IP Access Networks with QoS Support

Susana Sargento[a], Rui Valadas[b], Jorge Gonçalves[c], Henrique Sousa[d]

[a,b]University of Aveiro/Institute of Telecommunications, 3810 Aveiro, Portugal
[c]Portugal Telecom Inovação, 3810 Aveiro, Portugal
[d]Institute of Telecommunications, 3810 Aveiro, Portugal

ABSTRACT

The increasing demand of new services and applications is pushing for drastic changes on the design of access networks targeted mainly for residential and SOHO users. Future access networks will provide full service integration (including multimedia), resource sharing at the packet level and QoS support. It is expected that using IP as the base technology, the ideal plug-and-play scenario, where the management actions of the access network operator are kept to a minimum, will be achieved easily. This paper proposes an architecture for access networks based on layer 2 or layer 3 multiplexers that allows a number of simplifications in the network elements and protocols (e.g. in the routing and addressing functions). We discuss two possible steps in the evolution of access networks towards a more efficient support of IP based services. The first one still provides no QoS support and was designed with the goal of reusing as much as possible current technologies; it is based on tunneling to transport PPP sessions. The second one introduces QoS support through the use of emerging technologies and protocols. We illustrate the different phases of a multimedia Internet access session, when using SIP for session initiation, COPS for the management of QoS policies including the AAA functions and RSVP for resource reservation.

Keywords: Access Networks, QoS, Admission Control, Protocol Design

1. INTRODUCTION

The exponential growth of the Internet is pushing for a migration towards IP based access networks capable of supporting multiple services with different QoS requirements. Presently, Internet access is mainly dominated by dial-up connections. In the incumbent traditional telecommunications operator, a more advanced solution that combines the use of ATM and xDSL technologies supported on copper or copper and fiber, is also being deployed. These solutions provide only for limited resource sharing in the access network, since service separation is achieved through reserved bandwidth circuits. Moreover, since ATM is a connection-oriented technology, it complicates the management of access networks, due to the need to establish and manage virtual circuits. This problem is aggravated if on-demand resources are required (i.e., when using VB5.2). It is expected that using IP as the base technology in access networks, the ideal plug-and-play scenario, where the management actions of the access network operator are kept to a minimum, will be achieved easily. However, migration towards IP based access networks has to be done smoothly, reusing as much as possible current technologies. We also note that, a major factor to be taken into account in the design of any access network is the cost of the network elements and of the signaling functions.

This paper proposes an architecture for IP access networks with QoS support, targeted for both residential and SOHO users. In section 2, we give an overview of the evolution of access networks, focusing mainly the Internet access service. In section 3, we propose a solution for IP access networks without QoS support. In section 4, we discuss the main issues related with the introduction of QoS in IP access networks.

2. ACCESS NETWORKS EVOLUTION

Access networks most commonly used nowadays are supported on cooper pairs connecting user equipment to the local exchange (LE). In a dial-up access to the Internet (Figure 1), a circuit is established between the user and an Access Server (AS) via the PSTN. User interfaces can be analog or digital (ISDN). The AS implements the Point-of-Presence (PoP) of the Internet Service Provider (ISP). As a commercial strategy, the AS can be replaced by a Network Access Server (NAS) with wholesale capability, which can provide access to several ISPs simultaneously.

In a dial-up access, a fixed bandwidth is allocated to the user during the whole Internet access session. Given that the duration of a typical Internet access session is much longer than that of a phone call, the Internet access service places a

[a]e-mail: susana@av.it.pt; [b]e-mail: rv@det.ua.pt; [c]e-mail: jgoncal@ptinovacao.pt ; [d]e-mail: tsousa@av.it.pt

strong demand on the resources of the PSTN. Therefore, the AS (or NAS) should be placed as close as possible to the local exchange.

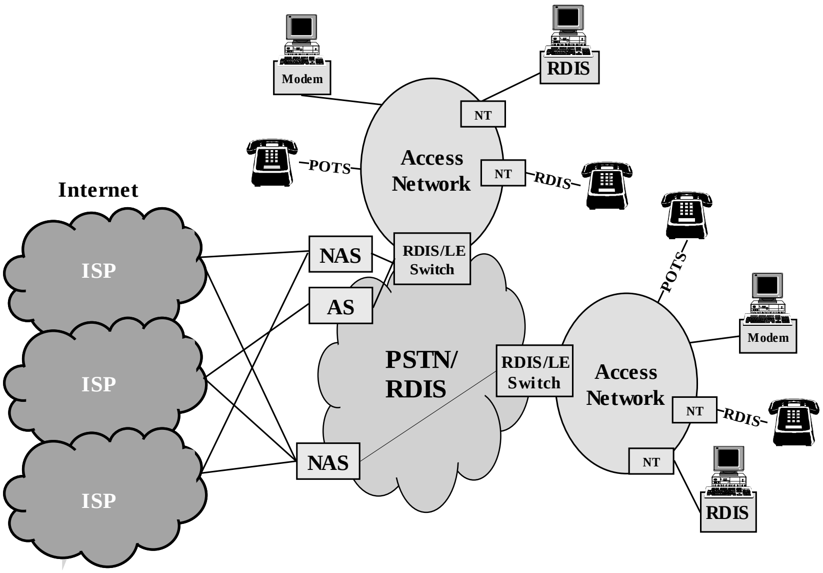

Figure 1. Dial-up access.

