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

Li Ru, Torsten Braun
Günther Stattenberger

IAM-00-009

November 2000

Abstract

Current Differentiated Services (DiffServ) are not yet fully adapted and integrated with mobile environments, especially when Mobile IP [1] is used as the mobility management protocol in the Internet. When a mobile node (MN) visits a foreign network and requests services based on Service Level Agreements (SLAs), the DiffServ Internet Services 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. Additional authentication, authorization and accounting (AAA) procedures must be provided for this case. This paper proposes a concept to combine the Service Location Protocol (SLP) and the Mobile IP AAA based architecture and presents a new extended AAA architecture which is independent of the availability of a foreign agent (FA) and works for IPv4 or IPv6 in a uniform manner. In this model, the MN becomes truly able to roam throughout the Internet, while needing substantially less administrative overhead. It only needs a password and a NAI to formulate its global passport. We provide a new feasible method of transferring the MN's SLA stored in the home domain to the foreign domain in a more secure and scalable manner. Meanwhile, several new IP options are also proposed in order to allow the MN to flexibly renegotiate the service level. In particular, the architecture supports mobile telephony over packet-based IP networks without having the need for GSM-like mobility management and accounting schemes. To conclude, a detailed specification about Quality-of-Service (QoS) signaling protocol for Mobile IP nodes is included. Once available, the AAA protocol and infrastructure will provide the economic incentive for a wide-ranging deployment of DiffServ in mobile environments.

CR Categories and Subject Descriptors: C.2.0[Computer-Communication Networks]: General; C.2.4[Computer-Communication Networks]: Distributed Systems; C.2.6[Computer-Communication Networks]: Internetworking.

General Terms: Security, Management, Documentation.

Keywords: Authentication, Authorization, Accounting, Home Domain, Foreign Domain, DifferServ ISP, SLA, AAA Broker, Bandwidth Broker, SLP.

1 Introduction

Today's Internet services are insecure and are restricted to best-effort data packet transport. Its main drawback is the lack of QoS support. QoS support is very essential for business and real-time applications such as Internet Telephony and on-line video retrieval. The Resource Reservation Setup Protocol (RSVP) is not applicable in large-scale Internet backbones due to scaling and billing problems. As a new and attractive approach, DiffServ [2] are expected to provide better QoS support than existing methods. Because mobility will inevitably be the main stream of future telecommunication, it is a fairly common requirement to provide network connectivity and resources necessary to the mobile users at any time and in any location. When a mobile host visiting a foreign network wants to get the same level of service that it gets at home, normally, the foreign ISP must care about how to charge the mobile node. In many models this service usage in a foreign domain requires Authorization, which leads directly to Authentication, and Accounting (AAA). These AAA functions are closely interdependent.
The rest of the paper is organized as follows. In Section 2 we review AAA concepts and describe the various system components of an AAA Server. In Section 3 the generic AAA architecture in Mobile IP with foreign agent is presented. Section 4 extends an AAA Architecture by introducing SLP. Section 5 discusses specific issues about AAA. Section 6 provide a detailed description of QoS signaling protocol for Mobile IP nodes. Finally, section 7 summarizes the key issues of our approach.

2 Generic AAA Architecture

An AAA infrastructure typically consists of a network of AAA servers that interact with each other using an AAA protocol [3]. The AAA servers authenticate users, handle authorization requests, and collect accounting data.

2.1 AAA concepts

Authentication is the process of verifying a claimed identity, in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the end-point of a channel (entity authentication). Authentication confirms that a user who is requesting services is a valid user via the presentation of an identity and credentials.

Authorization is the process of determining whether a particular right can be granted to the presenter of a particular credential and to allow him to get access to some resources which may range from simple Internet access to access to specific private resources supported by QoS. Authorization grants specific types of services to a user, based on his authentication, which services he is requesting, and the current system state.

Accounting is the process of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation. Typical information gathered are the identity of the user, the nature of the delivered service, the time the service begins, and the time it ends.

2.2 Basic AAA Entities and Model

The purpose of an AAA server is to authorize and characterize the individual services for the users. Therefore, any information which authenticate an user can be retrieved from the AAA server. Figure 1 shows the basic AAA model.

