IP-Based Access Networks for Broadband Multimedia Services

Susana Sargento and Rui Valadas, University of Aveiro and Institute of Telecommunications

Jorge Gonçalves, Portugal Telecom Inovação and Institute of Telecommunications

Henrique Sousa, Institute of Telecommunications

ABSTRACT

The increasing demands of new services and applications are pushing for drastic changes in the design of access networks for residential and SOHO users. Future access networks will provide full service integration, 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. In this article we start by giving a historical perspective of the evolution of access networks. We then describe an IP-based architecture targeted for integrated support of broadband multimedia services, designed to be low-cost and easily manageable. We illustrate the different phases of a multimedia Internet access session, when using SIP for session initiation, COPS and DIAMETER for QoS policy management, and AAA and RSVP for resource reservation.

INTRODUCTION

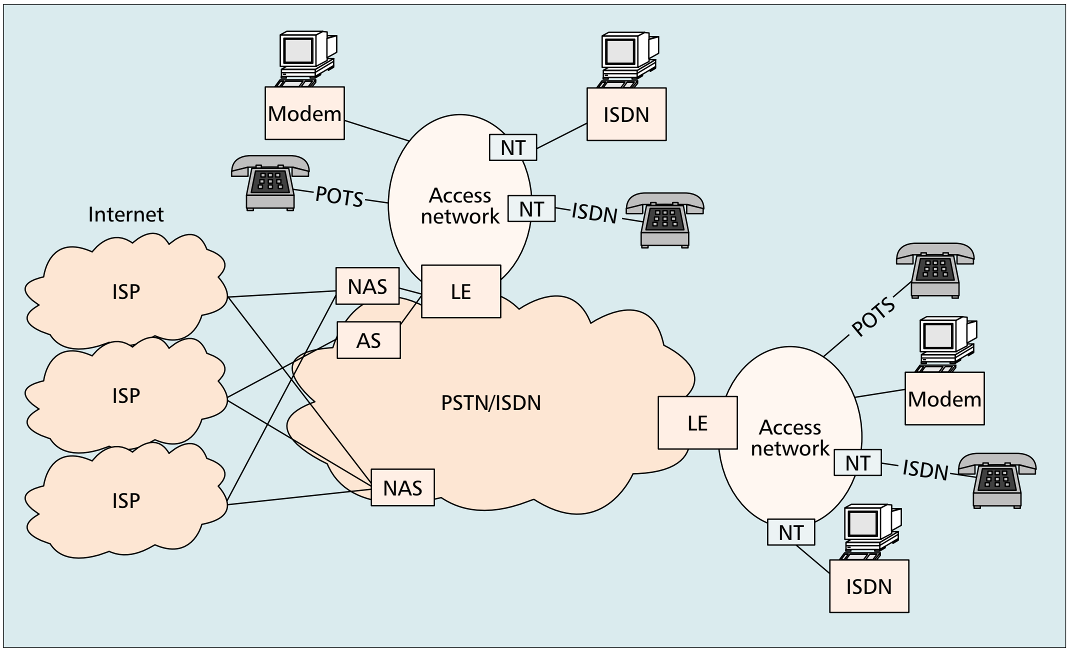
The exponential growth of the Internet is pushing for a migration to IP-based access networks capable of supporting multiple services with different quality of service (QoS) requirements. Presently, Internet access is mainly dominated by dialup connections. In the traditional incumbent telecommunications operator, a more advanced solution that combines the use of asynchronous transfer mode (ATM) and digital subscriber line (xDSL) technologies, supported on copper or copper and fiber, is also being deployed. These solutions provide only 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 toward IP-based access networks has to be smooth, reusing current technologies as much as possible. Also, a major factor to be taken into account in the design of access networks is the cost of the network elements and signaling functions. This article describes an IP-based architecture for access networks targeted for residential and small office/home office (SOHO) users that supports broadband multimedia services. We start by giving a historical perspective of the evolution of access networks.

