3GPP TR 23.802 V7.0.0 (2005-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architectural enhancements for end-to-end Quality of Service (QoS) (Release 7)

Keywords
UMTS, performance, architecture

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The exclusive usage of QoS mechanisms as described in TS 23.207 [4] is not enough to guarantee full end-to-end QoS when interworking with external IP network domains, e.g. in those backbone networks which do not themselves contain IMS network elements. This is mainly because the described QoS concept presumes that the interconnecting IP networks are controlled by PLMN operators or other IMS operators. As a result, it is problematical to provide complete end-to-end QoS guarantees when interworking with external IP network domains or backbone networks which provide IP QoS mechanisms.

Especially for delay-sensitive services with strict end-to-end QoS requirements such as conversational speech or streaming video, the existing QoS concept may not satisfy the service requirements when interworking with such IP network domains and backbone networks. Consequently, new QoS concepts that are scalable and can take into account overall end-to-end network performance must be assessed.

1 Scope

The present document investigates possible solutions to enhance the end-to-end QoS architecture as currently specified in TS 23.207 [4] to achieve improved end-to-end QoS in the case of interworking with IP network domains or backbone networks that provide IP QoS mechanisms and enhanced interworking with other next generation networks. Within this technical report, emerging QoS standardization efforts from TISPAN, ITU-T, and the IETF should be taken into account.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS)".

[3] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[4] 3GPP TS 23.207: "End-to-end Quality of Service (QoS) concept and architecture".

[5] RFC 1633: "Integrated Services in the Internet Architecture: an Overview".

[6] RFC 2205: "Resource ReSerVation Protocol (RSVP)".

[7] RFC 2209: "Resource ReSerVation Protocol (RSVP) Message Processing Rules".

[8] RFC 2210: "The Use of RSVP with IETF Integrated Services".

[9] RFC 2475: "An Architecture for Differentiated Services".

[10] RFC 2925: "Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations".

[11] RFC 2748: "The COPS (Common Open Policy Service) Protocol".

[12] RFC 2750: "RSVP Extensions for Policy Control".

[13] Internet Draft: draft-ietf-tsvwg-diffserv-service-classes-00,txt, "Configuration Guidelines for DiffServ Service Classes, Transport Area working group draft; February 11, 2005".

[14] RFC 3168: "The Addition of Explicit Congestion Notification (ECN) to IP".

[15] RFC 2208: "Resource ReSerVation Protocol (RSVP) Version 1 Applicability Statement. Some Guidelines on Deployment".

[16] RFC 3175: "Aggregation of RSVP for IPv4 and IPv6 Reservations".

[17] Internet Draft: draft-lefaucheur-rsvp-dste-02.txt, "Aggregation of RSVP Reservations over MPLS TE/DS-TE Tunnels, February 2005".

[18] Internet Draft: draft-babiarz-tsvwg-rtecn-03.txt, "Congestion Notification Process for Real-Time Traffic, February 18, 2005".

[19] RFC 4080, "Next Steps in Signalling (NSIS): Framework".

[20] Internet Draft: draft-ietf-nsis-qos-nslp-06.txt, "NSLP for Quality-of-Service signalling, Next Steps in Signalling working group draft; February 20, 2005".

[21] Internet Draft: draft-ietf-nsis-ntlp-06.txt, "GIMPS: General Internet Messaging Protocol for Signalling, Next Steps in Signalling working group draft; May 17, 2005".

[22] Internet Draft: draft-ietf-nsis-qspec-04.txt, "QoS-NSLP QSpec Template, Next Steps in Signalling working group draft; May 2005".

[23] Internet Draft: draft-ietf-dccp-spec-11.txt, "Datagram Congestion Control Protocol (DCCP); March 10, 2005".

[24] ITU-T Recommendation Y.1291: "An architectural framework for support of quality of service (QoS) in packet networks".

[25] ITU-T Recommendation H.360: "An architecture for end-to-end QoS control and signalling".

[26] MSF MSF-TR-QoS-001-FINAL: "Quality of Service for Next Generation Voice Over IP Networks".

[27] RFC 2747: "RSVP Cryptographic Authentication".

[28] RFC 3260: "New Terminology and Clarifications for Diffserv".

[29] RFC 2752: "Identity Representation for RSVP".

[30] RFC 2872: "Application and Sub Application Identity Policy Element for Use with RSVP".

[31] Internet Draft: draft-ietf-nsis-rmd-01.txt, "RMD-QOSM - The Resource Management in Diffserv QoS model, Next Steps in Signalling working group draft; February 15, 2005".

[32] RFC 3346: "Applicability Statement for Traffic Engineering with MPLS".

[33] RFC 3097: "RSVP Cryptographic Authentication -- Updated Message Type Value".

[34] RFC 3182: "Identity Representation for RSVP".

[35] RFC 3726: "Requirements for Signalling Protocols".

[36] GSMA PRD IR.34: "Inter-PLMN Backbone Guidelines".

Editor's Note: References may need to be removed if not required and other references may need to be added if required.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and TS 23.207 [4] and the following apply.

Admission administrative domain: The Admission administrative domain defines a set of bearer devices and gateways whose resources and routes are managed. One example could be the BCF.

IP-CAN: A general term of IP Connectivity Access Network. It includes GPRS, I-WLAN and also other type of IP-CAN which may be defined in 3GPP.

Off-path IP QoS control: An IP QoS control method, also may be called Path-decoupled IP QoS control in which QoS signalling messages are first routed to a node that is not assumed to be on the data path.

On-path IP QoS control: An IP QoS control method, also may be called Path-coupled IP QoS control in which QoS signalling messages are first routed to a node that is on the data path.

QoS signalling: signalling mechanism for the detection of backbone network QoS capabilities and the negotiation of QoS guarantees.

Editor's Note: Definitions may need to be removed if not required and other definitions may need to be added if required.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABCF	Access Bearer Control Function
AF	Application Function
AMR	Adaptive Multi Rate (*)
APN	Access Point Name (*)
BCF	Bearer Control Function
BGP	Border Gateway Protocol
BR	Border Router
CAC	Call Admission Control
COPS	Common Open Policy Service protocol
DCCP	Datagram Congestion Control Protocol
Diffserv	Differentiated Services
DSCP	Diffserv Code Point
E2E	End-to-End
ECN	Explicit Congestion Notification
ER	Edge Router
GERAN	GSM EDGE Radio Access Network (*)
GGSN	Gateway GPRS Support Node (*)
HTTP	Hyper Text Transfer Protocol (*)
IMS	IP Multimedia Subsystem (*)
Intserv	Integrated Services
IP-CAN	IP-Connectivity Access Network (*)
LAN	Local Area Network (*)
LDP	Label Distribution Protocol
LSP	Label Switching Path
MBAC	Measurement Based Admission Control
MPLS	Multiprotocol Label Switching Architecture
NSIS	Next Steps in Signalling
PDF	Policy Decision Function
PEP	Policy Enforcement Point
PHB	Per Hop Behaviour
QoS	Quality of Service (*)
RNC	Radio Network Controller (*)
RSVP	Resource ReserVation Protocol (*)
SDP	Session Description Protocol (*)
SIP	Session Initiation Protocol (*)
SNMP	Simple Network Management Protocol (*)
TFT	Traffic Flow Template (*)
TR	Transit Router

* This abbreviation is contained in TR 21.905 [1].

Editor's Note: Abbreviations may need to be removed if not required and other abbreviations may need to be added if required.

4 General requirements

Editor's Note: This section will describe the general requirements for enhancing the E2E QoS concept described in TS 23.207 [4] from a technical and architectural point of view.

4.1 Enhanced requirements for end-to-end QoS

- The end-to-end QoS interworking architecture shall support the provision of guaranteed end-to-end QoS in case all affected backbone and access networks are able to guarantee QoS.