In previous scenario, narrowband analog or digital circuits support the connection to the ISP, which is not compatible with the requirements of emerging broadband services. We start by noting that most broadband services are asymmetric, with the downstream traffic occupying more bandwidth. Taking into account this asymmetry, it was possible to evolve from copper access networks towards broadband access networks using Asymmetric Digital Subscriber Line (ADSL) technology. The star topology can be maintained with point-to-point copper connections from the Digital Subscriber Line Access Multiplexer (DSLAM) to each user terminal. The broadband traffic is supported by ATM connections over ADSL between the user ATU-R and the DSLAM, which aggregates several ADSL accesses. Internet traffic is routed to the Broadband Access Server (BAS) through Asynchronous Transfer Mode (ATM) connections and the voice traffic to the PSTN local exchange. In the DSLAM there is a splitter that separates the IP and voice traffic through frequency multiplexing. The BAS is the interface element between the access network and the IP core network. It distributes the traffic to different ISPs, authenticates the user and allows the terminal to choose an ISP.

In a star topology with point-to-point copper connections, ADSL allows an immediate solution for broadband service support. However, there is a scale problem since the distances involved impose a larger limitation on the number of ADSL connections per copper cable. SDH rings are now installed and being installed in the access network carrying basically narrowband traffic but paving the way to broadband traffic support. Last mile connections between users and SDH ring add-drops are supported by xDSL for broadband services. Typically, these copper connections are much shorter than those of the star topology. Cable TV distribution networks already installed and updated with upstream connectivity are also able to support broadband traffic.

In greenfield installations the use of very large service access nodes will allow the enlargement of the access network. This can justify an access network architecture based on a primary SDH ring and secondary SDH rings connected to the primary ring. PONs are an alternative solution to the secondary SDH rings. Last mile connections for residential and SOHO users, will be supported on xDSL over copper, with the possibility of extensive deployment of VDSL. Business users can be connected directly to the primary ring by SDH fiber connections.

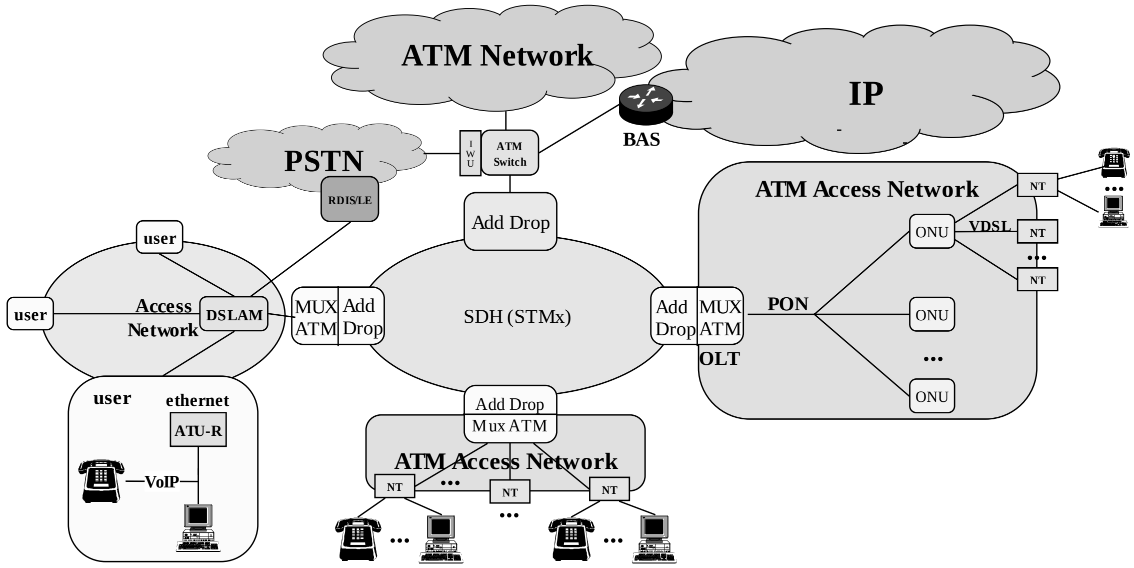

Figure 2. ATM based access networks.

Since ATM is a connection-oriented technology, it complicates the management of access networks, especially in the case of on-demand resource reservation. The creation, management and termination of virtual circuits in the access network requires the VB5.2 signaling protocol, which is extremely complex and involves much functionality on all network elements. Also, it is expected that IP traffic will soon become dominant in access networks. The transport of IP over ATM is the solution adopted today but has a high overhead. For the future, a more attractive solution can be IP over SDH or even IP over fiber. Thus our goal is to propose an IP access network that provides service integration and full resource sharing and supports, at the same time, QoS assurance and differentiation as required by future multimedia services.

3. OVERVIEW OF THE PROPOSED SOLUTIONS

Figure 3 shows the network elements of the proposed IP access network. We assume that the user can be either a single terminal or a Local Area Network (LAN). The Network Termination (NT) performs the adaptation between the user interface and the access network. Traffic from different NTs is aggregated into multiplexers (MUXs) and there can be several stages of multiplexing. The BAS interfaces the access network and the ISP. It can include several functions such as acting as an AAA proxy of the ISP or allowing the terminal to choose an ISP.