ACCESS NETWORK EVOLUTION

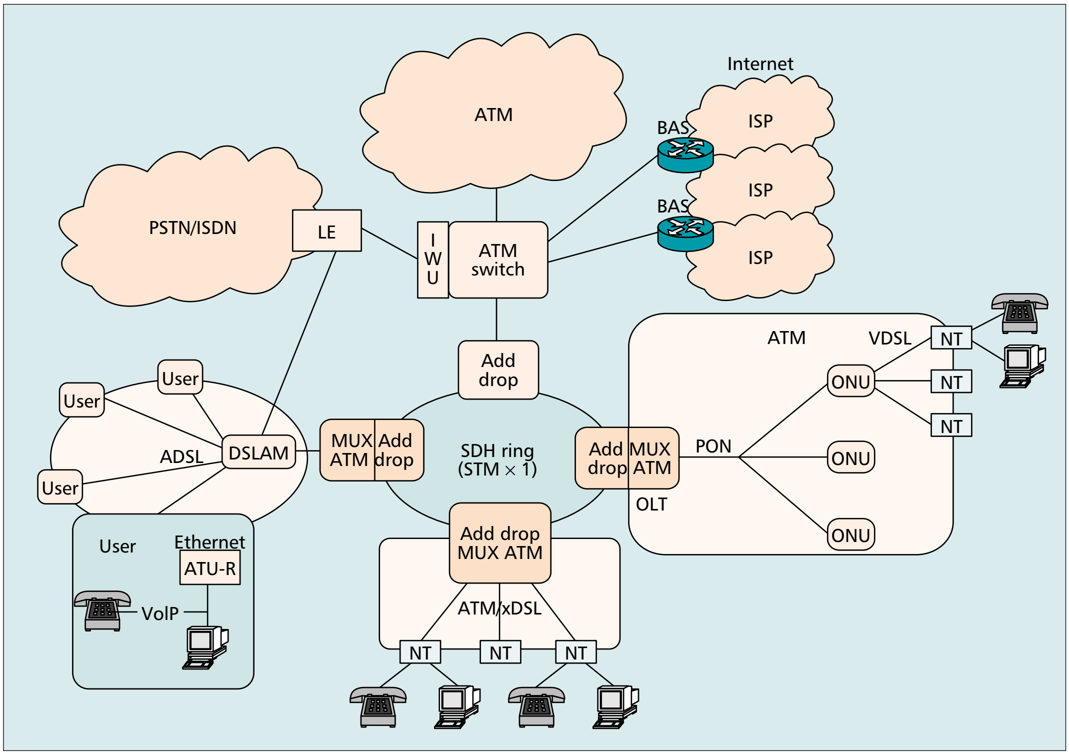
The most commonly used fixed access networks nowadays are supported on copper pairs connecting user equipment to the local exchange (LE). In dialup access to the Internet (Fig. 1) a circuit is established between the user and an access server (AS) via the public switched telephone network (PSTN). User interfaces can be analog or digital (e.g., integrated services digital network, 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. Because the duration of a typical Internet access session is much longer than that of a phone call, and a reserved bandwidth is allocated to each user during the whole session, the Internet access service places a strong demand on the resources of the PSTN. Therefore, the AS (or NAS) must be placed as close as possible to the local exchange.

Dialup access to the Internet is supported on narrowband circuits for connection to the ISP. Asymmetric DSL (ADSL) technology is being introduced to allow the support of emerging broadband services over the existing copper cable infrastructure. ADSL explores the asymmetry of most broadband services, which typically require more bandwidth in the downstream direction. It provides a bandwidth dependent on

0163-6804/03/$17.00 © 2003 IEEE



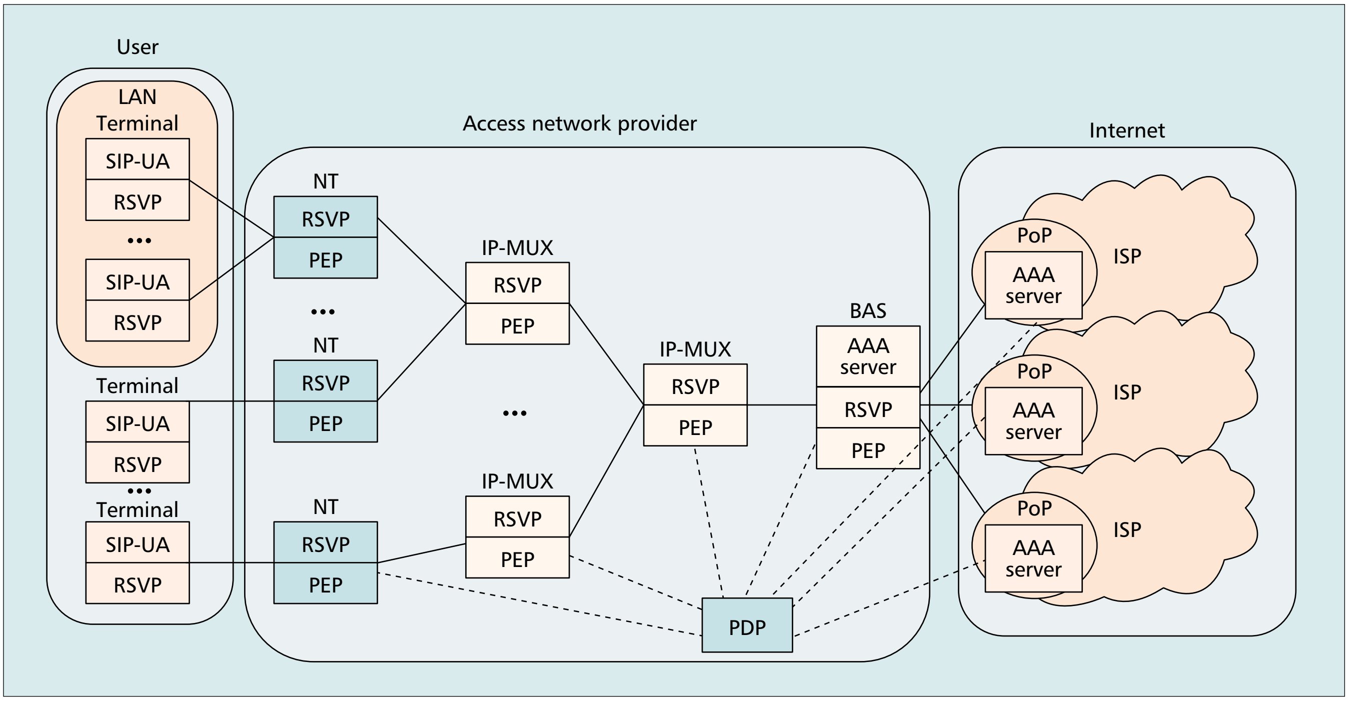
■ **Figure 1.** *Dialup access to the Internet.*



