ACCESS NETWORK INDEPENDENT SERVICE CONTROL SYSTEM FOR STREAM BASED SERVICES

Rami Lehtonen *Jarmo Harju*
Department of Information Technology, Tampere University of Technology
P.O.Box 553, FIN-33101 Tampere, Finland,
e-mail: rampe@cs.tut.fi, harju@cs.tut.fi

ABSTRACT

The purpose of this paper is to give an overview of the access network independent service control system that can be used to order stream based services for a number of terminals with different capabilities. A control system is needed to handle the parameter negotiation and service initiation between the client and the server system. The stream based service is adapted to different access networks via the control system's parameter negotiation procedure. The stream application may also dynamically change the service parameters like bandwidth. In addition, the control system allows us to separate the service control entity from the entities involved in the service contents (e.g. playing a media stream).

1. INTRODUCTION

The adaptation of IP-based networking paradigm in practically all types of communications networks opens huge possibilities for truly network independent provision and access of electronic services (e-services). While the Internet may remain as a global open source for information, teleoperators and content providers can use the same basic technology to create specialized services for registered subscribers. These service specific virtual private networks (SVPNs) are a combination of customer related databases, service databases, and network connections supporting sufficient security and QoS features. According to some opinions, there will be at least three distinct networks based on the available services: 1) the current global Internet with e-commerce, information services and e-mail, 2) a broadband network for entertainment services, 3) a mobile network with services suitable for PDA- or communicator type of user equipment. The technology and convergence in the digital world would not, necessarily, make this kind of separation inevitable or inconvenient. Instead, one can also imagine a situation that using just a few different equipments the user could flexibly control his or her access to all the information and entertainment published in digital form.

With the concept of SVPN it will be possible to build commercially feasible e-services, which can be largely independent of particular access technologies. From the users' point of view, the services should be easily available across the spectrum of different terminal equipments, such as remote control devices with TV sets (or media screens), mobile phones, PDAs, laptop and desktop computers. This kind of unified approach, although common in visionary talks, is currently far from reality.

Users from various access networks are currently connected to different service systems. From the user's point of view this approach is feasible enough, if the user is using only one access type and its services. But it has drawbacks, because the user can not roam between services designed for specific access networks. From the perspective of service provider the network convergence opens up possibilities for introducing new services and brings also cost effective way to manage the users and services. Thus, the service provider's vision is a common service system, a platform, which can be accessed from various access networks and which can be the basis for the service development.

This paper concentrates on defining an access network independent part of that SVPN system. To be able to access the service system from the different access networks, we need a common backbone network and a control system to map the service to different access networks. The backbone network, which will be based on Internet Protocol (IP) technology, connects the different access networks to the service system. The IP protocol was an evident

choice, because it is supported nowadays by the most access networks and it provides a way to distribute the service entities across the network.

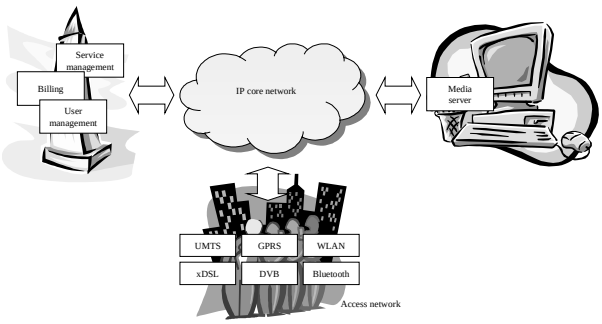

Figure 1. An overview of the SVPN system.

Figure 1 shows an overview of the SVPN system architecture. From the figure we can clearly notice that the IP backbone network connects the access networks together with the service system and with the media servers. The media servers provide the actual service stream and can be separated from the service administration system. The end user should be uniquely identified no matter what access network he/she uses. It is also important for the service system to know the relation between the user and the terminal equipment he/she uses, so the stream services can be sent to the right address.