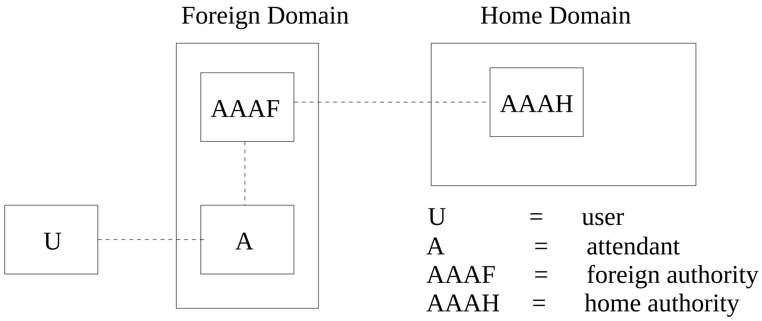


Figure 1: AAA Servers in Home and Foreign Domains

1. A user wants access to a service or a resource at the foreign domain.

2. 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 carry out the verification for 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, which mainly depends on secure authentication of the client's credentials, can negotiate the authorization which determines the nature of the service granted to the user.

3. A home domain's AAA server (AAAH) [1] has an agreement with the user and checks whether the user is allowed to obtain the requested service or resource. This entity may carry information required to authorize the user, which might not be known to the foreign ISP.

[1] In essence, the AAAF and the AAAH are both AAA servers and exactly the same in function. The AAAH refers to the AAA server in the user's home domain, while the AAAF refers to the AAA server in the foreign domain.

4. An attendant, which provides the service itself and 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.

2.3 System Components of the AAA Server

An AAA server needs several components shown in Figure 2 in order to be able to handle AAA requests and supply QoS in mobile environment. 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 the policy rules from its SLA repository for the answer.
- Forward the policy component to another AAA server for evaluation.
- Let the policy be evaluated by the resource manager.

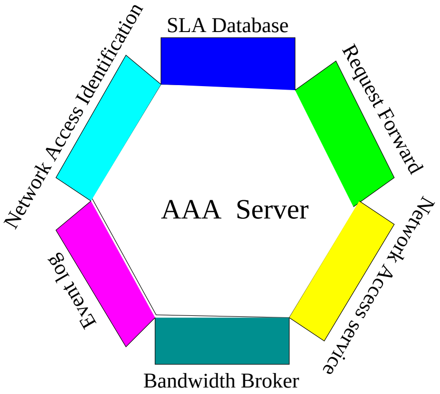


Figure 2: System Components of the AAA Server

For further details, please check the signaling description in section 6.

(a) Network Access Identifier

The Network Access Identifier (NAI) Extension (RFC 2794) [4] 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 and to provide assistance in the routing of the authentication request. The AAAF can map the realm portion of the NAI into an IP address of the MN's home AAA server.

(b) SLA Database

In DiffServ environments, customers are allowed to negotiate policies (SLAs) 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 independent policy should contain the following tuple: *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.

(c) Bandwidth Broker

The ultimate goal of network QoS support is to provide users and applications with high quality data delivery services, which 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. QoS can only be provided if the backbone networks of the ISPs are well designed and provisioned. So, a foreign ISP's AAA server needs to have an interface with the Bandwidth Broker (Resource Manager Component) to check whether the user requirement can be satisfied or supported. In section 5 we will discuss this issue separately.

(d) Request Forwarding

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 will 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.

(e) Network Access Server

The Network Access Server (NAS) may be an edge router system which provides different qualities, types, or service levels to different users based on policy and identity information [5]. A 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. This makes NAS 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.

(f) Authorization Event Log

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.

3 Mobile IP AAA with Foreign Agent

This section describes the use of AAA systems in combination with Mobile IP. For the sake of clarification, a very brief overview of Mobile IP is introduced here.

3.1 Mobile IP

The Mobile IP system consists of several network components: MN (Mobile Node), FA (Foreign Agent) and HA (Home Agent). The HA manages the mobility of an IP host between different IP networks by allowing a MN to have two IP addresses. One is its home address, which is permanently static and is used to identify TCP connections, the other is the care-of address which changes at each new point of attachment and can be thought of as the MN's topologically significant address. Namely, this new address indicates the network number and identifies the MN's point of attachment with respect to the network topology, and thus packets addressed to this care-of address will be routed by normal Internet routing mechanisms to the MN's location away from home. The home address enables MN to continually receive data on its home network, where Mobile IP requires the existence of a network node known as HA. Whenever the MN visits a foreign network, it must register its new care-of address with its HA, then the HA redirects the packets from the home network to the care-of address.