■ **Figure 2.** *ATM-based access networks.*

the distance and cable conditions up to a maximum of 6 Mb/s downstream and 640 kb/s upstream. The star topology, characteristic of legacy copper infrastructures, can still be maintained since the user terminals are connected to a DSL access multiplexer (DSLAM), collocated with the local exchange, through point-to-point copper connections (Fig. 2). The broadband and voice services are isolated via frequency-division multiplexing. The broadband traffic is supported by ATM connections over ADSL between the user ATM interface (ATU-R) and the DSLAM, which aggregates several ADSL accesses. Internet traffic is routed to the broadband access server (BAS) through ATM connections and the voice traffic to the PSTN local exchange. In the DSLAM there is a splitter that separates the broadband and voice traffic. The BAS is the interface element between the access network and the IP core network. It can distribute traffic to different ISPs, authenticate users, and allow each terminal to choose an ISP.

The BAS is the interface element between the access network and the IP core network. It can distribute traffic to different ISPs, authenticate the users, and allow each terminal to choose an ISP.



■ **Figure 3.** *Architecture of an IP-based access network.*

In a star topology with point-to-point copper connections, ADSL is an effective solution for broadband service support. However, there is a scalability problem since the number of ADSL connections per copper cable is severely limited by the distance between the user terminal and the DSLAM. Synchronous digital hierarchy (SDH) rings are now installed (and keep being installed) in the access network, carrying mostly narrowband traffic but paving the way to broadband traffic support. Last mile connections between users and SDH ring add-drops can be supported by xDSL for broadband services. Typically, these copper connections are much shorter than those of the legacy infrastructure since the add-drops are normally closer to the user terminal than the local exchanges.

Cable TV distribution networks already installed and updated with upstream connectivity are also able to support broadband traffic. Where CATV already exists, a cost-effective and highly competitive solution for a broadband access network is to add upstream capabilities. DOCSIS and EuroDOCSIS are generally recognized as winner protocols for the support of upstream and downstream IP transport.

In greenfield installations, other cost-effective solutions more adjusted to the requirements of multiservice broadband access networks can be identified. The use of very large service access nodes, edge switches/routers, and SDH management capabilities will allow the enlargement of the access network. This can justify an access network architecture based on a two-level hierarchy of SDH rings, with secondary rings connected to the primary one. Passive optical networks (PONs) are an alternative solution to secondary SDH rings (Fig. 2). In this scenario, last mile connections for residential and SOHO users will be supported on xDSL over copper, with the possibility of extensive deployment of very high data rate DSL (VDSL). In this scenario, business users can be connected directly to the primary ring by SDH fiber connections.

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 a lot of 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. In the remainder of the article we describe an IP-based access network that provides full service integration and resource sharing and supports, at the same time, QoS assurance and differentiation as required by future broadband multimedia services.

Architecture of IP-Based Access Networks with QoS Support

The design of a technological solution for next-generation access networks is deeply constrained by cost factors, because of the large number of network elements that need to be replaced or newly deployed. Traditionally, access network technologies have provided for very limited resource sharing. For example, in dialup networks users are completely isolated from each other, and in ADSL networks the broadband and voice services are separated at the physical layer. The lack of resource sharing can be mainly attributed to the cost of signaling. Resource sharing at the access network can help reduce the cost of bandwidth but requires more functionality, and therefore more complex and costly equipment. In future access networks, the critical balance between cost and functionality has to be carefully considered. Figure 3 shows the architecture of an envisaged IP-based access network, which was designed having the cost factor in mind while still providing for the integrated support of broadband multimedia services. A number of complementary functions need to be considered as part of the architecture: resource reservation, session signaling, QoS policy management, and authentication, authorization, and accounting (AAA). In the following sections we describe the various network elements and functions, and the technologies to be supported in the access network. We tried to reuse some of the terminology of ATM-based access networks.

Network Elements

In access networks for residential and SOHO environments, the user can be either a single terminal or a local area network (LAN). The network termination (NT) performs the adaptation between the user terminal and the access network. Traffic from different NTs is aggregated into IP multiplexers (IP-MUXs); several stages of multiplexing can be supported. The broadband access server (BAS) interfaces the access network and the ISP. It can include several functions such as acting as an AAA proxy of the ISP or as a DHCP server, or allowing the user terminal to choose an ISP. There are several options for the interfaces between the network elements. The interface between NTs and IP-MUXs can be xDSL or fiber to the home (FTTH). The interface between IP-MUXs or between an IP-MUX and the BAS can be SDH. IP over fiber is an expected target in the medium to long term.

Network Resilience

Since the core of the access network is based on IP-MUXs, there is no path redundancy at the network layer. We do believe this is not a requirement for access networks, and these networks can rely on physical layer redundancy, such as that provided by SDH. Therefore, at the IP layer the access network is a logical tree. Logical tree architectures simplify a number of functions like routing and addressing.

Routing

Given that the access network is a logical tree at the IP layer, traffic can be forwarded in the upstream direction without the need for any routing information. The BAS and IP-MUXs need only to maintain routing tables for forwarding traffic in the downstream direction. The maintenance of these tables simply requires reachability information to be advertised in the upstream direction. No routing metrics (and no shortest path routing algorithm) 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 (IP-MUX or BAS), only entries for networks or hosts that are downstream reachable from that element need to be included. The routing function can be implemented with a simplified version of a distance vector protocol such as RIP. In this case, the simplification is due to the absence of the count-to-infinity problem that complicates distance vector protocols, and also by the fact that no routing metrics need 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 is it desirable for security reasons), the addresses can be private.

