QoS Provisioning for Mobile IP Users

Günther Stattenberger — Torsten Braun

Institute of Computer Science and Applied Mathematics
University of Bern
Neubrückstrasse 10
CH-3012 Bern

{stattenb, braun}@iam.unibe.ch

ABSTRACT. *In wireless access networks bandwidth is a limited resource. Therefore, Mobile IP users will demand to receive QoS support. However, in a highly dynamic environment — as mobile environments — QoS provisioning is a difficult task. In this paper we propose a signaling protocol for mobile users to contact a bandwidth broker for negotiation QoS for a flow. This protocol can also be used for negotiating QoS for traffic aggregates between two bandwidth brokers. Two scenarios are designed to evaluate the protocol.*

KEYWORDS: *Mobile IP, Quality of Service*

1. Introduction

The scenario presented in this document shall prove the ability of a Bandwidth Broker (BB) using the QoS Management API [STA 01b] to provide Differentiated Services to a Mobile IP User. Using this API a QoS management application can be developed that is able to configure a heterogenous network via high-level configuration commands and abstract flow descriptions.

A mobile user might visit several access networks managed by different ISPs, but he desires to get a certain service wherever he is connected. Since the user has negotiated a Service Level Specification (SLS) with his home-ISP only, this SLS has to be transformed and transmitted to the foreign networks the mobile user visits. The BB managing the foreign network will then configure the network according to the SLS of the user.

This scenario depends on several additional new parts besides the QoS Management and the Mobile IP support: A communication protocol between the mobile host and the BB has to be specified in a way that enables the mobile host to negotiate a SLS with the BB. A similar communication protocol is needed for inter-broker communication.

1.1. *AAA issues*

A realistic scenario would also require AAA components. AAA servers in each domain could authenticate a user in a foreign domain, and grant for the behaviour of the user and for paying for the resources he used. For this purpose, a AAA architecture extension has been proposed in [BRA 01]. Here a protocol between a mobile user and a SLP directory agent has been defined, that allows a mobile user to authenticate at a foreign domain and authorize for the use of special services, in particular Quality of Service. Additional accounting messages have been introduced, too. This architecture can nevertheless easily be seperated from the components discussed in this paper. Therefore we assume, that during all actions the authorisation is granted by an external entity.

1.2. *Related Work*

Another approach to provide QoS to mobile users has been published in [CHA 01]. Contrary to the approach presented in this paper a non-centralistic approach is proposed. A flow description similar to ours is included as an IP option in binding messages for mobile IPv6, triggering router configurations. However, the main drawback of this solution is the missing security support, which most likely can’t be solved without a central authority.

2. Scenario Description

Using the small network shown in Figure 1 we can show the major points where the reconfiguration happens when the mobile user establishes a SLS at home and afterwards migrates from one domain to another.

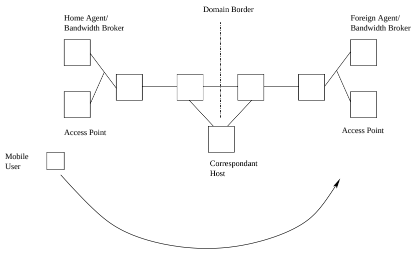


Figure 1. *Demo Scenario for QoS Provisioning to a mobile user*

2.1. *Negotiation of a new SLS*

After registering at the home agent the mobile host can send the information about the desired SLS to the home bandwidth broker. The negotiation starts when the mobile user sends a packet containing the bandwidth and some high-level information about the desired service [BAL 01] (e.g. delay-sensitivity, loss-sensitivity ...). The broker's communication interface translates this information to the internal, technical-oriented flow description of the broker and submits the result to the BB. The BB tries to set up the routers according to the user's requirements and reports success or failure back via the communication interface.