- The end-to-end QoS interworking architecture shall be able to handle the case that a backbone network or the access network of the other endpoint does not guarantee QoS or that there are temporarily insufficient resources although all networks are able to guarantee QoS.

- For some important services with strict end-to-end QoS requirements, such as conversational speech or streaming video, the QoS (such as bandwidth etc.) shall be assured in case of interworking with different IP network domains or backbone networks. In this case, the policing of the E2E QoS in UMTS network may be on a per service (i.e. on the basis of specific flows of IP packets identified by the service) or aggregated flow basis (i.e. on the basis of flows of different users and different services having the same QoS requirements).

- The E2E QoS interworking architecture shall support admission control in all network administrative domains in the path of a flow/aggregate/service subject to E2E QoS guarantees. Admission control should inform service control of the flow about the positive or negative outcome of admission control procedures. Service control at the UMTS edge is responsible for rejecting or releasing a flow/aggregate/service based, among others, on the outcome of admission control.

- The E2E QoS interworking architecture shall be able to support the ability to request resources for a given flow, aggregate or service to satisfy the required QoS derived from actual service needs and/or subscription information. Furthermore, when an interconnecting administrative domain does not provide QoS support, then the edge domains of a flow/aggregate/service need to be aware of the fact that E2E QoS is not really guaranteed for this flow/aggregate/service. In order to achieve this, the E2E QoS interworking architecture should provide means to discover whether one or more administrative domains in the path of a flow/aggregate/service is transparent to (i.e. not considering) QoS information.

- The E2E QoS interworking architecture shall be scalable to support large IP backbones. 'Large' both in terms of topology and link rates (multi-gigabit need to be supported).

- The E2E QoS interworking architecture shall be transport protocol agnostic, i.e. different transport protocols shall be supported (e.g. RTP, MSRP).

- The security, reliability, availability and resilience of the E2E QoS interworking architecture shall be considered.

- The E2E QoS interworking architecture shall be able to interwork with external networks that can report changing network conditions (e.g. link or equipment failures). If there are insufficient resources after changing network condition in the external network, sessions, that cause utilisation to exceed the remaining resources, shall be discontinued in a controlled way.

Editor's Note: How these sessions that cause remaining resources to be exceeded are determined is FFS.

- The E2E QoS interworking architecture shall be able to robustly interwork with external networks that have large fluctuations in traffic load or traffic type mix.

- The E2E QoS interworking architecture shall be able to support E2E QoS regardless of whether the different administrative domains involved in the path of a service use the same QoS provisioning method or different QoS provisioning methods.

- The E2E QoS interworking architecture shall be able to interwork with multi-service networks carrying different traffic types (i.e. in networks where also other traffic than 3GPP traffic is transported).

- When considering interaction between the UMTS network and the external network, the work of the ITU-T, TISPAN and the IETF NSIS working group shall be taken into account.

- Impacts on session establishment delay should be taken into account when considering alternatives for E2E QoS interworking architecture.

- The E2E QoS Interworking architecture shall take into consideration of mobility, simultaneous IP-CAN accessing aspects, e.g. handover between different IP-CANs and selection of IP-CANs in case of multi mode terminals.

- It is preferred that e2e QoS mechanisms developed in ITU-T, TISPAN and/or IETF be adopted rather than a new IP QoS signalling solution being developed by 3GPP. An objective is to align the 3GPP e2e QoS work with the ITU-T, TISPAN and the IETF NSIS working groups.

- The E2E QoS Interworking architecture shall primarily provide a network-to-network-interface between the 3GPP network and external networks. The already existing 3GPP QoS mechanisms shall be reused as much as possible, in particular the existing interface(s) towards the terminal (AF session signalling, bearer signalling). However, some enhancements e.g. to align with ITU-T and TISPAN, may be considered if deemed suitable and feasible for the mobile environment.

4.2 General issues of end-to-end QoS

Editor's Note: This section is for the investigation of the general issues of end-to-end QoS and the clarification of these issues.

4.2.1 Overview

The end-to-end QoS interworking architecture can only provide guaranteed end-to-end QoS in case all backbone and access networks on the path provide QoS guarantees. However, it is possible that a backbone network or the access network of the other endpoint does not guarantee QoS or that there are temporarily insufficient resources although all networks support the end-to-end QoS architecture are able to guarantee QoS. The end-to-end QoS interworking architecture may also try to find alternative paths to the other endpoint. In any case, the network provides the information about the available QoS that can be guaranteed (this can be also none) to the UE.

Editor's Note: How this information is carried to the UE is FFS. For GPRS, existing signalling mechanisms should be re-used as much as possible.

The UE makes the decision to request a service which requires guaranteed end-to-end QoS. Therefore, the UE shall also make the final decision whether to continue with the establishment of the session even if the desired QoS cannot be guaranteed temporarily or QoS cannot be guaranteed at all.

In order to achieve end-to-end QoS guarantees for an IP flow/flow aggregate/service aggregate, all the network administrative domains in the path of such IP flow may need to include the following functionality:

- ability to receive per IP flow/flow aggregate/service aggregate QoS information from a preceding network administrative domain;

- ability to process per IP flow/ flow aggregate/service aggregate QoS information. This is, to provide IP flow admission control based on the IP flow QoS information received from a preceding network administrative domain;

- ability to convey per IP flow/flow aggregate/service aggregate QoS information to a subsequent network administrative domain; and

- ability to receive and react to per IP flow/flow aggregate/service aggregate information from subsequent (down stream) administrative domain on their current QoS support condition.

It is specifically not assumed that the administrative domains use the same QoS provisioning techniques for realizing the above functionality. For example, one administrative domain may rely on on-path signalling approach discussed below, while another domain may rely on off-path signalling approach.

No assumptions are made with regard to the routing topology and configuration in and between the individual administrative domains.

The following general issues need to be solved to identify the requirements for the development of solutions that enhance the end-to-end QoS architecture:

- How are the end-to-end QoS requirements for a service generated and signalled?

- In the case of feedback based solutions, how is the end-to-end QoS support condition for a service signalled?

- How can the solutions provide end-to-end QoS for all applications (IMS and non-IMS applications)?

- How are end-to-end QoS provided for different type of connections (i.e. UE-UE, UE-Server, Server-Server, Server-UE)?
- How is the resource check on the end-to-end path combined with the general IMS session setup?
- What is the impact of insufficient or unavailable external resources?
- In case of off-path signalling, how is the next domain identified?
- How are external resources negotiated and allocated?
- How does dynamic routing impact the developed solutions?

Editor's Note: Additional issues may be identified.

4.2.2 Signaling of QoS requirements

Editor's Note: This section is for the investigation of the generation and signalling of QoS requirements.

In the general case the end-to-end QoS requirements of an application session need to be signalled along the end-to-end path to be able to provide QoS. This QoS requirements information can be in both the application (e.g. IMS) signalling level and the bearer path level. The application signalling level part of this information is available in the application signalling (e.g. SIP/SDP), i.e. bandwidth information and to some extent the QoS class, though it is not possible to differentiate between streaming and conversational. More detailed information may be signalled within the access network, e.g. for GPRS by means of the PDP context QoS parameters (QoS class, transfer delay, error rates). However, within the access network the values for the end-to-end path (especially the value for the end-to-end transfer delay) are not signalled.

In the bearer path level it is possible to convey QoS requirements using service class (i.e. DSCP). Having the service class based QoS requirements in the per packet bearer path level allows the bearer path per packet forwarding mechanisms to perform QoS functionality in line with the application's required bearer path behaviour. Diffserv Service Classes as indicated in [13] provide a universal mapping between QoS requirements and service class (DSCP) although this mapping does not include bandwidth requirements.

It is FFS how the end-to-end QoS values are generated and signalled. In the general case the UE needs to provide such information. For a number of specific services a set of QoS parameters may be standardized and thus already available in the network.

4.2.3 Resource check and IMS session setup

Editor's Note: This section is for the investigation of the possibilities to combine the resource check up with the IMS session setup.