RSVP and RSVP Extensions

Resource Reservation Protocol (RSVP) is widely used in the context of the integrated services (IntServ) architecture. In this case, resource 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, which is dynamically refreshed. Consequently, 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 IntServ, the differentiated services (DiffServ) architecture was proposed. In DiffServ, flows are aggregated in classes according to specific characteristics. Recently, an extension of RSVP for the support of signaling in the DiffServ architecture was proposed [1]. This extension brings the possibility of aggregating several end-to-end RSVP reservations. Admission control is only performed on an aggregated set of flows; 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 per-flow reservation state. The routers inside the network (the IP-MUXs in our case) maintain only the aggregate state. To achieve this goal, the IP Protocol Number in the end-to-end RSVP messages is changed from RSVP to RSVP-E2E-IGNORE upon entering the aggregation region, and restored to RSVP upon exiting. These messages are ignored by each router within the aggregation region whenever they are forwarded to an interior interface. In this way, end-to-end RSVP messages can be hidden from the IP-MUXs. However, the IP-MUXs still need to be RSVP aware to perform reservations of flow aggregates.

We argue that since RSVP is a widely deployed protocol and most multimedia applications are being developed assuming RSVP as the resource reservation protocol, support for RSVP in the access network is almost inevitable. Also, since RSVP has been upgraded to perform

Since the core of the access network is based on IP-MUXs, there is no path redundancy at the network layer. We do believe that this is not a requirement for access networks, and that these networks can rely on physical layer redundancy, such as the one provided by SDH.

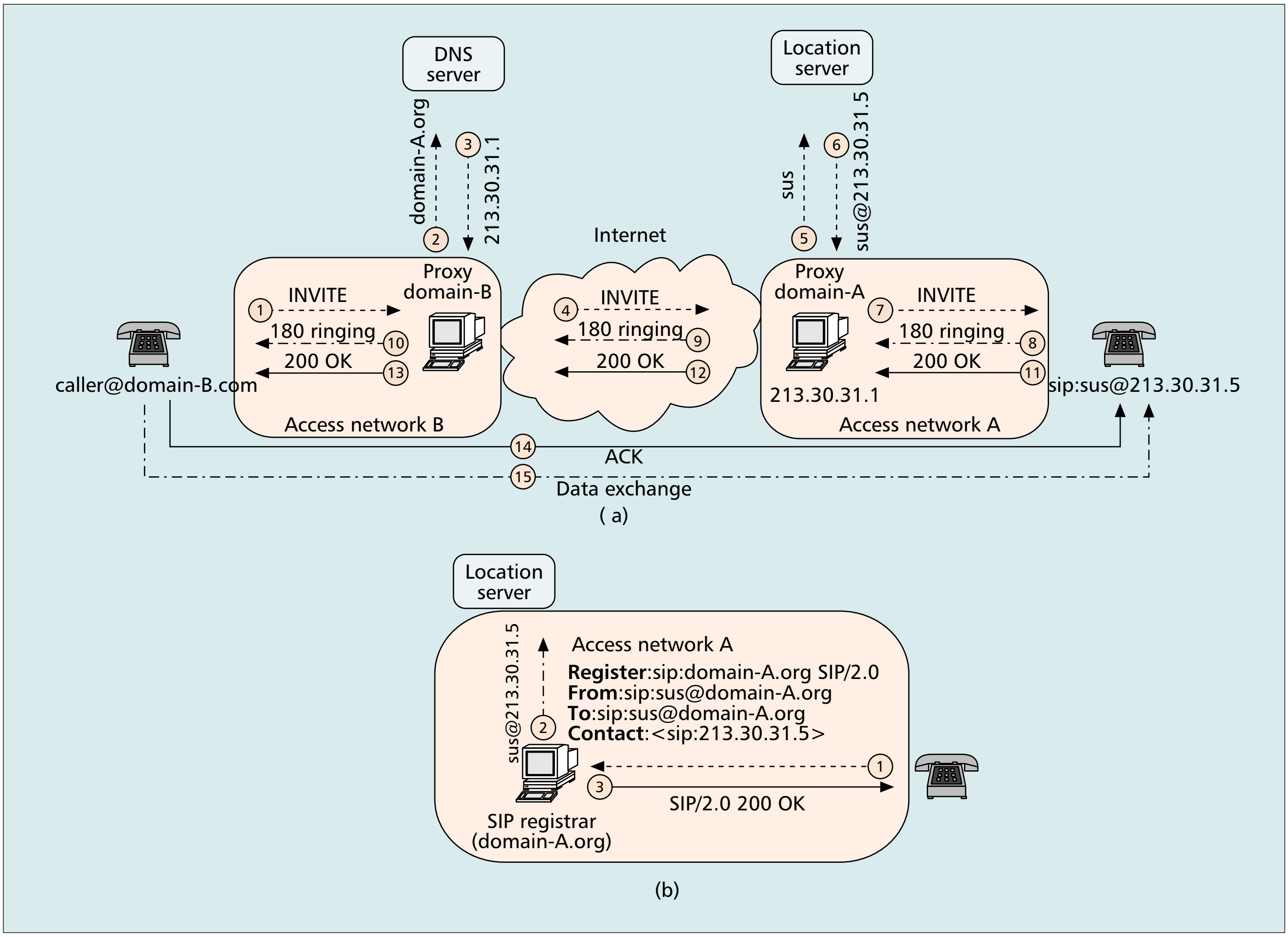


Figure 4. *a) Session initiation over access networks using SIP and b) user registration with SIP.*

resource reservation of both individual flows and flow aggregates, effectively allowing for mixed IntServ and DiffServ environments, its support in the access network provides a flexible framework for establishing trade-offs between cost and performance: IP-MUXs capable of processing more flows will achieve better resource utilization but will have higher cost.