3.2 Mobile IP AAA Architecture and Message Sequence

Within the Internet, a client belonging to one home domain often needs to use resources provided by another foreign domain (Figure 3). Usually, the foreign network ISP wants to make sure that the mobile user can pay for the connectivity. So before access to the resource is permitted, the FA in the foreign domain that attends to the client's request probably requires the client to provide some credentials for authentication. Apparently the FA is not able to make the decision itself, so it needs to contact the local AAA server, which maybe have to contact the client's home authority AAA server to verify the signature and obtain assurance of charge. Here a general Mobile IP AAA Architecture [6] using the roaming pull model [7] is provided for this case. [2]

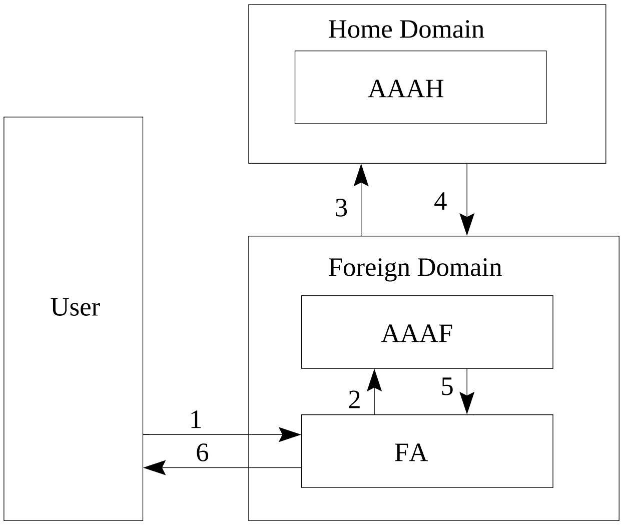


Figure 3: AAA for Mobile IP Message Sequence in DiffServ Environment

1. The user visiting a foreign network wants to use a certain level of QoS by requesting the allocation of 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 (e.g., identification, password, and an unforgeable signature). 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 (it is actually requesting one to be initialized) 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.

[2] There are three different kinds of authorization sequences [7]: push model, agent model, pull model. In the first two models, the user first needs to communicate directly with the home AAA server. But it is impossible, because at the beginning of a communication, the mobile user still hasn't completed the registration procedure to inform home agent its current location. Therefore, it doesn't have access to the network.

3. When the AAAF receives the registration of MN, it checks the realm part of the NAI provided by the MN to see whether the MN belongs to its own network. 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 home AAA looks up the corresponding policy in its SLA repository based on the user name, and forwards it to the AAAF in order to do the actual policy 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. Finally, the AAAF will notify the FA about the negotiation 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 by the AAA servers.

4 AAA Architecture extension

There is a main drawback in the Mobile IP AAA architecture described above in 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. This is the case in both IPv4 and IPv6.

4.1 Automatic Address Configuration

1. In IPv4, if one MN is connected to a link but receives no Agent Advertisements due to the lack of a FA, even after sending a number of Agent Solicitations, it can try several other ways to get connectivity. One of them is to attempt to obtain an address from a Dynamic Host Configuration Protocol (DHCP) [RFC 2131] server. If this is successful, then the MN can use this address as a collocated care-of address [3] and register it with its HA.

[3] A collocated care-of address is an IP address temporarily assigned to an interface of the MN itself. The network-prefix of a collocated care-of address must equal the network-prefix that has been assigned to the foreign link being visited by a MN. This type of care-of address might be used by a MN in situations where no FAs are available on a foreign link, a collated care-of address can be used by only one MN at a time.

2. As an evolutionary step from IPv4, IPv6 can be installed as a normal software upgrade in Internet devices. Because IPv6 is the next generation of the Internet Protocol, it will ultimately replace IPv4 as the primary network-layer protocol of the Internet. So we need to consider our AAA based architecture further in the context of IPv6. IPv6 differs from IPv4 in some very important issues. Among them, a major difference for IPv6 is that the natural repository for the attendant (FA) is no longer one part of the Mobile IP protocol model. Instead, in IPv6 a MN can configure its a care-of address by using Stateless Address Autoconfiguration [8] and Neighbor Discovery [9] or stateful configuration services (DHCP servers). When a mobile user comes to a foreign domain, he first listens to Router Advertisements. Because IPv6 defines both a stateful and stateless address autoconfiguration mechanism, periodic Router Advertisements which are sent to the all-nodes multicast address include options listing the set of active prefixes on a link and flags specifying which mechanism a host should use.

   the stateless autoconfiguration model A host generates its own address by using a combination of locally available information and information advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface token" that uniquely identifies an interface on a subnet. An address is formed by combining the two.

   the stateful autoconfiguration model (DHCP) Hosts obtain interface addresses and/or configuration information and parameters (e.g. netmask, a default router, the domain name server (DNS) for the local network, and various other bits of useful information from a DHCP server. Servers maintain a database that keeps track of which address has been assigned to which host.

It should be recognized that valid IP addresses are also network resources. If any mobile user is allowed to get an IP address by automatic address configuration, he/she can do anything at will. This has a tremendous impact on the network security, which makes the network very vulnerable to attack from the outside. As a result, the whole AAA architecture will not be useful at all. So we need to make some specific restrictions on methods of obtaining IP address. Meanwhile it is necessary to further develop an AAA architecture which is working equally in a uniform manner for IPv4/IPv6 no matter whether the FA exists or not. In order to resolve these potential troubles, here we introduce the concept of the Service Location Protocol (SLP)[10] into our architecture.