2.2. *Migration to a new domain*

When the mobile host moves to a foreign domain it first has to get a care-of address (CoA) by either a foreign agent or DHCP. Using this CoA the mobile host can now request the transfer of its home SLS to the new location. The transfer is initiated by signalling the request to the BB in the foreign domain. The broker can now perform the authentication separately and afterwards contact the home domain's BB for getting the user's SLS. Together with the CoA of the mobile user the foreign BB can now establish the service in the foreign network.

Alternatively the mobile user could establish a totally new SLS with the foreign BB without using the SLS at home. The procedure is then — set aside AAA issues — identical to the procedure in the last section.

3. Packet Format for SLS Flow Description

For the communication between the mobile host and the bandwidth broker and also for inter-broker communication an abstract flow description has to be specified. The flow description shown in Figure 2 can be mapped to different QoS strategies provided by the network by bandwidth brokers as long as the requirements of the flow are fulfilled. This packet contains the following information to specify a flow together with a certain service level:

– Source address and source port,

– Destination address and destination port,

– Protocol ID (TCP or UDP),

– a bandwidth value that specifies the average bandwidth of the flow in terms of kbit/s,

– a realtime flag, that indicates delay and jitter sensitivity of the flow,

– a loss sensitivity flag, whether the flow is critical against packet loss or not,

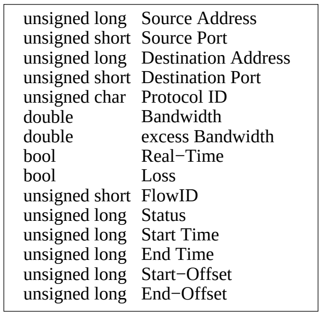
– a status byte, providing information about the status of the reservation (e.g. in work, ready, in progress etc.)

– a flow identification number,

– the absolute start and end time of the flow,

– the relative start and end time of the flow counting from now.

The detailled description of the packet entries can be found in [BAL 01].



unsigned long	Source Address
unsigned short	Source Port
unsigned long	Destination Address
unsigned short	Destination Port
unsigned char	Protocol ID
double	Bandwidth
double	excess Bandwidth
bool	Real−Time
bool	Loss
unsigned short	FlowID
unsigned long	Status
unsigned long	Start Time
unsigned long	End Time
unsigned long	Start−Offset
unsigned long	End−Offset

Figure 2. *Packet format for SLS signalling*

4. Protocol Specification

4.1. *Negotiation of a new SLS*

The messages that need to be exchanged between the mobile host and the BB in order to set up a new SLS are shown in Figure 3. Those messages are exchanged via the TCP protocol. Authentification information should be included, but this issue is not considered in this scenario.

In particular those messages are

1) The initial request message defining the Service Level of the new flow. This message contains a data structure shown in Figure 2, describing the flow specification in an abstract way [BAL 01]. Therefore the broker can decide how to configure the routers in a way that best fits for the current network topology.

2) The bandwidth broker translates the abstract packet data into a concrete router configuration. Now it tries to set up the routers that are involved during the transmission of the flow. The BB can also check in advance, if there is enough bandwidth reserved to accept the flow and reject the SLS if this is not the case (see message (4)). The API described in [STA 01b] manages all the translation and configuration and also provides the functionality to manage the bandwidth that is reserved.

3) Each router reports success or failure of the configuration back to the bandwidth broker.

4) The BB reports the status of the SLS back to the mobile host. Failure can be caused by errors during the configuration or — most likely — by unavailable bandwidth.

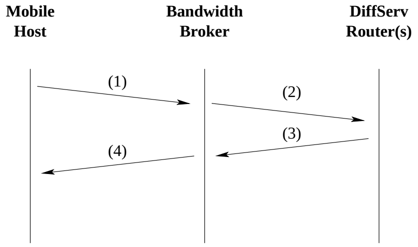


Figure 3. *Message sequence for negotiating a new SLS*

4.2. *Migration to a new domain*

If the mobile user connects to a foreign domain the SLS of its home domain has to be transferred to the foreign network. The mobile host can check whether it is connected to a foreign network by checking for a care-of address. The message sequence for this case is shown in Figure 4.