We consider two possible scenarios: (i) access network based on layer 2 technology (Ethernet); (ii) access network based on layer 3 technology. In the first scenario, the access network works like a switched Ethernet network, where the MUXs are layer 2 devices (Ethernet switches), the NTs are layer 2 (bridge) or layer 3 (router) devices and the BAS performs layer 3 functions. In the second scenario, all of them implement layer 3 capabilities.

There are several options for the interfaces between the network elements. The interface between NTs and MUXs can be xDSL (x Digital Subscriber Line) or FTTH (Fiber To The Home). The interface between MUXs or between a MUX and the BAS can be SDH (Synchronous Digital Hierarchy). IP over fiber is an expected target in medium-long term.

An important feature of the proposal is the use of layer 2 or layer 3 MUXs. We believe that access networks can rely on physical layer redundancy as it happens in SDH rings. Therefore, from the point of view of these layers, the access network is a logical tree. Logical tree architectures simplify a number of functions like routing and addressing.

Since the network is a logical tree, traffic can be forwarded in the upstream direction without the need of any routing information. The BAS and the MUXs need only to maintain routing tables for forwarding traffic in the downstream direction. The maintenance of these tables only requires reachability information to be advertised in the upstream direction. No routing metrics need to be involved since there is a single path between the BAS and each possible destination. The routing tables will be inexpensive since, for a given element (MUX or BAS), only entries for networks or hosts that are downstream reachable from that element need to be included. In case of layer 2 switches (first scenario), routing tables are typically maintained through a learning process. One advantage is that no routing protocol is needed. The disadvantages are

(i) the need for flooding information when the destination host is not listed in the routing tables, and the increased size of the routing tables since they include an entry per host. However, due to the topology of the access network flooding will only exist in the downstream direction. In case of layer 3 elements (second scenario), the routing function can be implemented with a simplified version of a distance vector protocol such as RIP (or RIPv6). In this case, simplification is explained by the absence of the count-to-infinity problem that complicates distance vectors protocols and also by the fact that the routing metrics need not to be involved. The addressing inside the access network is also considerably simplified. First, there is no need to assign an IP address to each interface; only a single IP address is required in each network element to support the operation of the routing protocol. Second, since there is no need to make these addresses known to external networks (nor it is desirable for security reasons), the addresses can be private. With layer 2 elements the addressing is of no concern since addresses are pre-assigned by manufacturers.

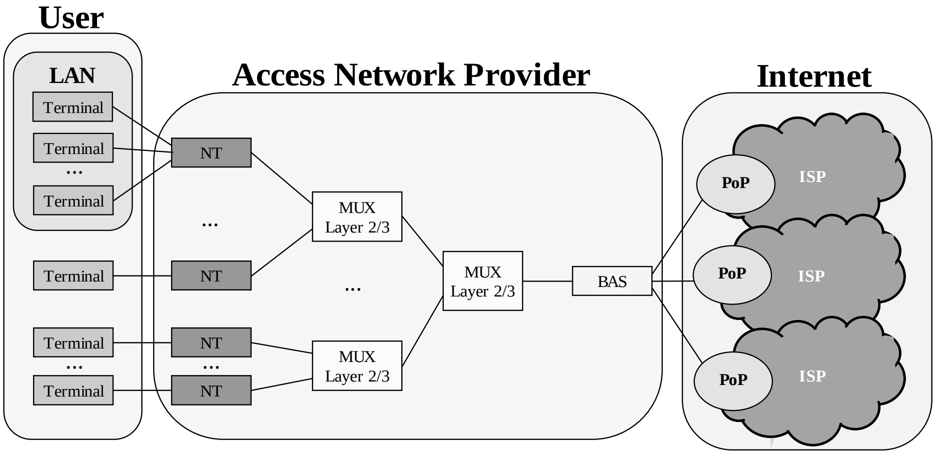

Figure 3. IP based access network.

4. IP ACCESS NETWORKS WITHOUT QOS SUPPORT

One intermediate step towards IP access networks with QoS support can be the evolution to access networks based on layer 2 or layer 3 switching but still with no QoS support. In this section we will describe solutions for this intermediate step that were designed with the goal of reusing as much as possible existing technologies.

Dial-up access to the Internet is based on the Point-to-Point Protocol (PPP). It comprises the following steps: establishing a call to the ISP, Authentication, Authorization and Accounting (AAA) of the user, and assignment of an IP address to the user terminal. The PPP protocol assumes that there is a point-to-point circuit end-to-end. It cannot be used directly in a network with routers or switches. In the case, a tunneling protocol is required. The tunneling protocol mainly used in layer 3 networks is the Layer 2 Tunneling Protocol (L2TP)[1], and in layer 2 networks is the Point-to-Point Protocol over Ethernet (PPPoE)[2]. Between the BAS and ISPs we may need to have again L2TP in order to forward the PPP session towards the selected ISP. The ISP selection can be done using the login string in a PPP authorization phase. When the BAS has a full wholesale capability, the PPP session ends at the BAS, which assigns IP addresses, and the access network provider needs a RADIUS Proxy to perform some AAA functions on behalf of ISPs. In both scenarios, we will study the possibility of initiating PPP sessions in user terminals or in the NT.

4.1 ACCESS NETWORK BASED ON LAYER 2 TECHNOLOGY

In the case of layer 2 access networks, the user initiating the PPP session needs to discover the Ethernet MAC address of the BAS so that the PPP messages can be routed in the access network. This is possible, using the PPPoE protocol. After this process, the different PPP phases can start. In this solution, for users that only have a terminal, the entire access network is considered an extended LAN where terminals are connected to the access network via bridges. MAC frames will transport PPP frames transparently from the user terminal to the BAS.