4.2 Service Location Protocol

SLP is a new IETF standards-track protocol providing a scalable framework to simplify the discovery and selection of network services such as printers, Web servers, databases and the future variety of emerging services. It is well suited to client-server applications and establishing connections between network peers that offer or consume generic services. As computers become more portable and increasingly various network services become available, the feature of SLP is becoming more important. There are three components involved in SLP: User Agents (UAs), which acquire service handles for user applications; Service Agents (SAs), which advertise service handles; Directory Agents (DA), which collect service handlers in a local network. Its working scenario and main signaling procedures are illustrated in Figure 4.

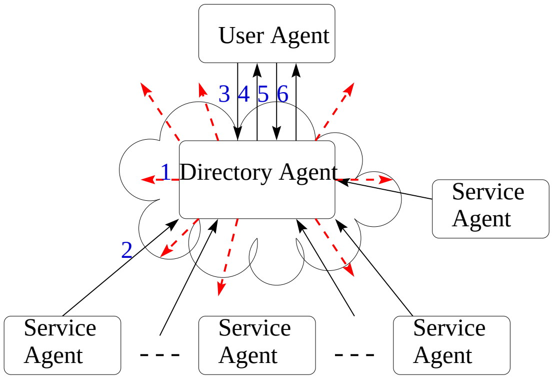


Figure 4: Message Sequence in SLP

1. The DA periodically multicasts DA advertisements on the link 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. In order to avoid the cases where service hardware breaks but the service continues to be advertised forever, registration information also includes a lifetime after which the service information is to be removed by the DA. Explicit deregistration can also remove service information. The DA should return an acknowledgement on receipt of a registration or deregistration.

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 information about the service or 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, either automatically or manually by a user, 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.

4.3 Integration of SLP and the AAA Architecture

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 5. One MN can search any service agent which is available in foreign domain (such as FA, DHCP server, printer etc.) via SLP according to the user's requirements.

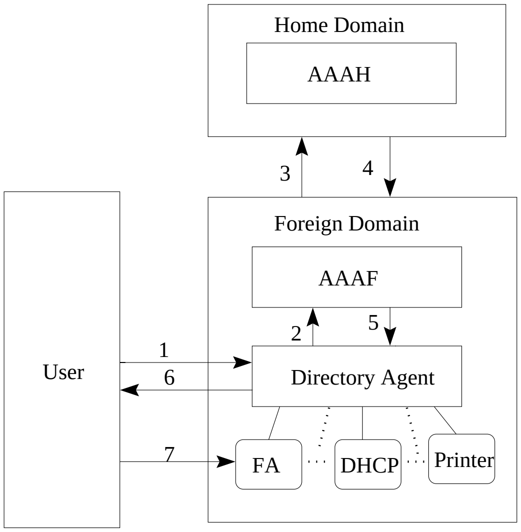


Figure 5: Message Sequence in SLP capable AAA Architecture

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 in order to strictly limit the network resource access by mobile users in some DiffServ domains, a system administrator is required to appropriately configure IPv6 routers in advance disabling the stateless autoconfiguration facility. It is clear that a mobile user desiring to access

a network in a foreign domain, he/she first has to get a valid IP address. 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 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. These informations 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 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 AAA server (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 home AAA server to further verify the user identity by mapping the realm part of the NAI.

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 for authentication, 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 micromoves between different subnets in the same ISP domain. [4]

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

[4] It is known that when Mobile IP is used for micro-mobility support, it results in high control overhead due to frequent notifications to the HA and high latency and disruption during handoff. One key Mobile-IP AAA requirements is to minimize Internet traversals in order to reduce latency.

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, while will be described and discussed in sections 6. Finally, the MN will issue a registration request to require access to the network.

5 Specific AAA Architecture Issues

5.1 Scalability

Figure 1 shows a configuration in which the AAA servers in foreign and home domain have to share a security association. Otherwise they could not rely on the authentication result, authorizations, nor even the accounting data which might be exchanged between them. However, this security model configuration can cause a quadratic growth of the number of trust relationships, as the number of AAA authorities increases. Requiring such bilateral security relationships is not scalable in the end. At the same time one can not expect that the network that the MN visits has already established a security association with its home domain. Alternatively, here we need dynamic trust relationship between AAAH and AAAF. This security relationship is dynamically created between two entities who may never have had any prior relationship, but the involved entities must have a mutually trusted third party. For example, a merchant trusts a cardholder at the time of a payment transaction because they both are known by a credit card organization. Similarly in Figure 6 we insert a broker as a third party between the AAA servers in different network domains to establish secure transactions in a more scalable way. The broker acts as a settlement agent, providing security and a central point of contract for many service providers and enterprises. It enables the foreign and home domains to cooperate without requiring each of the networks to have a direct business or security relationship with all the other network administrative domains. Thus, brokers offer the necessary scalability for managing trust relationships between otherwise independent network domains.