PACKET SCHEDULING

The access network must support, at the same time, several types of traffic: signaling traffic, reserved traffic (used to provide semi-permanent connections), the traffic of on-demand sessions, and best effort traffic. The packet scheduling disciplines at the access network elements will have two hierarchical levels. At the first level, the treatment given to the various traffic types is differentiated based on strict priority scheduling with three priorities: one for the signaling traffic, another for the reserved and on-demand traffic, and another for best effort traffic. The signaling traffic, the most sensitive, will be assigned the highest priority. However, in order to protect the network against malicious users, a rate limiter will have to be associated with this priority at the entry points of the access network (i.e., at the NT for upstream traffic and at the BAS for downstream traffic). Best effort traffic will be assigned the lowest strict priority, since it has no requirements in terms of bandwidth, packet loss, or average delay. Finally, the reserved and on-demand traffic will be assigned the middle priority. The traffic subject to this priority will be further differentiated using Weighted Fair Queuing or one of its variants, which allows assigning a minimum bandwidth to each flow or aggregate of flows. Thus, packet scheduling in the access network will be strict priority at a first level and Weighted Fair Queuing at the middle priority.

SIP BASICS

The Internet Engineering Task Force (IETF) defined a new signaling protocol, the Session Initiation Protocol (SIP) [2], to provide session initiation over the Internet. The main elements of the SIP architecture are user agents, registrars, and proxy and redirect servers. The user agents are the endpoints of sessions; registrars allow for user registration; proxy servers are application-layer routers that forward SIP messages; and redirect servers return alternative locations of user agents or servers. While SIP was developed to establish, modify, and terminate multimedia sessions over the Internet, it can play other roles, some of them required in access networks. For example, it supports user registration, which allows for pre-call terminal mobility, and it can be synchronized with the resource reservation and AAA process. In SIP, users are identified by URLs, which are similar to email addresses (e.g., sus@domain-A.org). In each session, the URL is resolved to an IP address by using the SIP proxy server and DNS lookups.

The basic SIP messages are INVITE, 180 Ringing, 200 OK, ACK, BYE, and REGISTER. Consider the example of a signaling exchange that involves two proxies, handling the session's domain of origin and domain of destination, respectively (Fig. 4a). The signaling is initiated by an INVITE message. The INVITE contains a description of the type of session that is requested. A multimedia session can include several streams. For example, a videoconference application may contain audio, video, and data, each stream having its own QoS requirements. SIP uses a description format, called Session Description Protocol (SDP) [3], to allow each party to declare its receiving capabilities and the characteristics of the media streams it wants to receive. The INVITE message also includes the destination's SIP URL, which is used for routing the request. If the IP address of the callee is known, the INVITE can be sent directly to him; otherwise, it is sent to the origin's domain proxy server, also called outbound proxy server. Upon receiving this message, the proxy performs a DNS lookup of the destination's domain name, which returns the IP address of the destination's domain proxy server. The INVITE is then forwarded to this proxy, which determines the IP address of the callee through a lookup on the associated location server. The callee answers with a 180 Ringing message indicating that the INVITE message was received and alerting has taken place. When the callee decides to accept the session, it sends a 200 OK message indicating also that the type of session proposed by the caller is acceptable. The final step in establishing the call is the ACK message sent by the caller, which is a confirmation that it can also accept the session. At this point, the session is started using another protocol, typically Real-Time Transport Protocol (RTP). The session is terminated through a BYE message that is confirmed by a 200 OK.

User registration is illustrated in Fig. 4b. When an IP address is assigned to a user, it sends a REGISTER request message to the proxy or redirect server to inform it of the IP addresses where it can be reached. The proxy server forwards the message to the Registrar server, which may or may not be located in the same element as the proxy. The Registrar server sends the IP address and URL to the location server to store the information in a database that can be accessed through DNS. Later, this information will be used by the proxy server to locate the user.

In the access network, the BAS will include an outbound SIP proxy server. A registrar server is also required but can serve more than one BAS. The proxy server has access, through the location server, to the database that contains the IP addresses of the users in its domain. It also performs routing functions, determining the next hop to which signaling should be relayed.