For users that have their own LAN, the NT may be a router and, in this case, PPP sessions may start in user terminals or in the NT.

a) PPP sessions initiated in user terminals

In this solution PPPoE needs to be supported inside the users' LAN (assuming Ethernet), and in the access network between the NT and the BAS. A user PPP session is carried, first, over a PPPoE tunnel inside the users' LAN and, second, using a PPPoE tunnel in the access network. Several sessions may be established at the same time to different ISPs.

b) PPP sessions initiated in the NT

In this solution (Figure 4) NAT is used in the NT. PPPoE is used only in the access network to provide a tunnel between the NT and the BAS. PPP sessions can be established dynamically as required, when the NT detects a new IP destination, or can be established at NT power-up. The user terminal has no capability to select the ISP.

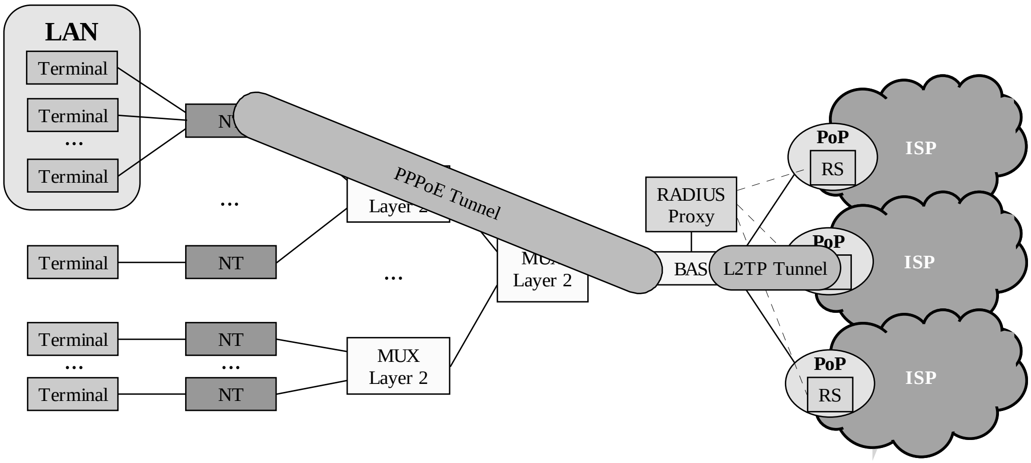

Figure 4. PPPoE and L2TP tunnels.

4.2 ACCESS NETWORK BASED ON LAYER 3 TECHNOLOGY

We consider the access network to be a private IP domain. Therefore, NTs, MUXs and BAS will be assigned private IP addresses. We restrict our attention to IPv4. These addresses will support L2TP tunnels multiplexing PPP sessions between BAS and NTs or IP tunnels for the transport of one PPP session in conjunction with a specific process located in a transport address of the endpoints. This new process is only justified if it can be optimized for the transport of a single PPP session.

As in previous scenario, we will discuss two cases: a) PPP sessions initiated in user terminals; b) PPP sessions initiated in the NT.

a) PPP sessions initiated in user terminals

In this case, the best way to transport PPP sessions from user terminals towards the BAS is having PPPoE from the LAN to the NT, assuming that Ethernet is used, and then using L2TP from the NT to the BAS . This solution is extremely complex in terms of tunnel software requirements and tunnel control, establishment and management. However, NAT is not necessary in the NT.

b) PPP sessions initiated in the NT

This case is similar to the one studied in previous scenario. However instead of using PPPoE in the access network, L2TP is needed to establish tunnels between the NT and the BAS (Figure 5). Therefore NAT is again required on the NT. Also PPP sessions can be established dynamically or at NT power-up. In the former case a one-to-one NAT translation may be implemented. Whenever a new session is requested, if there is no available IP address in the NT, the NT establishes a new PPP session and a new public IP address is assigned to it. The NT will then translate this IP address to the private IP address of the user. The advantage of this solution is the simplicity of the NAT, since it only has to translate one public IP address to a private one. The disadvantage is that more IP addresses are assigned to the NT and the cost may increase.

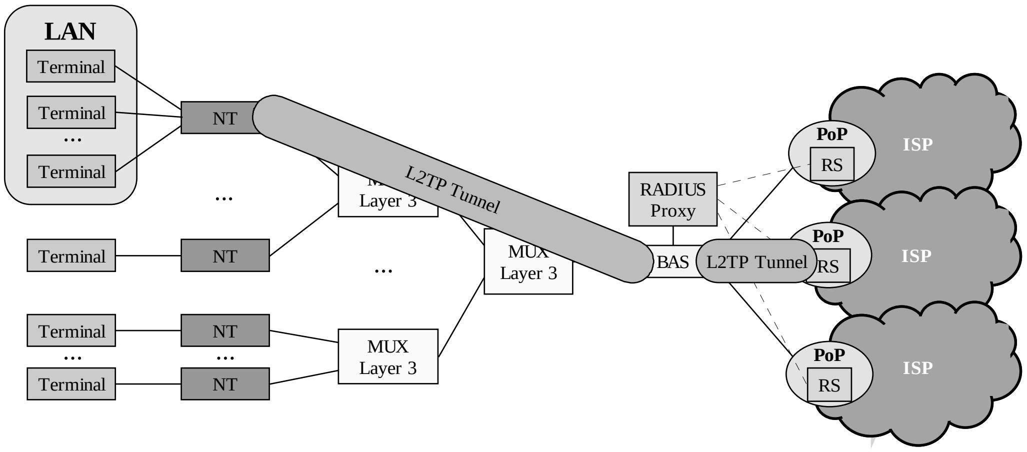

Figure 5. L2TP tunnels.