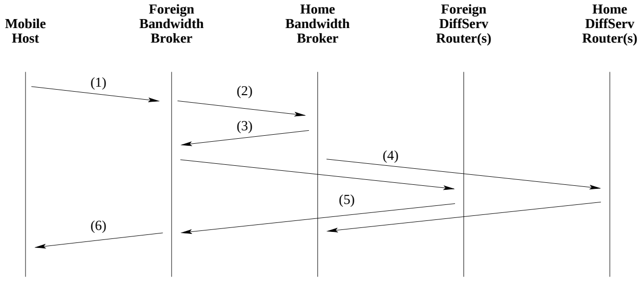


Figure 4. *Message sequence for SLS transfer to a foreign network*

As mentioned before, the protocol shown in Figure 3 can also be used, e.g. for changing the home-SLS to adapt it to the new environment.

1) The mobile host requests the foreign bandwidth broker to transfer its home SLS to the new location. This uses a special packet format, including the home IP address of the mobile host.

2) The foreign BB asks the home BB for the SLS of the mobile host. It has to use the home IP address of the mobile host for the query.

3) The home BB transmits the SLS to the foreign BB using the packet format shown in figure 2.

4) The foreign BB replaces the home IP address of the mobile node with the care-of address and configures the routers in its network. The home BB reconfigures the routers in the home network to release the resources used by the mobile user.

5) The routers report success or failure of the configuration back to the bandwidth brokers.

6) The foreign BB informs the mobile host about success or failure of the SLS transfer.

5. Translation of the SLS to Linux Router configurations

The information provided by the SLS packet format (Figure 2) is a rather high-level specification of service level information. This information can be translated to router configuration parameters like queue length etc. in several ways. A specific transformation has to be chosen by the programmer of the API class for the Linux Router [STA 01b]. Since the API is object-oriented a modification of the existing API is not very difficult. The programmer has to take care of being compliant to the DiffServ PHB standards. One possible translation will be presented in this section.

The first service-level parameter — the bandwidth — can be translated in a trivial way to the correct queue configuration parameter regardless of the service (expedited or assured forwarding) the flow will get: Each queue posseses a specific parameter allowing to specify the bandwidth of that queue.

The two other parameters — the RealTime and the Loss flags — specify different queue settings or even different queues (PHBs), depending on the ProtocolID field in the SLS. All possible combinations are shown in Figure 5 and are explaind below

1) If neither the realtime-flag nor the loss-flag is set for a flow, the flow can be handled by a low-priority assured forwarding service class. The bandwidth will be provided regardless of the transprot protocol.

2) A realtime flow based on TCP depends on low delay and low jitter. Low delay can be achieved by a small queue length, but the queue length must be large enough to let a reasonable-sized burst pass. Due to conflicts of an expedited forwarding traffic shaper at the ingress router (e.g. a token bucket filter) with the TCP congestion control mechanism (see [STA 01a]) this flow has to be mapped to a specially configured AF class.

3) A realtime UDP flow can be handled perfectly by assured forwarding. Assured forwarding can provide excellent delay and jitter values even for irregular flows with large bursts. The drawback of this PHB is a small chance of packet loss.

4) A loss-sensitive UDP flow has to be transfered by expedited forwarding. Assured forwarding cannot guarantee that a flow doesn't have to share the bandwidth with another flow at the ingress router, so some packets could get lost. In this case the excess bandwidth limitation has to be set very carefully to prevent packet loss during bursts.

5) A UDP flow that is both, realtime and loss-sensitive, has also to be transfered by expedited forwarding. This flow will most likely be regulated in advance, so that the bandwidth will not exceed the negotiated limit.Therefore no conflicts with a expedited forwarding traffic shaper will occur. Again burst potection is a critical issue.