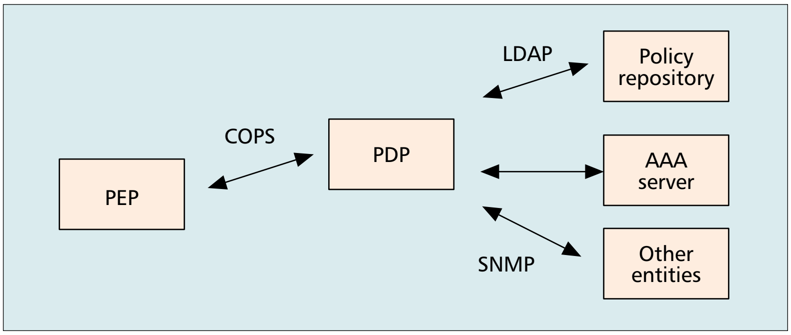


Figure 5. *The QoS policy management framework.*

SIP Addressing and ISP Selection

A key function in the access network that can easily be accomplished by SIP is the selection of the ISP. For this purpose, the user specifies in the URL the domain that identifies the ISP it wishes to select. For example, if there are two ISPs available, isp-X.com and isp-Y.com, and the user wants to access a service through isp-X, it will use URL user@isp-X.com and the request will be routed via the isp-X domain.

Recently, an extension to DHCP has been proposed that allows a single DHCP server to advertise one or more outbound proxy servers [4]. For this purpose, the so-called SIP server DHCP option carries either IP addresses or DNS fully qualified domain names to be used by the SIP client to locate a SIP server. So, as the user agent is assigned its IP address, it is also informed of the various ISPs available in the access network to which it has just connected.

QoS and Security Support with SIP

SIP includes mechanisms, called preconditions, for coordinating the session signaling and establishing end-to-end resource reservations or security tunnels. A precondition is a condition that must be met before session signaling can be completed. QoS and security support were additions to the basic SIP standard.

There are two options for the interaction between session signaling and resource reservation: QoS assured calls, implemented through mandatory QoS preconditions, or QoS enabled calls, implemented through optional ones [5]. In QoS assured calls, the caller will not receive a 180 Ringing message, indicating that the call may start, unless resource reservation has completed successfully. This type of service is equivalent to present circuit-switched telephony. The call setup time is longer due to the dependence on resource reservation. In QoS enabled calls, call setup and resource reservation are decoupled, and may proceed concurrently. In case of resource reservation failure, the caller can be notified and given the option of continuing the call with best effort service only. The call setup time is shorter, and the best effort call may still be useful to end users.

QoS Policy Management and AAA with COPS and Diameter

A multiservice network with QoS support places additional requirements in the AAA functionality. These functions need now to be performed

Note that in the access network, all packet flows cross the BAS, even if the calls are between end-users in the same access network. Therefore, the only element that is required to exchange accounting information with the PDP is the BAS.

on a user/service/QoS level basis. The current trend is to include the AAA functionality under the scope of a QoS policy management framework (Fig. 5). The IETF framework [6] defines two main architectural elements for policy control: the policy enforcement point (PEP) and policy decision point (PDP). The PEP is the element that enforces the policy decisions, and the PDP makes decisions based on the policies it retrieves from policy repositories, AAA 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 (e.g., user authentication, accounting, policy information storage). Common Open Policy Service (COPS) [7] is the suggested protocol to exchange information between the PDP and PEP. The interaction between the PEP and PDP works as follows. When the PEP receives a message that requires a policy decision, it formulates an event for a policy decision and sends a COPS Request message to the PDP. This message 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 the action the PEP should take. The PEP then enforces the policy decision by appropriately accepting or denying the request. To exchange information with the policy repository, for storage and retrieval of policy information, the PDP uses the Lightweight Directory Access Protocol (LDAP) [8]. 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.

A very important COPS facility is that it provides the download of the QoS configurations to the network devices. The PDP only needs to know that a device uses a certain set of rules, and then pushes those rules 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 AAA servers can be accessed using RADIUS or DIAMETER [9]. The RADIUS protocol has traditionally been used to provide AAA services for dialup PPP and terminal server access. DIAMETER is a replacement for RADIUS, which has better scalability and supports mobility. In both registration and call process, the SIP proxy server sends a COPS Request to the PDP, and this one contacts the DIAMETER server through DIAMETER exchange messages. The data delivered by DIAMETER protocol is, as in RADIUS, in the form of an attribute value pair (AVP), which is used to carry specific information like user authentication, service-specific authorization, and resource usage information.

In the access network all elements will include a PEP. The PEPs at the NTs and IP-MUXs need only to support the download of QoS configurations. The PEP at the BAS needs to support the triggering of COPS messages on specific events related to SIP. Note that in the access network, all packet flows cross the BAS, even if the calls are between end users in the same access network. Therefore, the only element required to exchange accounting information with the PDP is the BAS.

An Example of Message Flow in the Access Network

Figure 6 shows an example of a message flow in the access network in the case of QoS assured calls. The messages between the ISP and the called user are not represented. Also, we consider that resource reservation is performed in both directions. When a user wants to initiate a session, it sends an INVITE message toward the destination. The INVITE message includes a QoS attribute indicating mandatory resource reservation in both directions. The proxy server captures the INVITE message and sends a COPS Request message to the PDP to perform AAA and QoS policy functions. This COPS message includes information retrieved from the SIP message: SIP source and destination addresses, SIP call identifier, media information, and QoS attributes. After receiving a positive answer through a COPS Decision message, the INVITE message is forwarded to the destination via the ISP network that was selected by the user. Since the INVITE message includes preconditions, the called user must answer with a 183 Session Progress message using the so-called reliability mechanism [10]. The 183 message includes the IP address of the called user, and contains QoS and security attributes for each stream having a precondition. If the receiver is capable of meeting the preconditions, it just copies the QoS and security attributes of the INVITE to the 183 message; otherwise, it may propose new attributes, and a negotiation phase may start with the caller sending another INVITE message. The reliability mechanism forces the caller to reply to the 183 message with a PRACK message and the callee to acknowledge with a 200 OK message. The destination also requests, in the 183 message, a confirmation to be sent when the preconditions are met.