As an overview, the overall sequence of actions will be: (1) the NT initiates an L2TP tunnel (over the local IP) to the BAS; or the BAS may have a pre-established L2TP tunnel to the ISP; (2) the NT initiates PPP sessions to the ISP through the BAS; (3) if the BAS has a full wholesale capability it accepts or not the session (through the RADIUS proxy server); otherwise the PPP frame is forwarded to the ISP using the corresponding L2TP tunnel; (4) if the session is accepted, one public IP address is assigned to the NT; (5) the end-to-end data is then carried on the PPP session, multiplexed on L2TP tunnels with other PPP sessions.

4.3 DISCUSSION OF THE L2TP AND PPPOE SOLUTIONS AND QOS SUPPORT EXTENSIONS

The solutions described above are not simple to implement. The support of PPP requires the use of tunneling protocols. Tunneling introduces several problems: the need for specific software in the user terminals, the NTs and the BAS to create and manage the tunnels, the use of NAT, and the packets overhead. In terms of overhead the PPPoE solutions are less expensive. These solutions seem preferable and are available today for ADSL solutions.

Both tunneling solutions could be extended to provide limited QoS support. L2TP and PPPoE tunnels can carry QoS information in the packets, so that they can be recognized and differentiated by the network elements. L2TP tunnel encapsulation specifications using IP as the tunnel substrate, typically map the clear channel QoS fields of the IP header into the QoS fields of the tunnel IP header[3], allowing the tunnel to be supported in a semitransparent mode, where the tunnel path attempts to handle tunneled packets using QoS mechanisms activated indirectly by the encapsulated packet. In this scenario the QoS bits should always remain the same and both ends of the connection should use the same QoS settings. Moreover only the sessions with the same QoS requirements can be multiplexed in the same tunnel. In PPPoE the IEEE 802.1P/Q tag can be added to the Ethernet frame header. The Type of Service (ToS) or Priority (IPv6) values of the IP packet can be mapped in the priority bits of the tag. One important mechanism that is also required is the call admission one. As an example, if the RSVP protocol[4] is used to reserve resources, the RSVP messages must be synchronized with the end of the tunnel establishment and the beginning of the data transmission. Thus PPP and L2TP/PPPoE must be extended to wait for the resources reservation phase before starting to transmit the information.

The extension of these solutions to QoS support has some limitations. First the packet ToS/Priority values cannot be changed by a router/switch in the network between the origin and destination. Second, all the domains must be aware of it and use the same QoS settings, which is difficult since each domain has a different administration. Third and last, the admission control must be synchronized with PPP and L2TP/PPPoE. There is no guarantee that this third limitation can be solved. In next section we will propose and study a different solution that will overcome these problems.

5. IP ACCESS NETWORKS WITH QOS SUPPORT

A multi-service access network with QoS support requires a number of additional functions: packet classification, isolation scheduling and policing (while maintaining a high resource utilization) and call admission.

The signaling protocol for resource reservation is of major concern. RSVP[4] has been widely used in the context of the IntServ architecture[5]. Reservations are established and maintained on a per-flow basis. Flow admission requires the intervention of every router along the path between source and destination. The path itself is established and maintained by an independent routing protocol. Thus, it is necessary to maintain a flow state in each router and the signaling load is relatively high. The number of RSVP messages processed is proportional to the number of flows in the network. These disadvantages can lead to poor router performance.

To overcome the scalability problems of InterServ, the DiffServ architecture was proposed[6]. In DiffServ, flows are aggregated in classes according to specific characteristics. Recently it has been proposed an extension of RSVP for the support of signaling in the DiffServ architecture[7]. This extension brings the possibility of aggregating several end-to-end RSVP reservations. Call admission is only performed on an aggregated set of flows and therefore core routers need only to maintain the reservation state of each aggregate. The reserved aggregate bandwidth can be adjusted dynamically using this RSVP extension. Only the ingress and egress routers (NTs and BAS in our case) need to maintain the flow reservation state. The routers inside the network (the MUXs) maintain only the aggregate state. The protocol field in the IP header of RSVP messages is RSVP-E2E-IGNORE instead of RSVP. Therefore end-to-end RSVP messages are hidden from the MUXs. However the MUXs still need to be RSVP aware to perform reservations of flow aggregates.

We argue that since RSVP is a widely deployed protocol and since most multimedia applications are being developed assuming RSVP as the resource reservation protocol, the support of RSVP in the access network is almost inevitable, in the sense that all network elements need to be RSVP aware. Then RSVP can come into two flavors, which can co-exist in the same access network: Int-Serv RSVP or DiffServ RSVP. The latter requires less signaling in the access network and lowers state maintenance at the MUXs. The former allows resource reservation on a per flow basis. The exact trade-off between cost and performance can be left to the access network operator.