Setting the loss-critical flag does not make much sense for TCP flows, since TCP automatically retransmits lost packets. Therefore, this flag could be “abused” for indicating bandwidth-regulated or unregulated TCP streams. In this case a regulated TCP stream could be transfered by expedited forwarding, too. Nevertheless, this is not considered in this scenario.

6. Inter-Domain Broker Signaling

A second, more complex scenario is presented in Figure 6. For this scenario the bandwidth brokers in the home and the foreign networks also need to contact the BB in the correspondent host's (CH) network, because some of the routers are not in the domain of the home BB. In addition to configuring the routers in their own domains, the home and foreign BBs must signal the CH's broker the modified flow containing the egress router's address. The BB can determine this address by tracing its topology database (see [STA 01b]). It is important to signal the egress router's address, because

Real Time	**Loss critical**	**Protocol ID**	
0	**0**	**UDP/TCP**	**(1)**
1	**0**	**TCP**	**(2)**
1	**0**	**UDP**	**(3)**
0	**1**	**UDP**	**(4)**
1	**1**	**UDP**	**(5)**

Figure 5. *Translation of Service Level Information to Router Configuration*

the BB in the CH's network must be able to determine where the new flow enters its network. Since a bandwidth broker usually knows the topology of its own network only and additionally the addresses of the neighbouring egress/ingress routers, this is the only way to set up the flow correctly between two adjacent domains. The packet format for this message can be the same as in the first scenario (Figure 2). This fact extremely simplifies the broker signaling protocol.

When the mobile host roams toward the foreign domain, the reservation toward the home domain has to be deleted and a new reservation toward the foreign domain has to be established. The fact that perhaps some of the router configurations might already be established (e.g. in Figure 6 only the egress routers change) can not yet be considered and is subject of future research.

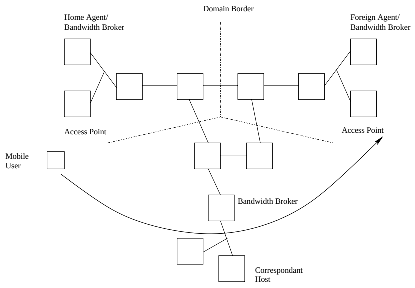


Figure 6. *A scenario for inter-domain broker signaling*

7. Conclusion

The scenarios presented in this paper will prove the ability of a bandwidth broker based on the QoS management API to configure a DiffServ network based on a SLS negotiated with a mobile user. Additionally, the possibility of the mobile user to roam between several domains, each managed by a different bandwidth broker, will be shown. It is a big advantage of this scenarios, that the Mobile IP infrastructure (e.g. the Foreign Agent and Mobile Host Daemons) don't need to be changed.

8. References

[BAL 01] BALMER R., GÜNTER M., BRAUN T., "Video Streaming in a DiffServ/IP Multicast Network", submitted for publication, May 2001.

[BRA 01] BRAUN T., RU L., STATTENBERGER G., "An AAA Architecture Extension for Providing Differentiated Services to Mobile IP Users", *Proceedings of the 6th IEEE Symposium on Computers and Communications*, July 2001.

[CHA 01] CHASKAR H., KOODLI R., "A Framework for QoS Support in Mobile IPv6", Internet Draft, March 2001, work in progress.

[GÜN 01] GÜNTER M., "Management of Multi-Provider Internet Services with Software Agents", PhD thesis, University of Bern, June 2001.

[KOO 00] KOODLI R., PERKINS C., "Fast Handovers in Mobile IPv6", Internet Draft, October 2000, work in progress.

[STA 01a] STATTENBERGER G., BRAUN T., "Performance Evaluation of a Linux DiffServ Implementation", submitted for publication, April 2001.

[STA 01b] STATTENBERGER G., BRAUN T., BRUNNER T., "A Platform-Indepent API for Quality of Service Management", *Proceedings of the IEEE Workshop on High Performance Switching and Routing*, May 2001.