrypt the authentication with its private key and look up its SLA repository. This database not only contains the user's identification but also specifies the maximum amount and type of traffic he can send and/or receive, which should be able to be indexed by the user name or password. Finally, the AAAH checks the security association table, uses a proper key (AAAB's public key or the shared-key between the AAAH and the AAAF) to encrypt the SLA information and sends the inquiring result to the correspondent node (the AAAF or the AAAB). Of course here it refers to the AAA broker.
6. The AAA Broker will decrypt the received message and issue a ticket to the AAAF. It encrypts the result with its private key and adds them to the IP packet as the IP Authentication Header [1]. This ticket is more like an entry visa, because it is typically issued by a different authority than the passport issuing authority and it does not have such a long validity period as a passport. The structure of this ticket is a digitally signed set of attributes which define the DiffServ service level of the mobile user when at home.
7. If the AAAF receives a positive reply from the external AAA server (AAAH or AAAB), it will decrypt the message with the proper key and store this SLA specification to establish a customer record in its visiting record table. Meanwhile it will establish an account number and generate a shared key for this valid user. This information should be encrypted with the MN's public key and appended as a key distribution IP option extension (Figure 7) to the message which the AAAF sends to inform the DA of the result of authentication.

Type=2222	Length	Security Parameter Index
User's Account Number And Shared Key Information		

Fig. 7. A Key Distribution IP Option Extension

8. When the DA is informed that this user is valid, it will add the user information (the username of the NAI) to its user records database and send an attribute reply to the MN. This message includes the original key distribution IP option and gives a list of available services for IP address allocation, such as FA, DHCP servers. Note that each item in user records database of DA also has a lifetime. They need to be refreshed periodically.
9. The MN first decrypts the key distribution IP option with its private key to achieve its account number and shared key in the AAAF. The UA on the MN chooses one service and gets a service handler from the DA. Finally, the MN will directly issue a service request message to the corresponding SA. In each service request message sent to the SA, the MN's has to offer the NAI extension and its account number option extension shown in Figure 8. This account number should be encrypted with the shared key between the MN and the AAAF.

Type=3333	Length	Security Parameter Index
User's Account Number in the AAAF		

Fig. 8. An Account Number Option Extension in Service Request Message

10. From each SA's viewpoint, it must contact the AAAF to further authenticate the user's identity for more security. When each SA receives the service request from the MN, first, it will have to send the NAI and the user's encrypted account number to the AAAF.
11. According to the username of the NAI, the AAAF uses the appropriate key to decrypt and check the validity of the user's account number. If the account number is consistent with the information in its visiting records table, the AAAF will inform the SA to supply the desired service to the MN. Otherwise, the AAAF will send a negative response to the SA and ask it to reject the request of this user.
12. For a valid user, the SA, which refers to a FA or DHCP server at this time, will allocate an IP address for the MN and deliver it in its service reply.
13. After this, the MN will continue with the mobile IP registration procedure and inform the HA about its current location.
14. Finally, the HA sends a registration reply to the MN indicating that the registration was successful and now it can get access to the network.

B. QoS Negotiation

After the MN has successfully got access to the network, it might further desire to enjoy QoS. First, it has to find an available SA providing Differentiated Services via the DA and specify what types of Differentiated Services are supported in this foreign domain. The basic operation is as follows:
- The MN sends an attribute message to the DA to request QoS.
- When the DA finds out his/her record in its user database based on the username of the NAI, the DA will assume that this user has been authenticated before and subsequently send an attribute reply to the MN, which gives the IP address of the SA supplying the DiffServ, such as a BB server.
- Then, the MN communicates with the BB to request the available DiffServ. The method of interaction between the MN and all the SAs is almost the same. The MN needs to send the encrypted account number and the NAI in its service request to the BB.
- The BB contacts the AAAF to further verify the user by the same procedure described above in phase 1 (initial for-

eign network access). For a valid user, the BB will give a list of supported DiffServ types in the request reply to the MN.

• The MN chooses its favoured DiffServ type among the various options.

• By default, the mobile user will be expected to enjoy the same service type as that he/she can get at home domain. As mentioned before, the SA will need to verify the user for each service request message, before making a reply. Therefore, after the BB gets the user's choice, it will still need to send the NAI and account number option extensions to the AAAF.

• If the account number provided by the MN is correct, the AAAF will look up and return back his/her corresponding SLA specification. Otherwise, the AAAF will ask the BB to reject the request of the user.

• When the BB gets a positive reply from the AAAF, the BB will appropriately configure the DiffServ routers at the foreign domain (e.g. first-hop routers) in order to support the MNs with the desired service according to the concrete QoS parameters specified in SLA. At the same time, the BB also sends a signal to the AAAF to trigger an accounting procedure on it.

• Finally, the user is informed by the BB that the requested service is now available.

C. QoS Level Modification

In some situations, the mobile user probably wants to or has to make some temporary changes of his service level due to various reasons (e.g. the charged price, the current network load, the available service type etc.). By default, the MN is expected to enjoy the same service level as that he/she can get at home domain. In order to change service level, a new option extension (Figure 9), which explicitly describes service type and necessary QoS parameters, must be defined.

- If the MN changes its QoS level, it will have to send a message including this QoS option extension to the BB.

- Each time the BB receives this kind of message including a QoS IP option extension, first, it will parse this request and only forward the NAI and encrypted account number to the AAAF. At the same time it also keeps the QoS IP option for the pending service request.

- When the BB gets a confirmation about the validity of this user identity from the AAAF, it will check its resource database to see whether the foreign network still has the ability to satisfy the client according to the current situation of the network load. If the required resources are available, the BB will immediately configure a set of DiffServ capable routers and inform the user that the service is available. Meanwhile, the BB is also required to send a signal to the AAAF to trigger an accounting procedure on it. Otherwise, a user will get a service reject message and has to degrade the service level or QoS parameters. A restart of the SLA renegotiation process is then required.

Type=3333	Length
The description of QoS parameters	

Fig. 9. A QoS IP Option Extension

ACKNOWLEDGMENTS

The work described in this paper was supported by the Swiss National Science Foundation Project No. 2100-057077.99/1

REFERENCES

[1] R. Atkinson. IP authentication header. RFC 1826, August 1995.
[2] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. An architecture for differentiated services. RFC 2475, December 1998.
[3] P. Calhoun and C. Perkins. Mobile IP network access identifier extension for IPv4. RFC 2794, March 2000.
[4] C. de Laat, G. Gross, and L. Gommans. Generic AAA architecture. Internet Draft, March 2000. work in progress.
[5] E. Guttman and C. Perkins. Service location protocol, version 2. RFC 2608, June 1999.
[6] D. Mitton and M. Beadles. Network access server requirements next generation NAS model. Internet Draft, May 2000. work in progress.
[7] C. Perkins. IP mobility support. RFC 2002, October 1996.
[8] S. Thomson and T. Narten. IPv6 stateless address autoconfiguration. RFC 1971, August 1996.
[9] J. Vollbrecht, P. Cahoun, S. Farrell, and L. Gommans. AAA authorization framework. RFC 2904, August 2000.
[10] J. Vollbrecht, P. Calhoun, S. Farrell, and L. Gommans. AAA authorization application examples. RFC 2905, August 2000.