The IMS session setup is based on a clear separation between the IMS session signalling and the allocation of resources. The IMS session setup is started but afterwards set on hold. At this time, both endpoints are responsible for requesting the required resources at least in their access network. The IMS session setup is only successfully finished if both endpoints received sufficient resources.

For the general end-to-end path a number of possibilities exist at which point in time and under which responsibility the external resources are requested. The external resource request may be coupled with the UMTS internal resource request, i.e. with the PDP context establishment. Both endpoints may be responsible for the resource request for the backbone network. Resources may either be requested by one of the endpoints for both directions or by both endpoints in either sending or receiving direction.

It is FFS how the responsibility for the resource request is solved and how the UE can detect that the other endpoint is not able to request resources for the backbone network.

4.2.4 Impact of insufficient or unavailable resources

Editor's Note: This section is for the investigation of the impacts of insufficient or unavailable resources on the IMS session setup.

The UE is responsible to decide if the resources that were granted by the network are sufficient for an application session. As long as only resources of the access network are taken into account, the UE may either accept insufficient QoS or may try to achieve the desired QoS at a later point in time. However, in case of end-to-end resources some more possibilities exist. Resources may be guaranteed by a backbone network but they also may only be statistically granted. It is also possible that there is no feedback at all from a backbone network on the end-to-end path. Consequently, the UE needs to be able to handle a number of cases with some of them being new, like the case that it is not possible to receive guaranteed external resources at all or the case that QoS becomes insufficient during the IMS session.

There are situations when even guaranteed resource in the backbone network or in the access network can be redrawn or made unavailable due to many events, e.g. network failure and urgent network resource re-allocation. In such situations, the network needs to provide the necessary network information to the decision points (network and/or UE) in order that reactive measures can be taken and that the application session is handled appropriately, in line with session policy and user wishes.

4.2.5 Identification of next domain for off-path signalling

Editor's Note: This section is for the investigation of solutions to identify the next domain in case of off-path signalling.

For off-path signalling the next domain needs to be identified by other means than IP routing.

4.2.6 Negotiation and allocation of external resources

Editor's Note: This section is for the investigation of impacts coming from the negotiation and allocation of external resources.

Backbone networks may apply a variety of mechanisms for negotiation and allocation of resources. For instance, a backbone network may support unidirectional as well as bidirectional resource negotiation. Depending on the capabilities of the other endpoint in the IMS session, the usage of such capabilities of backbone networks might allow the provision of end-to-end QoS which otherwise would not be possible.

4.2.7 Provision of end-to-end QoS for non-IMS applications

Editor's Note: This section is for the investigation of impacts coming from the provision of end-to-end QoS for non-IMS applications.

Even though it might be technically possible to provide most applications within the framework of IMS, there may be reasons to provide applications that will benefit from end-to-end QoS outside of the framework of IMS. An operator may for example have a streaming service where the additional complexity and cost of IMS would not be desirable. Other examples are TV and radio services that are provided over the Internet, and which an operator may want to make available for its subscribers. These services may require end-to-end QoS for enhanced end-user reception.

End-to-end QoS architecture used in the 3GPP network need also to comprise support for non-IMS applications.

5 Architectural concept

Editor's Note: This section will describe the different enhanced E2E QoS architectures including interaction with emerging QoS concepts from other standards organizations.

5.1 General end-to-end QoS reference model

5.1.1 Introduction

For describing the concepts of different ways to provide end-to-end QoS, figure 5.1.1.1 below is used as a reference model. The figure shows the location of the IP backbone network and the main interfaces. The IP backbone network provides IP packet forwarding service for the application nodes. *Application nodes* are the domain specific nodes that interface with backbone network, such as GGSN, PDF, etc.

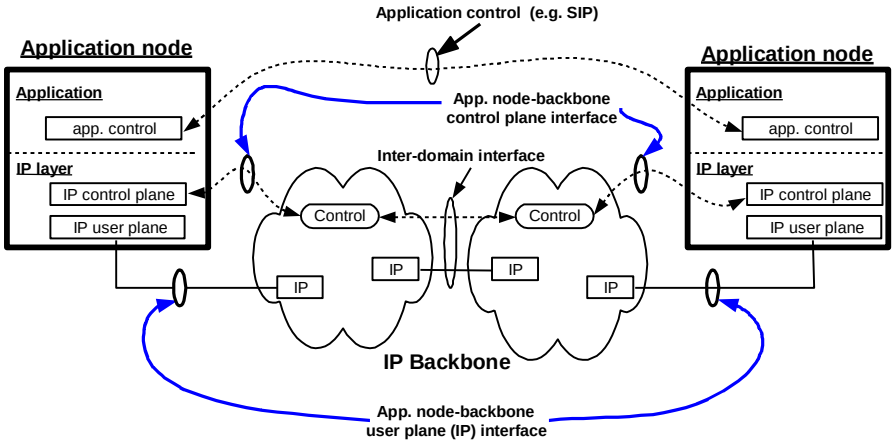


Figure 5.1.1.1: Reference model

The application node to backbone user plane interface is a pure IP level interface that provides the transfer of IP packets between application nodes. The application node to backbone control plane interface allows the communication of application node and IP backbone network. Note that, the communication between the application and the backbone network is also possible. This information exchange helps to provide end-to-end QoS for IP flows between application nodes.

Possible information exchange methods between application node and IP backbone network are:

- no information exchange at all;
- indirect control information is exchanged (e.g. via marking of user plane IP packets);
- explicit control function with aggregated resource reservation; and
- explicit control function with per-flow resource reservation.

The inter-domain interfaces of the IP backbone network, namely the user and control plane interfaces, are to provide the required QoS through multiple backbone IP domains. The application node to application node control interface is out of scope of this document.

A description of the most important provisioning schemes for QoS is given in annex B.

5.2 Connection models

5.2.0 Overview

The following connection models should be studied.

Editor's Note: The following connection models are not exclusive.

Editor's Note: The Figures might need to be updated regarding the IMS clouds.

Editor's Note: The terminology used in this document for the policy control architecture (e.g. functional entities and reference points) should be aligned with the rel-7 study on "Evolution of the policy control and charging" (TR 23.803).

5.2.1 UE-UE connection via interconnected proxying networks

5.2.1.1 General

In this case, a UE served by an application server connected to a remote UE via one or more interconnected networks which proxy signalling (e.g. interconnected IMS networks). In this case, mechanisms are required within intermediate networks for policy control interactions between the proxy and the underlying IP backbone network.

Two cases are possible depending upon whether the media packets are forced to follow the same path (via the same intermediate network) as the control packets or are allowed to take a different (more efficient/direct path). Both cases are valid and should be studied.

The pros and cons of the two approaches seem to depend on which charging models are to be adopted by interconnected networks.