5.2 Security Requirements

Nodes in two separate administrative domains often have to 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 associ-

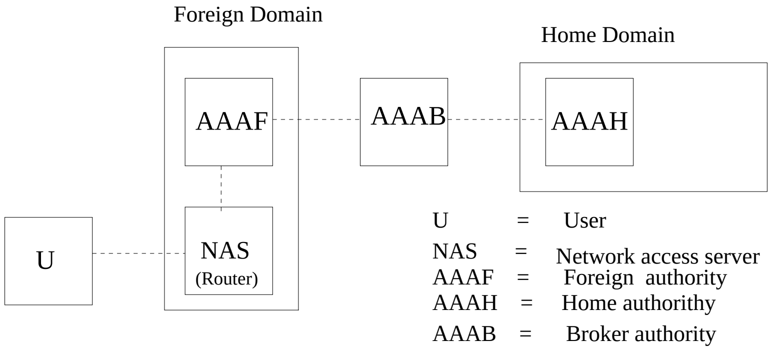


Figure 6: AAA Broker Model for Mobile IP

ations needed between different entities (Figure 7) will be of central importance in the design of a suitable AAA infrastructure for Mobile IP [11].

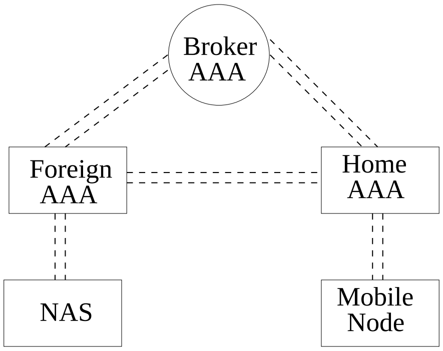


Figure 7: Mobile IP AAA Trust Model

1. 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.

2. Second, instead of requiring that the foreign domain keep current security associations with each possible home domain, acting as a mutually trusted third party entity, the AAA Broker establishes secure associations with a large number of administrative domain AAAH and AAAF, because otherwise they could not rely on the authentication results, authorizations, or even the accounting data which might be transacted between them.

3. Finally, it is clear that the NAS (attendant) can naturally share a security association with the AAAF. This is necessary for the model to work because the attendant has to know whether it is permissible to allocate the local resources to the client.

4. Since the MNs' credentials have to remain unforgeable, intervening nodes (e.g., either the routers or the AAAF) must not be able to access to any secret information which may enable them to reconstruct and reuse the credentials.

5. End-to-End Security. When AAA Servers communicate through intermediate AAA servers, such as brokers, it may be necessary that a part of the payload be encrypted between the originator and the target AAA server. The security requirement may consist of one or more of the following: End-to-End message integrity, confidentiality, replay protection, and nonrepudiation.

5.3 Network Provisioning In Mobile Environments

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. Upon SLA negotiation for new incoming DiffServ traffic, a request including a service type, bandwidth, a maximum burst, and other QoS parameters is sent to the BB in order to verify whether there exists unallocated bandwidth to meet the request and whether this foreign network is able to support this service level without congestion. That means that ISPs probably offer SLAs that guarantee QoS levels or have to offer discount depending on resource availability. If a request passes these tests, the BB has to communicate with the ingress and egress border routers to configure a group of DiffServ capable routers with the correct forwarding behavior for the desired service. Then, the available bandwidth is reduced by the requested amount and the flow specification is recorded. One point deserves special attention. In a DiffServ Network, the prerequisite of an end-to-end QoS guarantee is to fully establish the SLAs between DiffServ ISPs. Usually, this will need several ISPs to be involved. Therefore, a specific Broker signaling protocol is necessary to automate the SLAs negotiation and set up an unbroken chain of SLAs between all involved ISPs [12]. That means that authorization requests may be chained through a set of servers. Each server among them may have a contractual relationship with servers on both sides of it in the chain. They need to keep track of the session state, and be able to effect changes to the session if required. At the same time the BBs tracking the same session need to be able to initiate changes to the session, and to inform other resource managers when significant changes occur.

5.4 Accounting Management for MN in DiffServ Environment

5.4.1 The Requirements for Accounting

The topic of perfect charging systems is very complicated. A more detailed description about this aspect is beyond the scope of this paper. But in order to make the discussion complete here, we highlight the following typical problems which should be taken into account when providing DiffServ for the mobile users.