Now the RSVP process starts through the exchange of PATH and RESV messages between the sender and receiver [11]. The RSVP messages in the two directions may overlap, and there is no specified sequence. As mentioned before, RSVP can be used in both IntServ and DiffServ architectures. In DiffServ architectures (the case of this example) the elements between the NTs and the BAS only process reservations of flow aggregates; per-flow processing is only performed in the NTs and BAS. In an IntServ architecture, the RSVP messages do not go transparently from the NT to the BAS, but need

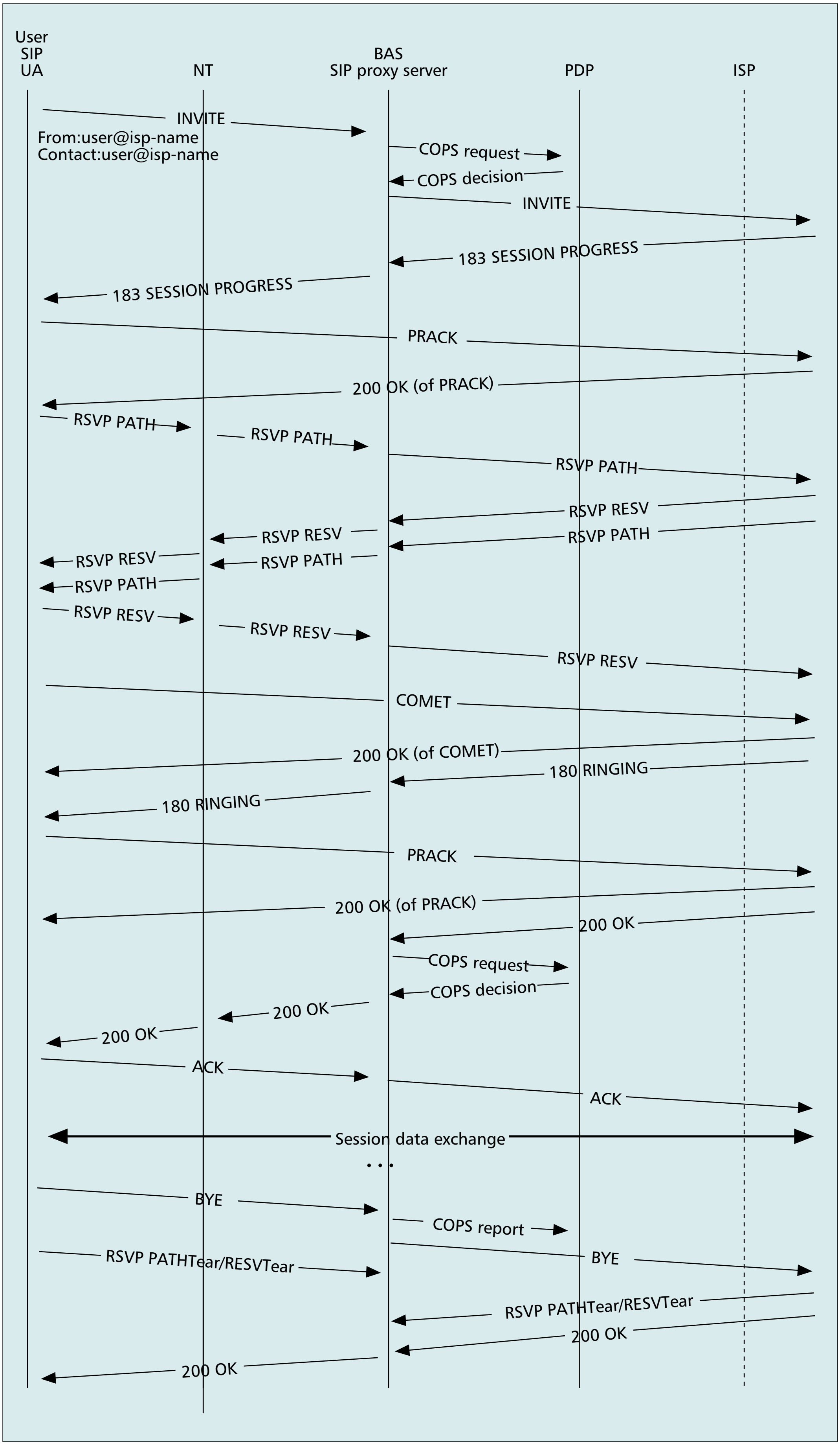


Figure 6. *A timing diagram of a multimedia Internet access session, with SIP, COPS, and RSVP.*

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 order to support broadband multimedia services, the access network must incorporate a number of newly introduced technologies: SIP for session initiation, COPS and DIAMETER for QoS policy management and AAA, and RSVP for resource reservation.

to be processed in the IP-MUXs. Upon a successful RSVP process in the direction from the sender to the receiver, the caller sends a COMET message to the callee. This message is a SIP extension that has an SDP body attached indicating the status of each precondition as "success" or "failure." When receiving the COMET message and upon success of the reservation in the direction from the receiver to the sender, the destination determines that all preconditions have been met and sends the 180 Ringing message to the caller, indicating that the call may start. In this case, the 180 message also requires the reliability mechanism (PRACK and 200 OK). Finally, the destination sends the 200 OK message (of the INVITE). The proxy server at the BAS, upon capturing this message, exchanges COPS messages with the PDP to update any changes in the session information and start the accounting functions. After the ACK message, the session data can be exchanged between the two peers. When terminating the session one user sends a BYE message and the other answers with a 200 OK. Also, both parties remove their resource reservations. The proxy server at the BAS captures the BYE message and sends a COPS Report message to the PDP to terminate the accounting of the session.