In a multi-service network with QoS support, the PPP apparatus is not suited for session initiation and AAA. The IETF defined a new signaling protocol, the Session Initiation Protocol (SIP)[13], to provide session initiation over the Internet. This protocol was first designed for Voice over IP and it is now being extended to other multimedia services. SIP was developed to setup, modify and teardown multimedia sessions over the Internet. To use SIP each user must be a SIP-enabled end-device. We call these users SIP User Agents (UA). With SIP, the resource reservation information is embedded into the session description, which has the advantage that it can become part of the negotiation. Thus, in the authentication phase the required resources for the service are already known.

The SIP message that starts the session setup is the INVITE message. A SIP URL is inserted in the message and is used for routing the request. The SIP URL is a name that is resolved to an IP address by using SIP proxy server and DNS lookups at the time of the call. The IP address of the proxy server that handles the UA domain is retrieved through DNS lookup. There are several possible responses to the SIP INVITE. We will only refer those that will be used later: 180 Ringing, 183 Session Progress and Success 200 OK. The 180 Ringing indicates that the called party has received the INVITE message and that alerting is taken place. The 183 Session Progress response indicates that information about the progress of the session is present in the message body media information. The Success 200 OK accepts a session and has a message body containing the media properties of the called party. After receiving the Success 200 OK, the session initiator acknowledges its reception with an ACK message. The completion of a SIP session is performed by sending a SIP BYE message.

A multi-service network with QoS places additional requirements in the AAA functionality. These functions need now to be performed on a user / service / QoS level basis. The following sentence illustrates some of the constraints that need to be accounted for when authenticating a user: “Provide the JitterFreeMPEG2 video service for authorized users between authorized points, but only at agreed-upon times”[9]. DIAMETER[10] is one AAA protocol that already supports QoS.

The current trend is to include the AAA functionality under the scope of a QoS policy management framework[8] (Figure 6). COPS[11] is the protocol used to exchange information between a Policy Decision Point (PDP) and a Policy Enforcement Point (PEP). The PEP is the element that enforces the policy decisions, and the PDP makes decisions based on the policies it retrieves from policy repositories, authentication servers and other entities. The policy repository is a remote database such as a directory service or a network file system. The PEP is a component of a network node and the PDP is a remote entity that may reside at a policy server. Usually there is a PDP in a network domain and several PEPs. The PDP may make use of additional mechanisms and protocols to achieve additional functionalities (user authentication, accounting, policy information storage, etc.). To exchange information with the policy repository, for storage and retrieval of policy information, the PDP uses the Lightweight Directory Access Protocol (LDAP)[12] protocol. The interaction between the PEP and PDP works as follows. The PEP receives a message that requires a policy decision. It then formulates an event for a policy decision and sends a COPS request message to the PDP. The request for policy control from a PEP may contain one or more policy elements. An example of a policy element is the authentication data. The PDP returns the policy decision in a COPS decision message specifying what action the PEP should take. The PEP then enforces the policy decision by appropriately accepting or denying the request.

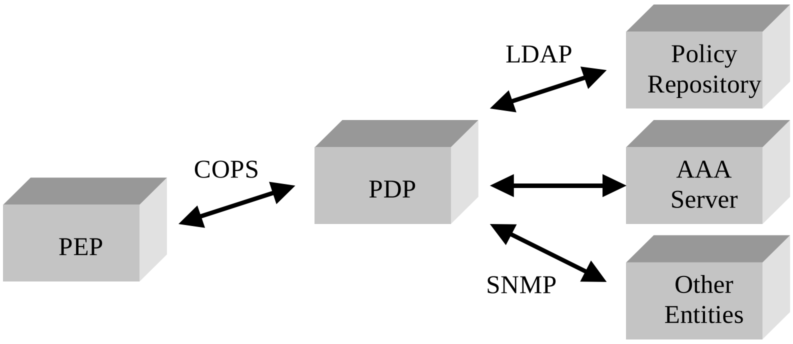

Figure 6. Policy framework using COPS.

A very important COPS facility is that it provides the download to the network devices of the QoS configurations. The PDP does not need to know anything about device interfaces. It simply knows that a device uses a certain set of roles, and then pushes those roles' policies to the device. The QoS policy configurations include the mechanisms for packet classification, the definition of the rate limits in the shapers, the definition of the service classes (in the case of a DiffServ network) and excess actions for out-of-profile traffic, and the scheduling mechanisms and drop preferences to be applied to packets according to their classification.

The PEP notifies its PDP of all events that require a policy decision. Thus, the PDP is a logical aggregation point for monitoring network activity. Moreover, COPS allows a PEP to asynchronously send report messages associated with a specific request to the PDP. These messages enable the PEP to provide the PDP with accounting and monitoring information regarding an existing request state.

In the following we will present a solution that is based on SIP for session initiation, RSVP for resource reservation, and COPS for the control of QoS policies including AAA.

In Figure 7 we show the software elements required in each network element and delimit the responsibility of each entity: the user, the network provider and the ISP. We assume that all network elements are layer 3 devices. All elements need to be RSVP aware. The users must be SIP-enabled. The COPS protocol must also be supported. However, the PEPs in the NTs and MUXs only need to support the download of the policy rules. To simplify the figure, the policy repository is not represented. Clearly other technologies could be considered for the support of some of these functions.