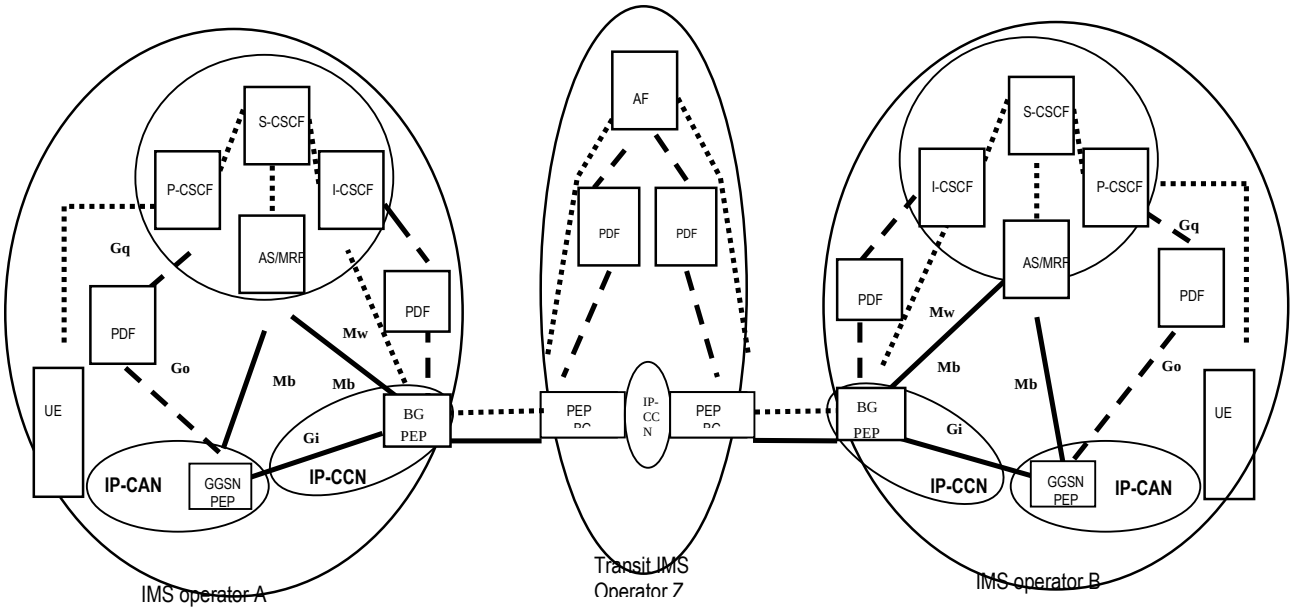
5.2.1.2 Control and media via the same intermediate network

In this connection model the control and media packets are routed through the same intermediate network. This implies a requirement to force the media to follow a particular path based on the routing of the application layer signalling.

By forcing media to follow the same path as the control, it is possible to treat each session as an individual entity. This approach allows application (e.g. IMS) interconnect agreements to be modelled on those used today for Circuit Switched calls. Charging by time, by data volume and by service is possible with this approach. Having PDF and PEP functions under control of an intermediate network AF/CSCF allows for policy control, QoS (bandwidth etc.) reservation and call admission control, if required by an Operator.

The main disadvantages of forcing media to follow the same path as the control are the inefficiencies that might be introduced in terms of the path taken by the media packets.

Figure 5.2.1.2.1 shows one example of a UE-UE connection via interconnected proxying networks where the service is based on IMS.



NOTE 1: The IP-CCN, BG and BG PDF in the networks of IMS operator A and B that are shown in Figure 5.2.1.2.1 are not currently included within the 3GPP Architecture, but they are included here for better understanding of the problem domain. Only those parts of them contributing to E2E QoS would be within the scope of this study.

NOTE 2: Some functions exist in 3GPP specifications that may be similar to the BG entity in the figure. E.g. the GPRS BG and SEG as specified in TS 33.210 and the BGW for the Gp interface as specified in TS 23.060.

NOTE 3: There may be more than one border gateway (BG) element at the edge of the network. The representation of a single element in the figure above is for simplicity and does not imply that it is required for the signalling and the media to traverse the same border gateway.

Figure 5.2.1.2.1: UE-UE connection via interconnected IMS networks with control and media via the same intermediate network

Several entities are required in the interconnected proxying networks, e.g. (proxy) AF and PDF, to provide QoS in the corresponding backbone IP networks. QoS negotiation among the different domains is done by (proxy) AFs and backbone IP network can provide QoS. The way to provide QoS within the backbone IP network depends on the QoS policy of the intermediate operator.

IP-CAN specific QoS mechanism is used within IP-CAN for QoS provision. The PEP in GGSN and BG may be part of the QoS mechanism for the IP-CCN. The details of the QoS mechanism for the IP-CCN is FFS.

5.2.1.3 Control and media via different intermediate networks

In this connection model the control and media packets are not routed through the same intermediate network. The media packets could route directly between the IP-CANs or via a different intermediate network.

The main advantage of allowing the media to take the most direct/efficient path is potentially lower cost and superior quality of experience (less delay etc.)

If media packets are allowed to take the most direct path between UEs then it is not clear what charging model can be used other than charging by aggregate between operators.

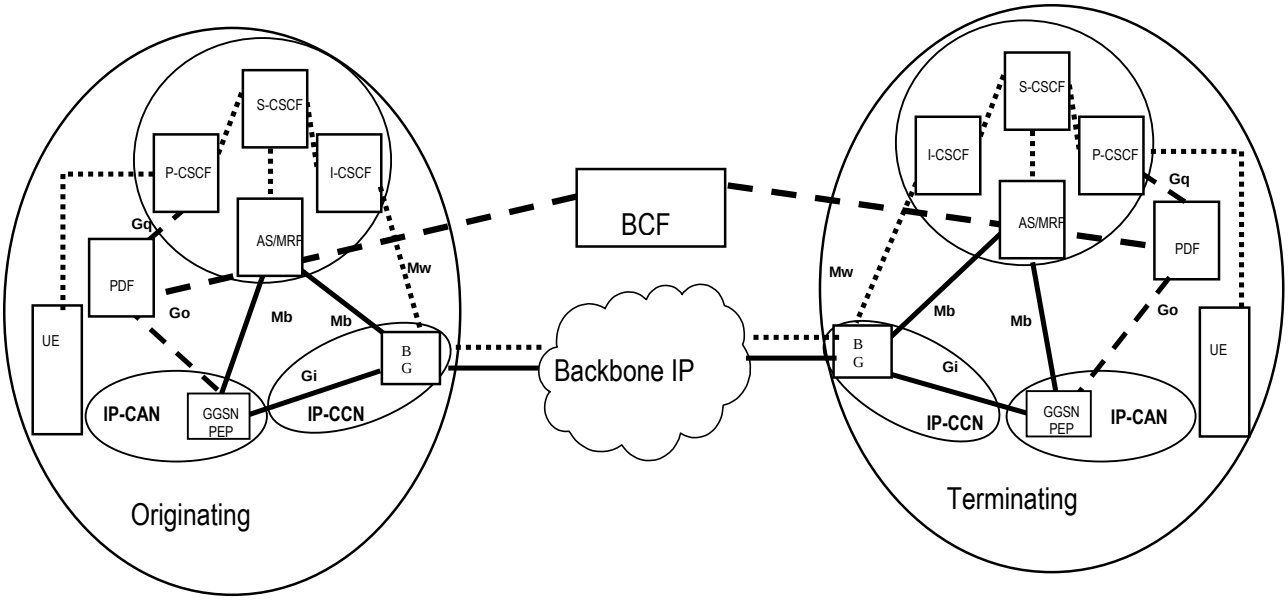
In this case the connection models of 5.2.2, 5.2.3 or 5.2.4 apply.

5.2.2 UE-UE connection via backbone IP networks with off-path QoS signalling

UE served by IMS connects to peer UE via a backbone IP network with off-path QoS signalling. This signalling is transferred between policy decision points, i.e. between PDF and BCF. The backbone IP network is an abstraction that represents the set of inter-connecting network administrative domains between two IMS systems.

BCF performs QoS management within the backbone IP network. Gu interface is defined as the interface between the PDF in IMS and BCF in the backbone IP network.

Editor's Note: Definitions and more detail explanations of the BCF and Gu interfaces would be described in section 3 or 5.



NOTE 1: The IP-CCN and the BG in the originating and terminating operator are not currently included within the 3GPP Architecture, but they are included here for better understanding of the problem domain. Only those parts of them contributing to E2E QoS would be within the scope of this study.
NOTE 2: Some functions exist in 3GPP specifications that may be similar to the BG entity in the figure. E.g. the GPRS BG and SEG as specified in TS 33.210 and the BGW for the Gp interface as specified in TS 23.060.
NOTE 3: There may be more than one border gateway (BG) element at the edge of the network. The representation of a single element in the figure above is for simplicity and does not imply that it is required for the signalling and the media to traverse the same border gateway.
NOTE 4: How QoS guarantee shall be achieved within the IP-CCN shall be studied.