Multiple Session Record Usually a single accounting record is produced per session. But it is necessary to generate several accounting records from a single session when pricing changes during a session. For instance, the price of a service can be higher during peak hours than off-peak or roaming might cause a change in the tariffs. In another example it is possible that a session could be re-established with improved QoS. This would require the production of accounting records at both QoS levels. To permit accounting systems to tie the records together, a session identifier needs to be present in each of the record. In most cases, the network device will determine when multiple session records are needed, as the foreign device is aware of factors affecting foreign tariffs such as QoS changes or roaming.

Scaling And Reliability With the continuing growth of the Internet, it is important that accounting management systems are scalable and reliable [13]. In the case of usage sensitive billing, loss of accounting data can directly translate to revenue loss. A high degree of fault resilience is necessary in accounting management.

Stop Accounting When a Mobile IP user moves to another foreign domain, he doesn't need to send any notification to the original FA. The binding of care-of address and home address in HA will be updated from the latest registration requisition message, otherwise the binding will become invalid due to a timeout. Therefore, in order to stop counting time in DiffServ Networks, a new Deregistration message needs to be defined by which the customer can inform the default router explicitly to terminate the service. Meanwhile, as network operations grow in sophistication, NAS might provide real-time monitoring of port and user status, so that the state information can be used to implement policy decisions, monitor user trends, and provide the ability to possibly terminate access for administrative reasons. For example, in some cases when the MN suddenly crashes, after a specific period of time during which its default router doesn't receive or send any IP packets, it is reasonable for this router to assume the MN has crashed and stop accounting for it.

5.4.2 Accounting Signal Description

Internet charging is a very complicated research issue, so we only simply apply some ideas presented in a VPN Charging System [12]. In brief, the complete charging system works as shown in Figure 8. Billing is based on SLAs which are either pre-configured or dynamically setup if a SLA negotiation protocol exists.

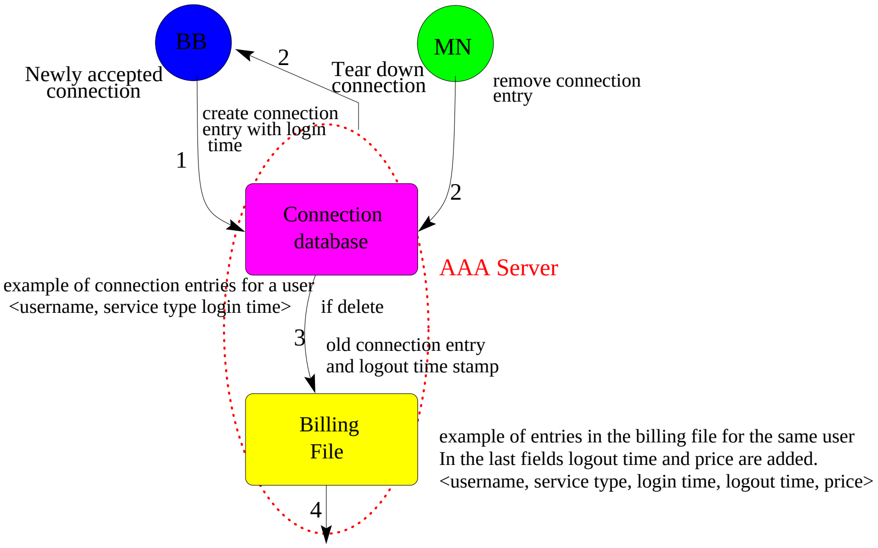

BB
MN
Newly accepted connection
2
Tear down connection
remove connection entry
create connection entry with login time
1
2
Connection database
AAA Server
example of connection entries for a user
<username, service type login time>
if delete
3
old connection entry and logout time stamp
Billing File
example of entries in the billing file for the same user
In the last fields logout time and price are added.
<username, service type, login time, logout time, price>
4

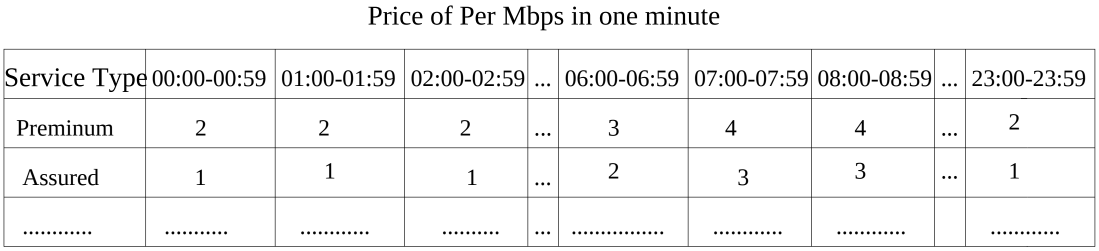
Figure 8: Cost calculation

1. If a new mobile user's request is accepted, namely his bandwidth requirement can be fulfilled, the BB should give a positive signal to trigger the accounting procedure in the AAA server. Meanwhile that connection along with the login time is recorded in the connection database.