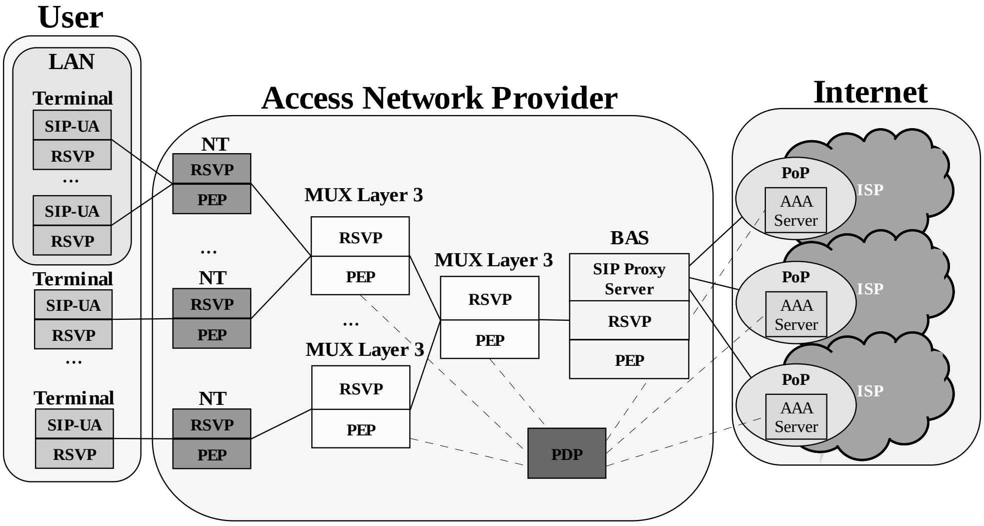

Figure 7. Required elements with SIP, COPS and RSVP.

In Ref. 15 two different scenarios concerning the interaction between call setup and QoS setup are defined: QoS assured and QoS enabled calls. In QoS assured calls the SIP call setup is coupled and synchronized with the QoS setup. In this scenario the caller will not receive a 180 Ringing, indicating that the call may start, unless the reservation has been successfully setup. This type of service is equivalent to present circuit switched telephony. Call setup time is longer due to the dependency on QoS setup time. In QoS enabled calls the SIP call setup and QoS setup are decoupled and may proceed concurrently. In case of QoS setup failure, the caller can be notified and given the option of continuing the call with best effort service only. Call setup is shorter and the best effort call may still be useful to the end user.

Figure 8 shows the messages that need to be exchanged in a QoS assured calls scenario. In the example, we only show the messages exchanged in the access network, i.e., between the session initiator and the ISP. Note however that the ISP is also communicating with the called user. Also, we will consider resource reservation to be bi-directional. Both end-users are senders and receivers.

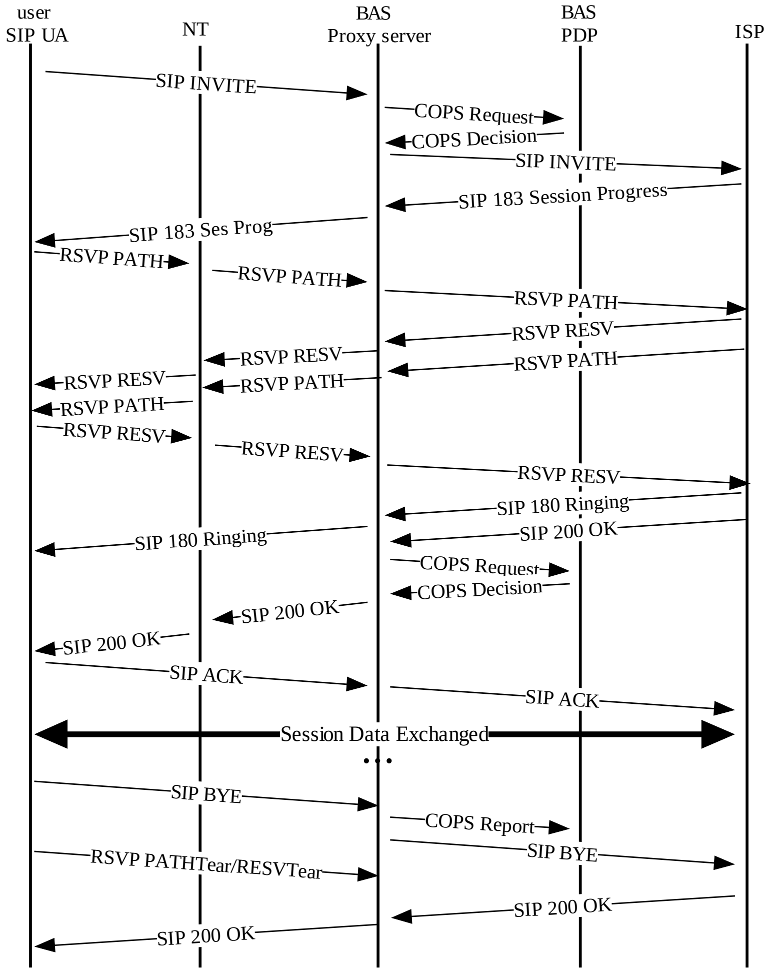

Figure 8. Timing diagram of a multimedia Internet access session, with SIP, COPS and RSVP.