However, before we can talk about access network independent service system, we need a control system that adapts the service to the different access networks and manages the user information within the SPVN. This paper concentrates on defining a service control system for stream based services, even though the control system allows us to use it also for transaction type of services. The emphasis is in defining and transmitting the generic parameters that are necessary for launching personalized services provided by SVPNs. While the details of the user interface will depend on the terminal equipment, a generalization of the concept of Electronic Programming Guide (EGP) can be roughly applied to get an idea of the functionality of the user interface. It has similarities with portal services, and user's selections and input to the system could be based on customized web or wap browsers.

In this paper, we make a clear distinction between the order (purchase) of the service and the delivery of the service (e.g., a media stream) itself. For example, a UMTS phone can be used as a remote controller for obtaining digital TV programs or other media services to the terminal equipment attached to some fixed network. This will impose new requirements to the utilization and management of subscriber information, and, more importantly, it will affect the operation and management of the services in the SVPNs.

2. ACCESS NETWORKS

Access networks have different characteristics e.g. in terms of bandwidth, delay, price and mobility. Still, from the service provider's point of view, practically all access networks could support the concept of SVPN. There can also be several hierarchical levels in the access to the Internet, for example:

- Telephone network access
  * Analog telephone line/ISDN/xDSL
- CableTV access
  * DVB
- Leased lines access
  * LAN
    - Wireless LAN
    - Bluetooth
- Cellular network access
  * GSM/GPRS/UMTS
    - Bluetooth

All of these network technologies (horizontal technologies) will support IP, although their capabilities to support e-services vary greatly. In this paper the main objective is to study and describe mechanisms for obtaining (ordering, purchasing) services via an SVPN by using any of these access networks. In this chapter the main characteristics of these access networks from the SVPN's point of view are discussed.

The telephone networks provide many different access methods for the data traffic: analog traffic by using modems and digital traffic by using ISDN or xDSL. These access methods are currently the most commonly used and they provide a wide range of access bandwidth from a modem's few tens of kilobits/s to a xDSL's several Mbits/s. However, the real bandwidth between the user and the Internet may also depend on the ISP's connections to the Internet. For example the connection speed between the user and the ISP is not normally the limiting factor anymore with the xDSL technology. The telephone network can introduce some difficulties in creating the mapping between the end users and the end system, because some of the access methods use dial-up connection and thus the IP address of the end system is not fixed. Normally the user is not authenticated at all, but the authentication can be performed between the user and the access network (ISP) if needed. The quality of service issues can be rather easily adapted to this type of access network. The main quality of service problems are related to the high delay and low bandwidth.

CableTV network and especially DVB presents a quite new connection type to the IP world. The connection is normally a unidirectional wideband broadcast connection from the network towards the user. The upstream control connection is thought to be established e.g. via telephone network. From the

SVPN's point of view the DVB network is a quite ideal method to provide stream services that need wide bandwidth, if the upstream control connection is somehow available. Although the DVB network can be seen rather fixed and the end system mobility is not critical, it might be beneficial to arrange the return channel via e.g. cellular network to avoid a mesh of cables. Because of the wideband connection, the quality of service issues are not so critical with the DVB networks.

The leased line access provides usually a high bandwidth and low delay pipe towards the Internet. The end systems are connected to the local network either via wired connection, such as LAN, or via wireless connection, such as WLAN or Bluetooth. From the mobility point of view the leased line access with the wired connections can be considered fixed and thus the mapping between the user and the end system is rather simple. The wireless connectivity is more challenging from the SVPN's perspective, because of mobility, wireless radio interference and limited bandwidth compared to the wired counterparts. The total bandwidth in WLAN is several Mbits/s, but it is shared between active users, so the bandwidth to one user is still quite limited. In Bluetooth access the maximum bandwidth between the master and slave device is approximately 700 kbits/s. The working distance is limited with these techniques for 10 to 100 meters without a handover to another access point, so it is possible that the user changes the access point quite often.