Editor's Note: It is for further study whether the BG element is a PEP or not.

Figure 5.2.2.1: UE-UE connection via backbone IP networks with BCF

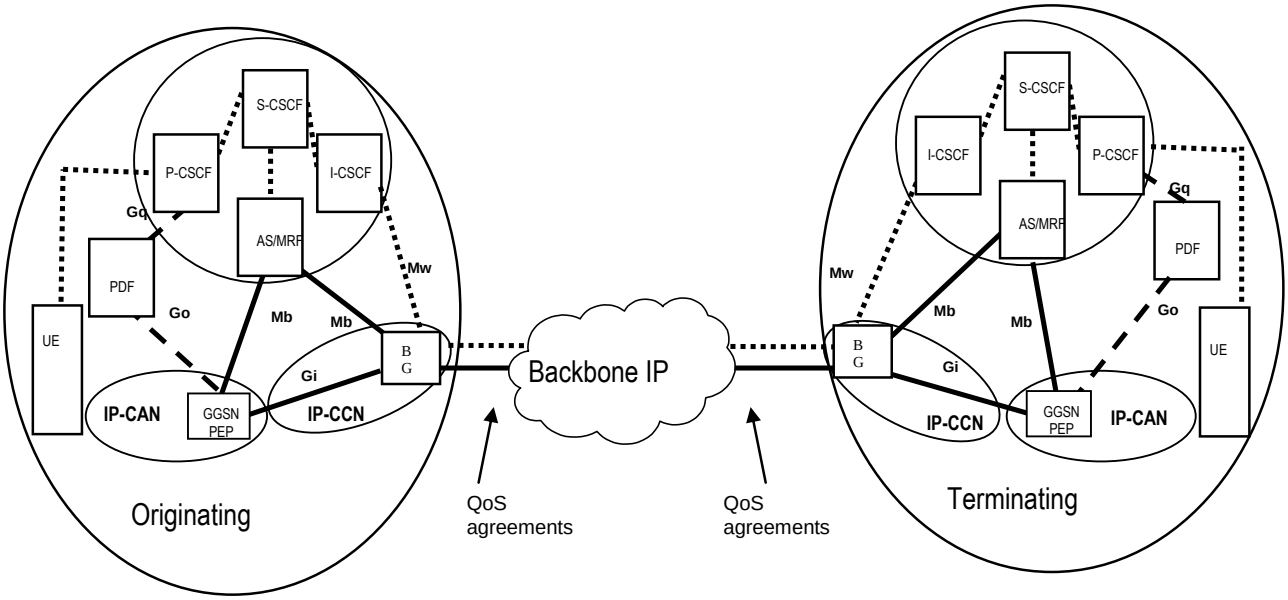
This connection model is an extension of the IMS Rel-6 one to include a horizontal QoS signalling component between the IMS PDF and an equivalent functional entity, named BCF, in the backbone inter-connecting IP network.

Any vertical interface between the BCF in the backbone IP network and other nodes within this network are considered outside the scope of this TR.

The BCF negotiates QoS with the PDF of the IP-CAN. The way to provide QoS within the backbone IP network depends on the QoS policy of the backbone operator.

5.2.3 UE-UE connection via backbone IP networks without QoS signalling

UE served by IMS connects to a remote UE via one or more backbone IP networks. QoS relationships are established between the different backbone IP network providers, between backbone IP network providers and PLMN operators and between different PLMN operators, without requiring per-session signalling. The backbone IP networks may be administered by PLMN operators.



NOTE 1: The IP-CCN and the BG in the originating and terminating operator are not currently included within the 3GPP Architecture, but they are included here for better understanding of the problem domain. Only those parts of them contributing to E2E QoS would be within the scope of this study.
NOTE 2: Some functions exist in 3GPP specifications that may be similar to the BG entity in the figure. E.g. the GPRS BG and SEG as specified in TS 33.210 and the BGW for the Gp interface as specified in TS 23.060.
NOTE 3: There may be more than one border gateway (BG) element at the edge of the network. The representation of a single element in the figure above is for simplicity and does not imply that it is required for the signalling and the media to traverse the same border gateway.
NOTE 4: How QoS guarantee shall be achieved within the IP-CCN shall be studied.

Editor's Note: It is for further study whether the BG element is a PEP or not.

Figure 5.2.3.1: UE-UE connection via backbone IP networks without QoS signalling

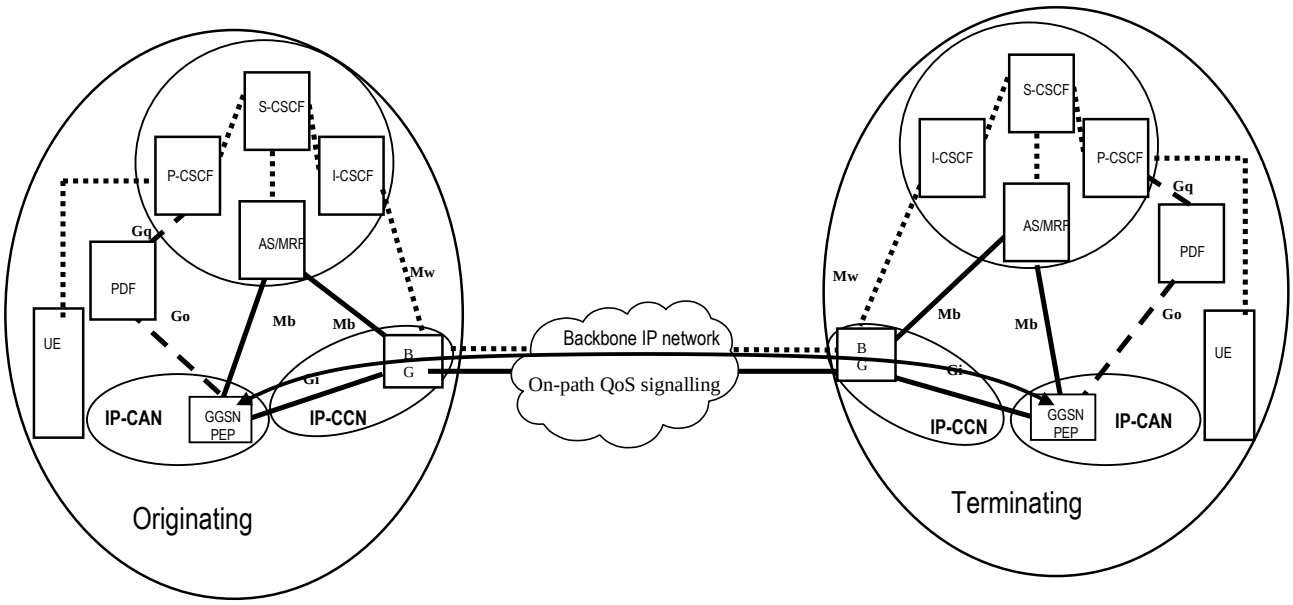
There is no means to signal with the routers regarding On-Path IP QoS control. The routers transit user packets based on the static configuration depending on the QoS policy of the backbone operator. QoS is provided based on the static QoS policy in backbone IP network.

There may be SLAs established between the IP-CAN and Backbone IP Network or its aggregates based on DiffServ Service Classes [13]. Under such deployment scenarios, network usage feedback on the bearer path could be used together with QoS resource control within the IP-CAN network to provide resource availability information into IMS session control decisions.

5.2.4 UE-UE connection via backbone IP networks with on-path QoS signalling

UE served by IMS connects to a remote UE via one or more backbone IP networks with on-path QoS signalling. The backbone IP networks may be administered by PLMN operators.

In on-path signalling model, QoS signalling messages are transferred between PEPs through routers that process user data packets.



NOTE 1: The IP-CCN and the BG in the originating and terminating operator are not currently included within the 3GPP Architecture, but they are included here for better understanding of the problem domain. Only those parts of them contributing to E2E QoS would be within the scope of this study.