When a user requests a service it sends an INVITE message towards the destination. The Proxy server captures the INVITE message and sends a COPS message to the PDP to perform AAA functions. The message contents sent to the PDP are the source, destination, SIP call identifier and possibly the media information and the amount of bandwidth requested. All these contents must be present in the SIP INVITE message[13]. Also, in the INVITE message there is information concerning the requirement of a reservation process, and in the case where several protocols for reservation are available in the network, they are indicated in the INVITE message. After receiving a positive AAA answer, the INVITE message is forwarded to the destination. A SIP 183 message is sent to the user with the IP address of the remote peer and indication of the session's progress. Now, the RSVP process starts through the exchange of PATH and RESV messages between the sender and receiver[14]. We assume the use of RSVP both in IntServ and DiffServ architectures. In DiffServ architectures the elements between the NT and the BAS only perform per class admission and state storage. Per flow functions are only performed in the NTs and BAS, as explained above. Upon a successful RSVP process, a success message (SIP 200 OK) is sent to the session initiator. The BAS, through the proxy server, upon receiving the success message exchanges COPS messages with the PDP to update any changes in the session information and start the accounting functions. In this solution, all packet flows cross the BAS, even if the calls are between end-users in the same access network. Therefore, the only required element to exchange accounting information with the PDP is the BAS. Upon the SIP ACK message, the session data can be exchanged between the two peers.

The RSVP messages in the two directions may overlap and there is no specified sequence. The case we described is a scenario with DiffServ architecture. In an IntServ architecture, the RSVP messages do not go transparently from the NT to the BAS, but need to be processed in the MUXs.

An alternative to the previous solution to perform both AAA and reservation functions could be the use of the COPS-RSVP protocol. COPS-RSVP can be used to condition acceptance at a network element based on AAA. However, it is still required a signaling protocol to initiate and configure the session.

In the case of a simple Internet access without QoS requirements, i.e., using a best-effort service, no RSVP reservation is required. However, the user must still be authenticated to make sure that it can access the service. COPS policy and monitoring is required to provide these functions. Also, a signaling protocol is required to trigger the COPS, to configure the session and to assign an IP address to the user in the case of IPv4 protocol. The INVITE message contains the information of the type best-effort to be assigned to the service requested from the user. The time diagram is similar to that of Figure 8 without the reservation messages. In case of semi-permanent reserved bandwidth connections between the ISP and the user, SIP is not required. The QoS policy rules for this reserved bandwidth are configured manually or through COPS download. Both the shapers of the NT and BAS, respectively in the upstream and downstream directions, must be configured with a rate equal to the reserved bandwidth. This is an additional functionality required in a network that supports semi-permanent connections.

Finally, note that there is the need to reserve bandwidth for the signaling messages. Also it is required to associate a shaper with this reserved bandwidth to prevent malicious users from sending excessive signaling messages to the network.

6. CONCLUSIONS

This paper proposed an architecture for access networks that is based on layer 2 or layer 3 multiplexers, which allows a number of simplifications in the network elements and protocols (e.g. the routing and addressing functions). We discussed two possible steps in the evolution of access networks towards a more efficient support of IP based services. The first one still provides no QoS support and was designed with the goal of reusing as much as possible current technologies; it is based L2TP and PPPoE tunneling for the transport of PPP sessions. The second one introduces QoS support through the use of emerging technologies and protocols. We illustrate the different phases of a multimedia Internet access session, when using SIP for session initiation, COPS for the management of QoS policies including the AAA functions and RSVP for resource reservation.

7. ACKNOWLEDGEMENTS

This work was partially funded by Portugal Telecom Inovação. Susana Sargento wishes to thank Fundação para a Ciência e a Tecnologia, Portugal, for support under grant BD/15678/98.

8. REFERENCES

1. W. Townsley et al., “Layer Two Tunneling Protocol, L2TP”, RFC 2661, August 1999.
2. L. Mamakos et al., “A Method for Transmitting PPP Over Ethernet (PPPoE)”, RFC 2516, February 1999.
3. Internet Page, http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/qsvpn_wp.htm.
4. R. Braden et al., “Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification”, RFC 2205, September 1997.
5. R. Braden et al., “Integrated Services in the Internet Architecture: an Overview”, Internet RFC 1633, June 1994.
6. S. Blake et al., “An Architecture for Differentiated Services”, RFC 2475, December 1998.
7. F. Baker et al., “Aggregation of RSVP for IPv4 and IPv6 Reservations”, Internet Draft draft-ietf-issll-rsvp-aggr-02.txt, March 2000.
8. R. Yavatkar, “A Framework for Policy-Admission Control”, RFC 2753, January 2000.

9. QoSForum, “Introduction to QoS Policies”, White Paper, 1998.
10. P. Calhoun et al., “Diameter Base Protocol”, Internet Draft draft-ietf-aaa-diameter-03.txt, May 2001.
11. D. Durhan et al., “The COPS (Common Open Policy Service) Protocol”, RFC 2748, January 2000.
12. M. Wahl et al., “Lightweight Directory Access Protocol (v3)”, RFC 2251, December 1997.
13. M. Handley et al., “SIP: Session Initiation Protocol”, RFC 2543, March 1999.
14. H. Schulzrinne et al., “Interaction of Call Setup and Resource Reservation Protocols in Internet Telephony”, Technical Report, June 1999.
15. H. Sinnreich et al., “AAA usage for IP Telephony with QoS”, Internet Draft draft-sinnreich-aaa-interdomain-sip-qos-osp-00.txt, January 2001.