In addition to the access techniques introduced earlier, we can control and use the SVPN via cellular access. UMTS and GPRS provide an IP based connectivity to the cellular end systems and thus they offer a wide coverage for the SVPN services. The cellular access can be seen mostly as a control connection, because of the quite slow connection speed and high delay, but it is also possible to use the cellular access for the actual services. In the first release of the GPRS the connection speed is few tens of kbits/s for one user. In the later releases the speed will increase, but the usage of multimedia services is still restricted. The advantage of the cellular access is a working infrastructure on the user identification, mobility and billing. This can be integrated to the SVPN system if the SVPN operator is also managing the cellular access network.

General problems from the SVPN's point of view that can be associated with almost every access network include firewalls, NAT systems, mobility, security, quality of service issues, billing and user management. These issues are discussed in Chapter 5 in more detail.

3. SERVICES

The service control system architecture specified in this paper was designed mainly for stream services, but it supports also transaction type of services. The service trends and types are shortly introduced here before we take a closer look at the service control architecture overview.

3.1. Service trends and types

Traditional way to implement services is based on vertical layer model, where the services are specified individually for each access type. To be cost effective in terms of service production, maintanance and deployment, it is sensible to build the services on top of general service network, which can be further mapped to different transport and access layers. This mapping can be performed via gateways or proxies. Also the services should be produced in a general way, where the access network independence is always in the designer's minds. Figure 2 depicts the idea of moving from vertical services to horizontal services.

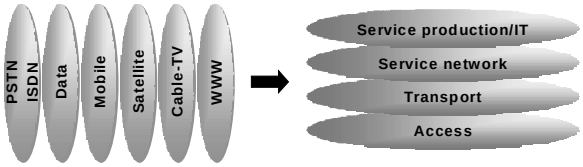

Figure 2. From vertical services to horizontal services. [1]

In order to work, the horizontal service concept must introduce user specific services. This means that the user must get a personalized view of the available services and must be able to change and modify the view and the content. Additionally the user expects an easily controlable and seamless user interface from the different access networks. From the network operator point of view the services should be built from general building blocks and the operator should be able to distribute the services across the IP network. The third party media servers, containing for example video and audio, should be easily connected to the service network. This means that the service control must be separated from the actual service as much as possible.

The service types can be roughly classified to transaction services and stream services. The transaction services are similar to the most of the current Internet services, in which the user continuosly interacts with the service application. The stream services, on the other hand, could tolerate or benefit from the separation of the service control and the actual service delivery.

4. SVPN ARCHITECTURE

The general requirements concerning the stream service control were closely taken into account, when the SVPN architecture was defined. One of the biggest requirements was to be able to separate the service ordering entity and the actual service end-point from each other. Other ideas behind the SVPN design were

- a simple control protocol (WAP/HTTP), which acts as a remote controller for the service system,
- a generic service architecture that provides the service interface to different access networks and enables the service control from different access networks,
- mobility in terms of users and services (content),
- centralized user and service control databases and distributed service databases,
- easy management for user and service provider,
- scalable and efficient SVPN architecture,
- IP protocol with secure interactions, and
- interesting and access network independent services.

The following Figure 3 illustrates the draft architecture for the SVPN (Service specific Virtual Private Network). The user and possible **media servers (MS)** are connected via IP core network to the operator's VPN network and thus logically to the SVPN. The **access server (ACS)**, which can be distributed to several servers, provides service interfaces towards the user. The access server is connected to the user and service **databases**, which contain information about the users, their locations, security contexts and services. The access server controls the service scheme according to the information it gets from its databases and from the user.

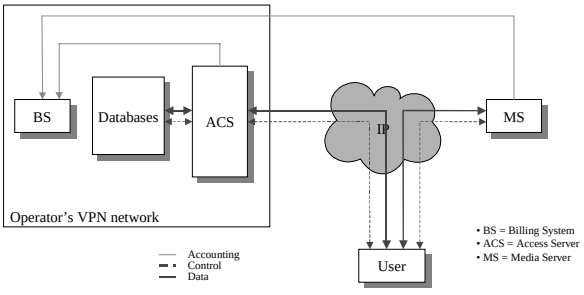

Figure 3. SVPN architecture.