NOTE 2: Some functions exist in 3GPP specifications that may be similar to the BG entity in the figure. E.g. the GPRS BG and SEG as specified in TS 33.210 and the BGW for the Gp interface as specified in TS 23.060.

NOTE 3: There may be more than one border gateway (BG) element at the edge of the network. The representation of a single element in the figure above is for simplicity and does not imply that it is required for the signalling and the media to traverse the same border gateway.

Editor's Note: It is for further study whether the BG element is a PEP or not.

Figure 5.2.4.1: UE-UE connection via backbone IP networks with on-path QoS signalling

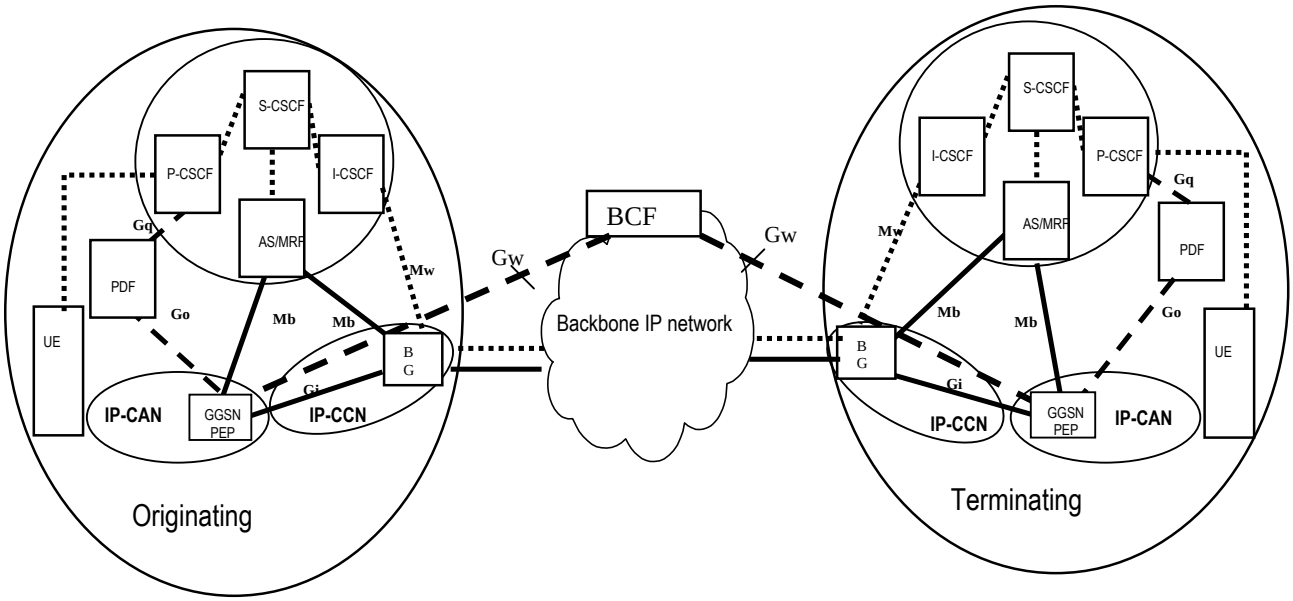
The PEP in the IP-CAN and the routers in the IP-CCN and the backbone network could be able to handle signalling regarding On-Path IP QoS control (e.g. RSVP, RSVP-TE, Aggregate-RSVP or MPLS-TE technology). The routers receive On-Path IP QoS control messages from IP-CAN or another backbone IP network. In order to provide QoS in the IP-CCN, on-path signalling handling can be selectively enabled on the Border Gateway and/or other nodes based on topology and E2E QoS requirements.

IP-CAN specific QoS mechanism is used within IP-CAN for QoS provision.

5.2.5 UE-UE connection via backbone IP networks with hybrid-path QoS signalling

UE served by IMS, or by UMTS only, connects to peer UE via a backbone IP network with hybrid-path QoS signalling. Gw reference point is defined as an interface between GGSN and the resource controller in backbone IP network, i.e. between GGSN and BCF. In the case of the UE served by IMS, i.e. some PDF is available in sessions and the GGSN is profiled with PEP function, Gw also is treated as an interface between PEP and BCF. Gw reference point is used for transferring the QoS signalling. The backbone IP network is an abstraction that represents the set of inter-connecting network administrative domains between two IMS systems.

Editor's Note: Definitions and more detail explanations for Gw interface would be described in section 3 or 5. .The procedures on Gw interface should be aligned with PCC [i.e. TR 23.803] once it is finalized. QoS guarantee in IP-CCN is FFS.



NOTE 1: The IP-CCN and the BG in the originating and terminating operator are not currently included within the 3GPP Architecture, but they are included here for better understanding of the problem domain. Only those parts of them contributing to E2E QoS would be within the scope of this study.

NOTE 2: Some functions exist in 3GPP specifications that may be similar to the BG entity in the figure. e.g. the GPRS BG and SEG as specified in TS 33.210 and the BGW for the Gp interface as specified in TS 23.060.

NOTE 3: There may be more than one border gateway (BG) element at the edge of the network. The representation of a single element in the figure above is for simplicity and does not imply that it is required for the signalling and the media to traverse the same border gateway.

Editor's Note: It is for further study whether the BG element is a PEP or not.

Figure 5.2.5.1: UE-UE connection via backbone IP networks with BCF

Different from off-path mode, QoS negotiation in this mode would be initialised by GGSN, not by PDF. In the hybrid-path, the GGSN is able to identify the BCF domain by means of IP routing. This allows GGSN to be able to connect the BCF whether the PDF is available or not. In the case there is no PDF, it is required that the GGSN knows the next hop in the backbone network based on some IP-CAN bearer information, e.g. APN for GPRS. PDF would not be modified or extended functionally in this mode.

5.3 Issues of connection models

Editor's Note: This section is for investigation of the connection models from the perspective of QoS and clarification of issues. Details are FFS.

5.3.1 Type of information to be exchange end to end

In order to guarantee End-to-End QoS, a connection model should implicitly or explicitly:

- convey abstract QoS information. This is the QoS parameterisation should be independent of the actual QoS solutions used at lower levels within the network, and of the transport technologies used in the network.
- convey appropriate QoS information to describe the QoS requirements of the IP flow. The actual information may depend on the nature/type of the flow (e.g. RT, streaming, etc).
- allow abstraction in the definition of a flow. E.g. it should be possible to define a flow as:
  - all packets with the same source IP address;
  - all packets with the same source and destination IP addresses;
  - all packets with the same five-tuple: source and destination IP addresses, originating and destination port numbers and protocol ID;

- etc.

- it may be appropriate to convey QoS related information to describe the current network QoS condition along the bearer path. This information should be available whenever the specific flow wants to utilize the QoS resources of the flow's bearer path.

Flow abstraction should be provided in a per flow basis. i.e. the "definition" of a flow itself needs to be signalled through the path of the QoS signalling when establishing the flow.

5.3.2 Information stored in PDF after negotiation

After QoS negotiation with the backbone IP network, the PDF may store the information during the session about the backbone network and QoS, which could include:

- QoS information negotiated with the backbone network:
  - bandwidth allowed in the backbone network, including uplink and down link;
  - more information is TBD.
- backbone network information:
  - negotiation mode (i.e. on-path mode or off-path mode);
  - BCF IP address if the negotiation mode is off-path;
  - more information is TBD.

5.3.3 Usage of QoS signalling

In order to guarantee End-to-End QoS, QoS signalling through the backbone IP network(s) plays an important role in some of the models presented in this TR. For these models QoS signalling is especially important for scenarios in which the backbone IP network(s) is not owned or managed by the PLMN operators of the IP-CANs.