2. After a certain period when the user wants to disconnect the connection, he must explicitly send a deregistration message. As network access server, the default router is required to provide real-time monitoring of port and user status. So once the default router receives this deregistraion message from the mobile client, it will notify the BB on the local AAA server to perform some proper processes.

3. The BB immediately terminates the service offered to this user and releases the corresponding resource which ever is occupied by him/her. At the same time the AAAF also should delete this user's connection entry from the connection database and add it to the billing database with the logout time stamp added to that entry. In fact, before being added to the billing database the system invokes the pricing table to compute the price of a

specific connection. Here we assume an ISP creates and publishes a price table, which is a pricing matrix similar to the one shown in the Figure 9. For example, if a mobile user has used assure service from 6:10 a.m. to 8:30 a.m. then the price can be calculated as:
2*[(3*10)+(4*60)+(4*30)]=7.80 SFr.



Price of Per Mbps in one minute

Service Type	00:00-00:59	01:00-01:59	02:00-02:59	...	06:00-06:59	07:00-07:59	08:00-08:59	...	23:00-23:59
Preminum	2	2	2	...	3	4	4	...	2
Assured	1	1	1	...	2	3	3	...	1
....	....	....	....	...	....	....	....		....

Figure 9: Price Database

4. At last, the AAAF will distinguish between inter-domain and intra-domain accounting events and routes them to interested parties appropriately (the AAA Broker or the AAAH).

6 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 10.

Phase 1: 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 (Public-Key Authentication) and appended as an option extension to every attribute request message sent to the DA (Figure 11). [5] These authentication information tends to be valid for a long period, is difficult to forge, and has

[5] Because the purpose of Type Number is only to identify the distinct type of an option extension in IP packet. So, here in order to illustrate the format of this two option extensions

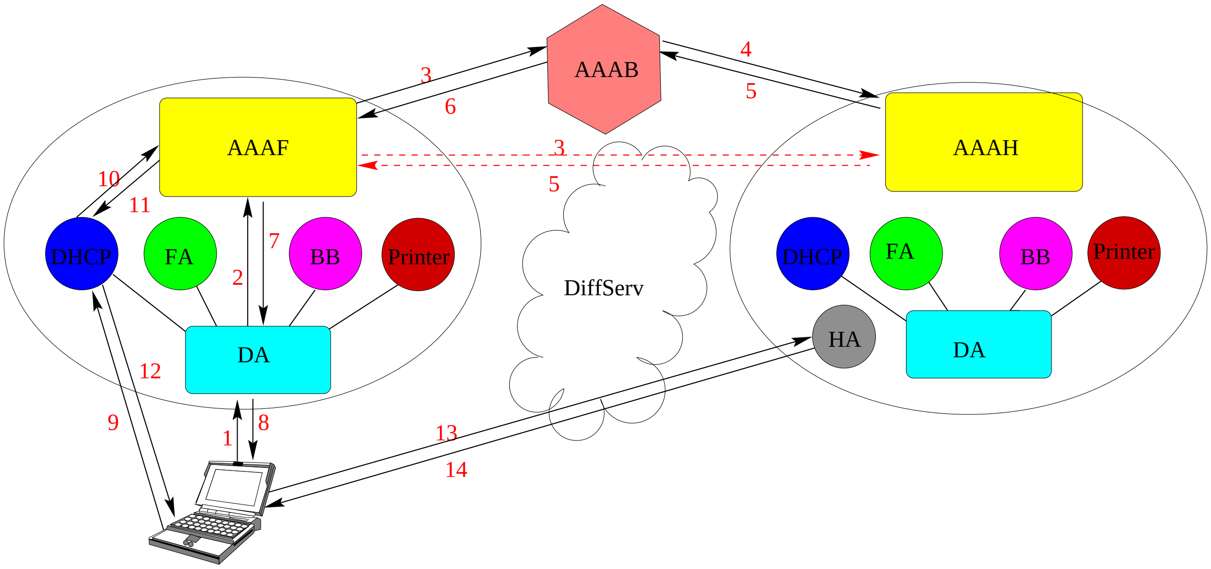


Figure 10: Message Sequence in Negotiation Procedure

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

Type=1111	Length	Security Parameter Index
Confidential Information		

Figure 11: 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.

newly defined, the numbers 1111, 2222 or 3333 are just arbitrarily chosen. Due to the fact that each option extension has to have a unique type number, the two numbers shouldn't have any confliction with the existing standard option extension in IP packet header.