The services can be launched from inside the operator's network and from the separate media servers. The media servers are normally used for services that require a lot of bandwidth and therefore must be implemented near the user (streaming services). MS takes care of the actual service (for example MS can send the ordered video stream to the user) and does not have much control for the service system.

The **billing system (BS)** collects and stores billing information from the services used by the client. This billing information is sent by the media server and the ACS after the service has been provided to the user.

4.1. Service control architecture

Figure 4 presents an overview of the service access architecture. The client consists of the *source entity* and *destination entity*. The source entity is the part of the client system that gives service commands to the server system. The client system contains HTTP- or WAP-client for that purpose. The destination entity is responsible for negotiating parameters with the server system. It also handles the data stream control together with the server system. The destination entity is located either in the same system as the source entity or it is implemented in a separate system. The destination entity contains normally commercial streaming capable software and a process that is able to start applications (e.g. stream application) in the destination client system.

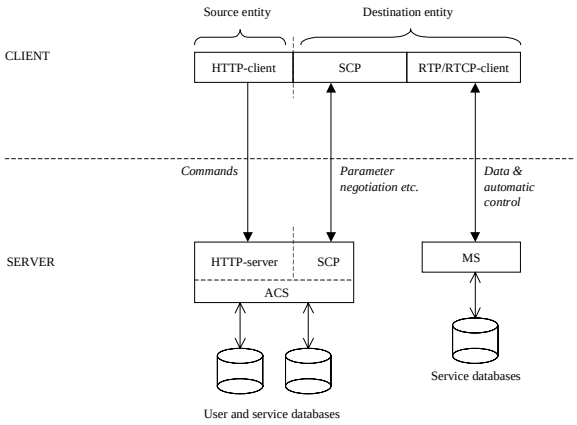

Figure 4. Service architecture between the user and the service provider.

The server side consists of access server (ACS) and media server (MS). Also a number of user and service databases are connected to these servers. The access server runs a HTTP-server and communicates with the client either via HTTP or service control protocol (SCP; proprietary protocol). The media server is a modified commercial server, which is capable of sending and controlling data streams.

Client's source entity
The client's source entity is responsible for the initial control of the service. For stream services, the client's source entity launches the service by contacting the access server and requesting a data stream service. In transaction type of services like browsing through web pages, the client's source entity is responsible totally for the service handling in the client's system.

Access server
The access server is responsible for taking requests from the clients through the HTTP server. According to those requests the ACS either serves the client directly or continues the service control chain by contacting the client's destination entity. In the latter case the service control parameters are negotiated between the ACS and the client's destination entity. The actual service and the service control in the ACS is based partly on the client's source entity input and partly on the information located in the ACS's user and service databases. The HTTP server side and the SCP side can be implemented on different systems.

Client's destination entity
The client's destination entity is logically and possibly physically separate unit from the client's source entity. The client's destination entity is responsible for service control parameter negotiation with the ACS, and receiving and controlling the actual service with the media server. It is also responsible for joining a specific multicast group, when the service uses multicast transmission.

Media server
The media server is responsible for sending data streams to the client's destination entity. It must also be able to control the data stream specific quality of service parameters according to the information received from the client's destination entity.

4.2. Advantages of using service control protocol between client and server

The service scenario presented in Figure 4 can be implemented without the service control protocol between the user and the server systems (then the service control logic is implemented between the access server and the media server). However, if we implement the service control protocol in the client's destination entity we can have the following advantages:

- We are able to start applications in the destination client system and instruct them to do the service initialization.
- The overall control of the service details, such as destination ports, is in the destination entity and the source entity does not have to know them beforehand.
- We have better possibilities to cope with the firewalls when the service is launched from the client's destination entity.
- This approach gives us the possibility to change the encoding keys between the destination entity of the client and the access server before the actual data stream transmission.
- Also other important parameters like possible bandwidth and delay parameters can be negotiated beforehand.
- By using the service control protocol the destination entity can deny the data transmission during the connection setup, if the data is considered hostile or originating from an unknown machine.
- Joining to the multicast transmission is possible because the join request is initialized from the client side (destination entity).