QoS signalling through the backbone IP network(s) provides:

- means for detection of backbone IP network capabilities regarding provisioning of guaranteed QoS;
- means for negotiation of QoS requests according to policies and available resources of the backbone IP network(s);
- flexibility regarding the selection of the route and the QoS provisioning method in the backbone IP network(s);
- means for fast and accurate provision of information about changes of the conditions on the path caused by a backbone IP network;
- means for provision of additional information that may be required in the backbone IP network(s) to provide QoS like information describing the originating IP-CAN operator and the traffic. Such information may be required by an backbone IP network for authentication, authorization, accounting on a per operator basis.

5.4 Architecture for off-path IP QoS interaction between UMTS network and external IP network

5.4.1 General

This section describes an architecture for off-path QoS interaction between UMTS and an External IP network providing QoS-enabled IP transport services.

To provide IP QoS end-to-end, it is necessary to manage the QoS within each domain. In UMTS network, to enable coordination between events in the application layer and resource management in the IP bearer layer, a logical element, the Policy Decision Function (PDF), is used as a logical policy decision element. It is also possible to implement a

policy decision element internal to the IP BS Manager in the GGSN. In the external IP network, a logical element, the Bearer Control Function (BCF) is used to control the external IP bearer service path.

When resources not owned or controlled by the UMTS network are required to provide QoS, it is necessary to interwork with the external network that controls those resources. One alternative to provide highly ensured end-to-end QoS capability for realtime services is to interwork with external IP network, using interaction between the Policy Decision Function and the Bearer Control Function.

5.4.2 Description of functions

5.4.2.1 QoS management functions for off-path end-to-end IP QoS in the UMTS network

Policy Decision Function (PDF) is as defined in TS 23.207 [4]. In addition, it is responsible for communication with BCFs in interconnecting networks via the Gu reference point.

The PDF makes policy decisions based on information obtained from the AF and the result of interacting with the other related BCF.

One way in which the PDF can discover its adjacent BCF is by using a static configuration mechanism in the PDF. For example, the PDF can find the appropriate BCF through static configuration of the FQDN or IP address of the BCF which manages the external gateway router which interacts with the GGSN. For load sharing and redundancy, if the GGSN in the UMTS network is connected to redundant external gateway routers which are managed by redundant BCFs, the multiple BCFs' addresses are configured in the PDF. The policy to select the appropriate BCF is decided by the operator's redundancy policy and the equipment capabilities.

5.4.2.2 QoS management functions for off-path end-to-end IP QoS in the external network

Bearer Control Function (BCF) is the alias of a logical function element in external network which performs QoS control within the external IP network.

For load-sharing and redundancy reasons multiple BCFs may be provided in each external IP network.

Editor's Note: It is FFS how a configuration with multiple BCFs should look like and how they interwork with the PDF (e.g. to coordinate resources etc).

The techniques and mechanisms in the BCF and IP backbone required for performing QoS control together with the interface(s) between the BCF and the IP Backbone are out of scope of this TR.

5.4.2.3 Interaction between UMTS network and external networks

Within the UMTS network, there is resource management performed by various nodes in the admission control decision. The resources considered here are under the direct control of the UMTS network.

In the external networks, it is also necessary to perform resource management to ensure that resources required for a service are available. Where the resources for the IP Bearer Service to be managed are not owned by the UMTS network, the resource management of those resources would be performed through an interaction between the UMTS network and that external network.

When interaction is needed between the UMTS network and the external network, resource requirements are explicitly requested and either granted, negotiated or rejected through the exchange of signalling messages between PDF and BCFs in the external network. The interface between PDF and the BCF element in backbone IP network, named the Gu reference point, may transfer QoS and other information which can be used for policy decisions.

Before sending the QOS request, the PDF shall choose the connected external network by which the media data can be transferred to the terminating nodes. So the PDF should be profiled at least with the following information:

- a list of external networks to different terminating IMS domains.
- a list of alternative external networks to the same IMS domain.

- the property of any external network in the list, which may include:
  - on-path or off-path QOS management architecture;
  - the IP address of BCF to access if in off-path.

Editor's Note: It is FFS how the PDF choose the connected external network and how links are configured for the off-path scenario. Does the signalling (Gu) traffic and the media use the same or different links? How are these links negotiated among the different networks?

5.4.3 Enhanced capabilities of functional elements

This section provides functional descriptions of enhanced capabilities in GGSN, PDF, and AF.

5.4.3.1 GGSN

The functionality is the same as defined in TS 23.207 [4].

5.4.3.2 PDF

Service-based Local Policy Decision Point

- The PDF shall exchange the QoS information with the other related BCF via the Gu interface.

5.4.4 Reference points between functional elements

5.4.4.1 Go reference point (PDF - GGSN)

The functionality is the same as defined in TS 23.207 [4].

5.4.4.2 Gq reference point (PDF - AF)

The functionality is the same as defined in TS 23.207 [4].

5.4.4.3 Gu reference point (PDF - BCF)

5.4.4.3.1 Gu functional requirements

The Gu reference point is used for exchange of QoS information between PDF and BCF element in backbone IP network.

5.4.4.3.2 Information exchanged via Gu reference point

Service information:

The service information below is derived from Gq reference point, which may include:

- session Id (to uniquely identify the session).
- information defining the IP flows of the media stream. E.g.
  - direction (bi-directional, uplink / downlink);
  - 5-tuple (source/destination address and port number, protocol Id);
  - indication of the maximum and/or mean bandwidth required.
- an indication of the requested type of service information per service-flow.

Editor's Note: The information passed over the Gu interface may also include other information required to negotiate resources in the external IP networks.

Operator/network information:

This information is used to identify whether the request or response signalling is from the agreement subscribers, which may include:

- PDF IP address, or PDF fully qualified domain name (in the signalling from PDF to BCF);
- BCF IP address (in the signalling from BCF to PDF).

The result of Session Admission Control (SAC):

The result of SAC by PDF and BCF should be sent via the Gu interface.

5.5 Architecture for on-path IP QoS interaction between UMTS network and external IP network

5.5.1 Overview

This section describes an architecture for on-path QoS interaction between UMTS and an External IP network providing QoS-enabled IP transport services.

5.5.2 RSVP

5.5.2.1 General

This section describes RSVP and some of the extensions that have been made to RSVP that meet a number of requirements such as improving its scalability and security characteristics. In this scenario the GGSN acts as an RSVP Sender and Receiver.

RSVP [6] is a control signalling protocol that requires the introduction of states for specific information flows, although reservation states are "soft" in that they are regularly renewed by messages sent from the initiator of the reservation request. If not renewed, the reservations are timed-out. Resources are reserved for forwarding packets meeting specified criteria (protocol id and port number) from a specific destination address to the initiator of the reservation. Receivers initiate requests for resource reservations along the path that the packets will follow. Nodes which do not support RSVP pass on the reservation request and so there is no guarantee that the path will be fully reserved, although an indication is sent to the reservation initiator that a non-RSVP link has been encountered. The resources need to be available and access policy conditions have to be met for a reservation to be successfully applied. The Sender advertises a data flow by sending a Path message to the receiver of the data flow. The Receiver of the data flow may initiate a reservation for the data flow by sending a Resv message. The Resv message follows the Path message upstream hop-by-hop using the installed path states. The integrity and authentication of RSVP messages can be ensured using the RSVP Integrity object as described in RFC 2747 [27].

A Policy Data object, identifying a user or an account for example, can be included to control reservation access and usage policy [12]. RFCs 2752 [29] and 2872 [30] further define how users and applications can be identified and authorised to make resource reservations.

Reservations can be aggregated over a single RSVP reservation which dynamically adapts to the characteristics of the reservations being aggregated [16]. Aggregation can reduce the load of processing many independent reservations on the routers on the aggregation path as long as the aggregate reservation is not adapted to every individual reservation but modified less frequently. Algorithms and policies for predictive reservations are described in RFC 3175 [16]. Differentiated Services techniques for packet classification and forwarding behaviour are used such that a number of aggregated reservations may be established between a pair of routers, each corresponding to a certain class of traffic and identified by a Differentiated Services codepoint. A number of possible traffic classifications are possible ranging from mapping all individual RSVP reservations to one DS codepoint and per-hop forwarding behaviour, through mapping all Guaranteed Service reservations to one DS codepoint and all Controlled Load reservations to another, to in addition using policy information to classify traffic.