CONCLUSIONS

This article describes an architecture for IP-based access networks targeted for residential and SOHO users. The main elements of the architecture are the NTs, IP-MUXs, and BAS. The use of IP multiplexers instead of IP routers helps simplify a number of functions and reduce the cost of the access network. In order to support broadband multimedia services, the access network must incorporate a number of newly introduced technologies: SIP for session initiation, COPS and DIAMETER for QoS policy management and AAA, and RSVP for resource reservation. The recent introduction of an RSVP extension to support flow aggregation provides a flexible framework for establishing trade-offs between cost and performance in the access network. All access network elements are RSVP-aware and include a policy enforcement point. In addition, a SIP proxy server is collocated with the BAS. The BAS has access to a policy decision point, which contacts the AAA servers at the ISPs and the policy repository. Packet scheduling is required at all network elements to discriminate the various types of traffic. We consider a hierarchy with strict priority scheduling at the first level and Weighted Fair Queuing at a second level to handle user traffic with QoS requirements. In the article we also illustrate the message flow of a multimedia Internet access session.

REFERENCES

[1] F. Baker *et al.*, "Aggregation of RSVP for IPv4 and IPv6 Reservations," RFC 3175, Sept. 2001.

[2] M. Handley *et al.*, "SIP: Session Initiation Protocol," RFC 2543, Mar. 1999.

[3] M. Handley and V. Jacobson, "SDP: Session Description Protocol," RFC 2327, Apr. 1998.

[4] H. Schulzrinne, "DHCP Option for SIP Servers," Internet draft draft-ietf-sip-dhcp-06.txt, Mar. 2002.

[5] W. Marshall *et al.*, "Integration of Resource Management and SIP," Internet Draft draft-ietf-sip-manyfolks-resource-07.txt, Apr. 2002.

[6] R. Yavatkar, "A Framework for Policy-Admission Control," RFC 2753, Jan. 2000.

[7] D. Durhan *et al.*, "The COPS (Common Open Policy Service) Protocol," RFC 2748, Jan. 2000.

[8] M. Wahl *et al.*, "Lightweight Directory Access Protocol (v3)," RFC 2251, Dec. 1997.

[9] P. Calhoun *et al.*, "Diameter Base Protocol," Internet draft draft-ietf-aaa-diameter-10.txt, Apr. 2002.

[10] J. Rosenberg and H. Schulzrinne, "Reliability of Provisional Responses in SIP," Internet draft draft-ietf-sip-100rel-06.txt, Feb. 2002.

[11] H. Schulzrinne *et al.*, "Interaction of Call Setup and Resource Reservation Protocols in Internet Telephony," Tech. rep., June 1999.

BIOGRAPHIES

SUSANA I. SARGENTO (ssargento@dcc.fc.up.pt) graduated in electronics and telecommunications engineering from the University of Aveiro, Portugal, in 1997, and is a Ph.D. student at the same university. In September 2002 she joined the Department of Computer Science in the Sciences Faculty of the University of Porto as an assistant professor. She is also a researcher in the Computer Networks Group of the Laboratory of Artificial Intelligence and Computer Science (LIACC). Her main research interests are in the areas of resource management for multiservice networks and architectures for future IP networks.

RUI T. VALADAS (rv@det.ua.pt) graduated in electrical and computer engineering from Instituto Superior Técnico, Lisbon, Portugal, in 1986, and received a Ph.D. degree from the University of Aveiro, Portugal, in 1996. He joined the University of Aveiro in 1986, where he is now an associate professor in the Department of Electronics and Telecommunications Engineering. He is also a researcher at the Institute of Telecommunications — Aveiro Pole, where he leads the Networks and Multimedia Communications Group. His main research interests are in the areas of traffic engineering for multiservice networks and wireless optical communications.

JORGE GONÇALVES (jgoncalves@ptinovacao.pt) graduated in electronics and telecommunications engineering from the University of Aveiro, and holds an M.Sc. degree from the same university. Since 1999 he is the head of the Access Network Management unit at Portugal Telecom Inovação, the R&D company of Portugal Telecom. From 1991 to 2002 he was involved in European RACE, ACTS, and Eurescom projects in areas related to ATM networks, access networks based on IP technologies, and network management.

HENRIQUE SOUSA (tsousa@av.it.pt) graduated in electrical engineering from the University of Porto in1969. From 1974 to 2000 he worked for the Research Center of Portugal Telecom (PT Inovação). He was engaged in the development of signaling systems for a digital exchange system and participated in RACE I and II projects. From 1994 to 2000 he was responsible for access network systems development. He joined the Institute of Telecommunications — Aveiro Pole in 2000.