4.3. Message flow for stream type of services

The architecture defined in this paper allows us to use stream type of services where the destination system is separate from the source system. This is achieved by separating the source and destination entities in the client side in a way that they can be on another system. The source entity is a normal HTTP or WAP capable client (www-browser). The destination entity consists of an SCP application, which handles the service control protocol tasks towards the ACS and starts client applications based on the information it gets from the ACS. So, in a way the client applications (e.g. Real Player) are also included in the destination entity.
The server side consists of a media server and a service control protocol capable application in addition to the HTTP server and databases. The media server is normally separated from the ACS and therefore contains separate service databases. The message flows for the stream service is presented in Figure 5.

1. The client sends HTTP request for a specific service. The request contains all necessary parameters for that service.
2. The service is processed by the ACS's HTTP server, which queries the needed information for that service from the databases. The user parameters and security information can be checked before the request is processed further. Also information about the destination entity is queried from the databases if the user has not given it.

3. The ACS's service control protocol capable application negotiates about connection, security and other parameters with the destination entity of the client side. The destination entity can also refuse the connection set-up at this point.
4. According to the negotiated parameters, the client's service control logic starts a stream capable application.
5. The stream capable application connects to the media server and requests data. After that the client communicates periodically with the media server and informs the media server about the connection quality and other parameters.
6. The media server queries its databases and searches the stream to be sent to the client's destination entity.
7. The media server sends the data stream to the client's destination entity according to the specified parameters.

The message flow defined here for data streams may also be applied to the transaction type of services, when the destination entity is in a different system than the source entity.

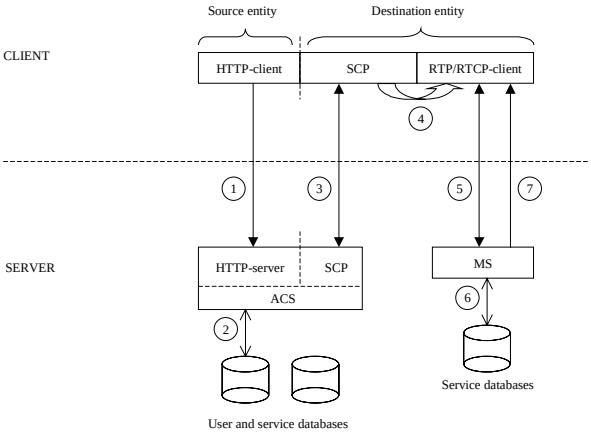

Figure 5. Stream type service – message flow.

5. CONTROL SYSTEM CHALLENGES

Before the SVPN concept can be successfully adapted to the service platform, we need to solve a number of problems related to service and client management, billing, security and access control. The recognized challenges in the above areas are introduced below.

5.1. Service management

The service management plays an important role in the SVPN concept, but it is not directly related to this service control architecture specified in this paper. The main function of the service management is to keep the service databases both in the ACS and MS up-to-date. Also the information between the databases must be synchronized properly and the management system must be aware of the chances in the database information.

The management system should provide an easy-to-use control system to manage the service information, and this is quite a challenge. The ACS service database must keep track of the media server's current location and files, encryption keys to different streams, possible data transfer rates, billing information, interface to client management databases etc. Because of the large amount of information to be stored, the databases must be distributed to several servers. This creates additional problems with security, efficiency and operation.

5.2. Client management

The client management and its properties can be separated to two different categories; user and device management.