- 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, so when its lifetime expires, it will be deleted to make room for new entries. This lifetime variable 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 the AAAF, IP address of the 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 micromoves 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 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 mobile user.
- If so, the AAA server directly sends the authentication option extension of the IP packet to the AAA server in 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 the AAAF and this 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, the 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 (RFC 1826)[14]. 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 (th AAAH or the 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 12) 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		

Figure 12: 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 periodically refreshed.

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 automatically or manually, and gets a service handler form 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 13. 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		

Figure 13: An Account Number Option Extension in Service Request Message

10. Because 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 has 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 at this time, will allocate an IP address to the MN 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.

Phase 2: QoS Negotiation

After the MN has successfully got access to the network, it might further desire to enjoy QoS service. 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 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 BB server.

- Then the MN communicates with the BB to inquiry 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 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. 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 favorite 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 was mentioned before, for each service request message, before making a reply, the SA will need to verify the user. 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 legitimate, 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.

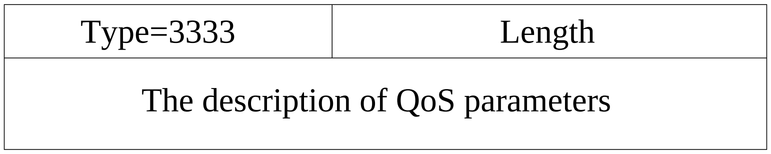
- When the BB gets a positive reply from the AAAF, according to the concrete QoS parameters specified in SLA, the BB will appropriately configure the DiffServ routers at the foreign domain (e.g. first-hop routers) in order to support the MNs with the desired service. At the same time, the BB also sends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

Phase 3: QoS Level Modification

In some situations, the mobile user probably wants to or has to make some temporary changes about his service level due to various reasons (e.g. the charged price, the current network load, the available service type and so on). 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 14), 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 usr 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 ready. 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	

Figure 14: A QoS IP Option Extension

7 Conclusion

With the increasing popularity of portability and ease of network access, it becomes natural for users to expect to be able to access the Internet at any time and from anywhere, and to transparently remain connected and continue to use the network as they move about. We have proposed a new AAA based architecture for QoS provisioning to Mobile IP users. This architecture works in a uniform manner for IPv4 or IPv6 independent of the existence FA. A detailed signaling protocol specification is further presented in order to support QoS negotiations in mobile environments. In this model, one MN becomes truly able to roam throughout the Internet, while on the other hand needing substantially less administrative overhead. It only needs a password and a NAI to formulate its global passport. Meanwhile we also considered some key issues, such as scalability, security, resource management and accounting requirements. Once available, the AAA protocol and infrastructure will provide the economic incentive for a wide-ranging deployment of Mobile DiffServ IP Differentiated Service.

References

[1] C. Perkins, “IP Mobility Support”, RFC 2002, October 1996.

[2] S. Blake, D. Black, M. Carlson, F. Davies “An Architecture for Differentiated Services”, RFC 2475, December 1998.

[3] C. de Laat, G. Gross, L. Gommans, “Generic AAA Architecture”, Internet Draft, draft-irtf-aaaarch-generic-01.txt, March 2000.

[4] P. Calhoun, C. Perkins “Mobile IP Network Access Identifier Extension for IPv4”. RFC 2794, March 2000.

[5] D. Mitton, M. Beadles,“Network Access Server Requirements Next Generation NAS Model”, draft-ietf-nasreq-nasmodel-02.txt, May 2000.

[6] S. Glass, T. Hiller, S. Jacobs, C. Perkins “Mobile IP Authentication, Authorization and Accounting Requirements”, Internet Draft, draft-ietf-mobileip-aaa-reqs-03.txt, March 2000.

[7] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, “AAA Authorization Framework”, RFC 2904, August 2000.

[8] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration”, IETF RFC 1971, August. 1996.

[9] T. Narten, E. Nordmark, and W.Simpson, “Neighbor Discovery for IP Version 6”, IETF RFC 1970, August.1996.

[10] E. Guttman, C. Perkins, “Service Location Protocol, Version 2”. RFC 2608, June 1999.

[11] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans,“AAA Authorization Application Examples”, RFC 2905, August 2000.

[12] I. Khalil, T. Braun “Implementation of a Bandwidth Broker for Dynamic End-to-End Resource Reservation in Outsourced Virtual Private Networks”, 25th Annual IEEE Conference on Local Computer Network, LCN, November 9-10, 2000, Tampa, Florida.

[13] J. Arkko, Ericsson, “ Requirements for Internet-Scale Accounting Management” Internet Draft, draft-arkko-acctreqlis-00.txt, August 1998.

[14] R. Atkinson, “IP Authentication Header”. RFC 1826, August 1995.