User management

The user management differs from the device management in a way that it covers the user information and its relations to the services whereas the device management is related more or less to mobility management. The user management must keep track of users and their registered services. Before the user can use a certain service he/she must registrate first. The user management database contains information about the user parameters and the service parameters, so after a successful user authentication the registered services are available to the user. The SVPN supports user specific services and thus the ACS has to provide an efficient platform architecture to keep up with frequent database calls. The users must be also associated to the client devices in order to provide the services between different access networks and devices. This problem area is covered next in the device management subchapter.

Device management

The ACS's user database can contain information about the user equipment and their IP addresses. So when a user wants to order a service stream for example to his TV, he can just inform the ACS to send the data stream to the TV. The exact location (IP address) of the TV is fetched from the ACS's user database. In case where the address information is not available, the user must provide it. The problem with the information stored in the ACS's user database, is that it can be easily outdated without proper update procedure. In the registration phase the basic information of the user equipment can be installed to the user database. Later on the user can make manual changes to that information, but an automatic update procedure would be more than useful. The support for automatic update procedure can be implemented to

the SCP protocol. Then the client's destination entity running the SCP protocol must contact the ACS side for the updates.

5.3. Billing

The user and service control and the actual service data are separated across the IP backbone network. So the billing information related to the services must be collected from the media servers and the ACS separately. This can create problems, because the information can be different in those network elements. The ACS provides the billing information about the services that are agreed and ordered by the user. On the other hand the media server provides billing information about the services that are actually used. Different problems with the authentication, encryption and connectivity can cause that these two billing information sources have different billing data available. It is up to the billing system to handle this kind of differences.

Another problem with the billing comes from the idea that the control traffic should not be billed from the user, only the service. This is a serious problem when the access network is owned by a different service provider than the owner of the service system. The service providers must have an agreement how the access network usage can be paid to the other service provider. From the real life experiences it is easy to say that this is quite difficult if not impossible. If the same service provider manages both the access and the service system, it is possible to use a service based billing.

5.4. Security

Before the user is able to use SVPN services, he/she must be properly authenticated. The SVPN's authentication is performed with end-to-end principle between the user and the ACS. The authentication can be based for example on the digital signature on the GSM's SIM card received from the user and the ACS must compare it with the information in its user databases. In order to access the SVPN the user must thus registrate with the SVPN operator and change the authentication and also encryption keys. The registration can be performed either manually or on-line with the service provider. The problem with this kind of authentication is that we have to provide the interface to the authentication card in every equipment, independent of the access network. This means additional requirements to the user equipment. It must also be remembered, that even though we have this kind of authentication mechanism, we have to provide the username and password for every transaction to protect the user properly.

The control traffic within the SVPN should be always encrypted properly. Also the actual stream data sent by the MS should be encrypted. The negotiation procedure specified in the SCP must then provide the encryption key for the user, before the user connects to the MS. The encryption key can vary depending on the stream.

5.5. Access control

When the client's destination entity is a different system than the client's source entity and the service connection is intended to be established to the client's destination entity, which is behind either a firewall or NAT system, we must use special tricks to establish the SCP parameter negotiation and the actual stream connection.

Client's destination entity behind a firewall

The first problem with the firewalls is the SCP parameter negotiation connection. The connection is established by the ACS, so the connection request must be able to pass the firewall, which is between the ACS and client's destination entity. The SCP protocol must use a well-known port number and the firewalls should be configured to pass messages with that protocol number through. In addition to that the firewalls can be configured to pass the SCP messages only if the IP source address is known to belong to a trusted host (ACS).

The second problem comes into picture when the data stream is sent by the media server to the client's destination entity. If the client cannot be contacted by using a UDP based connection, the media server automatically tries to send the data stream by using a TCP based connection. If the streaming fails, the server switches to the HTTP streaming, which should be able to pass the firewall, because the HTTP connection is first established from the client's side. However, this problem should be solved by the vendors, who provide the stream applications.

Client's destination entity behind a NAT system

Another difficult area for this kind of service control and streaming are networks using network address translation (NAT), when communicating outside the private network. Usually those networks use private addressing inside the private network, which must be translated to the public addresses. This address translation hides the IP address of the client and the ACS is not able to initiate a connection to the client's destination entity. The address translation also makes the use of e.g. IPsec impossible.

A possible solution to this NAT problem is to use IP-in-IP encapsulation for the messages originating from the ACS. The outer IP header contains the NAT server's public IP address in the destination IP address field and the inner IP header contains the client's private IP address in the destination IP

address field. So the ACS must be aware of the both IP addresses before the SCP connection is established. The NAT server then strips the outer header off and forwards the inner datagram to the client's destination entity. The forwarding decision can be made based on the port number of the inner datagram in a way that the NAT server only forwards datagrams carrying SCP protocol. This mechanism thus does not use the NAT functionality at all. For all other connections initiated from the client the NAT is used. The Figure 6 presents the tunneling mechanism using IP-in-IP encapsulation.

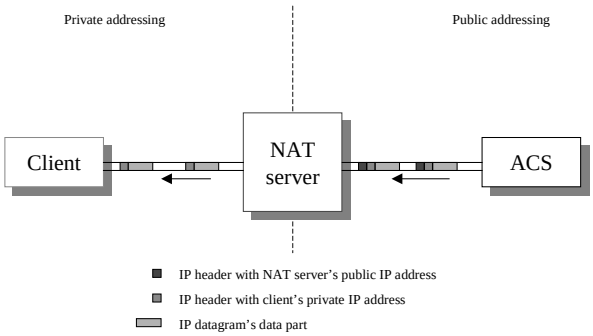

Figure 6. Client's destination entity behind a NAT system.

For the SCP messages, which are originated from the client's destination entity, the NAT server must not use NAT. Instead it should tunnel those datagrams to the ACS by using IP-in-IP encapsulation. The tunneling should be used in order to keep up the connection association in the ACS. The tunneling functionality between the ACS and NAT server is based on the SCP protocol and the trusted relationship between these entities.

5.6. Quality of service

In order to handle the QoS within the SVPN, we have to address the QoS problems individually for each access network. It is evident that the wireless media is more vulnerable than wired counterparts in terms of bandwidth, delay and bit error rate. However, we can increase the quality of the wireless links by introducing new QoS schemes and reservation algorithms to them.

The first version of UMTS/GPRS supports only best effort traffic but the next version should be able to use different classes of service [2]. The Bluetooth v.1.0 specification does not give direct QoS guarantees, but leaves the problem to the implementors of the Bluetooth products [3]. Some level of quality can be achieved by implementing the Bluetooth master with a QoS control block that can differentiate between Bluetooth slaves. Perhaps the next version of the Bluetooth standard comes along with the radio level QoS mappings. The WLAN does not provide any additional QoS than the other wireless access networks, even though the bandwidth within the WLAN is significantly bigger than what is available with the GPRS and Bluetooth. It must be also remembered, that before we can talk about end-to-end QoS, the core and the access network must both provide similar QoS properties to the data stream.

6. CONCLUSIONS

The high number of different access networks creates unwanted problems to the users in terms of mobility, identification and services. In the next generation networks the services should be defined so that the user can experience seamless connectivity within the different access networks. The SVPN control system introduced in this paper enables us to control data streams independent of the access network. It also gives us a possibility to control the data stream service from a different access network that the service itself uses. This is achieved by separating the service control entity from the entities involved in the service contents. In addition to the service control, the client and the service system can negotiate between various parameters. However, the SVPN concept introduces a bunch of problems related to user and device control, security, billing, access control and quality of service. To overcome these problems the SVPN control system as well as the server system must be further developed.

REFERENCES

[1] Eurescom P901, deliverable 1, "*Investment analysis Framework Definition and Requirements Specifications*", 1999.

[2] 3rd Generation Partnership Project, "*QoS Concept and Architecture (Release 1999)*", 2000.

[3] The Bluetooth Special Interest Group (SIG), "*Specification of the Bluetooth System*", Version 1.0 A, July 26th 1999.