It is necessary to ensure that the data packets associated with an aggregated reservation follow the path of the aggregate reservation using a technique such as IP-in-IP tunnels, GRE tunnels, or MPLS. This is because the aggregate RSVP

Path messages contain the IP addresses of the aggregating and de-aggregating routers rather the IP addresses of the individual end-to-end flows as is normally the case in RSVP. MPLS has the advantage of allowing traffic engineering.

It is also possible to use the Resource Management in Diffserv (RMD) concept, which was introduced as a possible method for dynamic admission control for Diffserv [31], with RSVP. In some of the nodes or in the nodes within a network region, simplified RSVP operation is used: storing only aggregated reservation states and using a simple resource management function in these nodes.

5.5.2.2 Description of functions

5.5.2.2.1 QoS management functions for RSVP based on-path end-to-end IP QoS in the IP-CAN

IP-CAN Gateway (GGSN) is responsible for transmitting and receiving RSVP messages to be used for on-path signalling with the external network. To that end, it may operate either as:

- An RSVP node on the end-to-end RSVP signalling path. This may be the case, for example, when the UE supports the initiation and termination of RSVP signalling, as defined in TS 23.207 [4]. The IP-CAN Gateway behaves as an RSVP node which receives, processes and transmits RSVP messages. RSVP reservations handled by the IP-CAN Gateway are per-flow reservations; or

- An RSVP aggregation node on the end-to-end RSVP signalling path. This may be the case, for example, when the UE supports the initiation and termination of RSVP signalling, as defined in TS 23.207 [4]. The IP-CAN Gateway behaves as a RSVP Aggregator/Deaggregator node [16]. The IP-CAN Gateway handles per-flow reservation on the IP-CAN side and handles aggregate reservation on the external network side.

And/or operate as:

- An RSVP Proxy. This is the case when RSVP signalling is not initiated/terminated by the UE. The IP-CAN Gateway acts as the RSVP signalling end-system and initiates/terminates RSVP signalling on behalf of the Policy Decision Function. The IP-CAN Gateway may initiate/manage per-flow reservations or may initiate/manage aggregate reservations. Initiation/Maintenance/Tear-down of reservations is based on resource requests received from the Policy Decision Function.

According to the exchanged signalling with the external IP network, the IP-CAN gateway may communicate with the Policy Decision Function that resources cannot be committed.

5.5.2.2.2 QoS management functions for RSVP based on-path end-to-end IP QoS in the external network

IP Backbone Edge Router is the function which exchange RSVP signalling with the IP-CAN gateway.

5.5.2.2.3 Interaction between the IP-CAN and external networks

Within the IP-CAN, there is resource management performed by various nodes for end-to-end QoS support. The resources considered here are under the direct control of the IP-CAN operator.

When interaction is needed between the IP-CAN network and the IP Backbone network, resource requirements are determined by the IP-CAN gateway and explicitly requested and either granted, negotiated or rejected through the exchange of RSVP signalling messages between IP-CAN gateway and IP Backbone Edge Router. In the case of GPRS, the interface between the GGSN and the Provider Edge element in backbone IP network is the Gi reference point.

5.5.2.3 Enhanced capabilities of functional elements

This section provides functional descriptions of enhanced capabilities in GGSN.

5.5.2.3.1 GGSN

The functionality is as defined in TS 23.207 [4] and in section 5.5.2.2.1 above.

5.5.2.4 Reference points between functional elements

5.5.2.4.1 Go reference point (PDF - GGSN)

The functionality is the same as defined in TS 23.207 [4].

5.5.2.4.2 Gq reference point (PDF - AF)

The functionality is the same as defined in TS 23.207 [4].

5.5.2.4.3 Gi reference point (GGSN - PE)

5.5.2.4.3.1 General

This functionality is as defined in TS 23.207 [4].

5.5.2.4.3.2 Gi functional requirements

The Gi reference point is used for exchange of QoS information between GGSN and IP Backbone Edge Router.

5.5.2.4.3.3 Information exchanged via Gi reference point

Service information:

The information exchanged via the Gi reference point includes:

- Information characterising the set of packets benefiting from the RSVP reservation. In the case of per-flow reservation, this will effectively be the 5-tuple (source/destination address, source/address port number, protocol Id) encoded over the RSVP IPv4/IPv6 Session object and the RSVP IPv4/IPv6 Filter-Spec/Sender-Template objects. In the case of aggregate reservation as per RFC 3175 [16] this will be the 3-tuple (source/destination address, DSCP) encoded over the RSVP-Aggregate-IPv4/IPv6 Session object and the RSVP-Aggregate-IPv4/IPv6 Filter-Spec/Sender-Template objects.
- Information characterising the QoS requirement (Intserv service type, bandwidth).
- Optional, credentials which can be used by the IP Backbone to identify the network generating the RSVP reservation request as a party authorised to make such RSVP reservations.

5.5.3 MPLS-TE

This section describes the MPLS-TE.MPLS-TE defines the concept of Label Switched Path (LSP) priority, which is used to set up LSP priority with some resource, and allows higher LSP (i.e. with the higher priority) to grab the resource of lower LSPs. This mechanism can ensure that:

- in the case all of the resource of higher LSP are used out, there still are resource reserved by the lower LSP.
- important LSP will always set up the optimum path without the restriction of available reservations.
- while the LSP reroutes the path, important LSP shall have priority of first routing.

MPLS-TE defines 8 priority classes, which from the highest '0' to the lowest '7', and 2 types, which are the setup priority and hold priority. Setup priority controls the admission and sets up LSP with the resource which have not been set up, and hold priority controls the admission to the resource which have been set up. During the setup of a LSP, if the resource is insufficient, the setup priority of the LSP should compare with the hold priority of the other LSPs, which have been setup, to decide whether the LSP is more important and then grab the other LSPs' resource. For further description of MPLS-TE see RFC 3346 [32].

5.5.4 Feedback based call admission control

End-to-end QoS provisioning in the current 3GPP standard as specified in TS 23.107 [3] and TS 23.207 [4] uses Diffserv mechanisms on the IP bearer level, for example Service Level Agreements (SLAs), to ensure QoS. The

involved networks are assumed to be at least statically dimensioned to cope with the agreed traffic volumes, but this is not limited to static SLAs, when dynamic SLAs are used, this mechanism will continue to function without modification in the more dynamic environment. Traffic exceeding these agreed limits is expected to be handled using normal Diffserv traffic shaping functions, e.g. dropping of random packets. Such mechanisms is however not always very friendly to real-time traffic e.g. flows used to carry IMS IP telephony calls. Instead a mechanism capable of either blocking a real-time flow completely or letting it through completely would be a more appropriate mechanism to control the traffic volumes. The feedback based call admission control (CAC) function described below has such a characteristic.

A solution which can prevent overload situations of real-time traffic in intermediate networks employs a CAC function in the PLMN, e.g. in the GGSN or in a node in the IMS Core. The CAC function is queried at session activation. The CAC function must also be made aware of the congestion situation in any intermediate networks along the end-to-end path. A method to provide the CAC function with such information is by feedback from the intermediate networks. Congestion or bandwidth limitations in these networks are indicated by a remarking of either the DS-field or the ECN-field, in the TOS byte (for IPv4), in IP headers of packets forwarded through congested points of these networks. Remarking in a node should start when bandwidth resources get close to its limit, i.e. before actual congestion occurs.

For the remarking solution there is only a logical or implicit relation between the control planes in the application nodes and the nodes in intermediate IP backbones, i.e. there is no specific signalling protocol used.

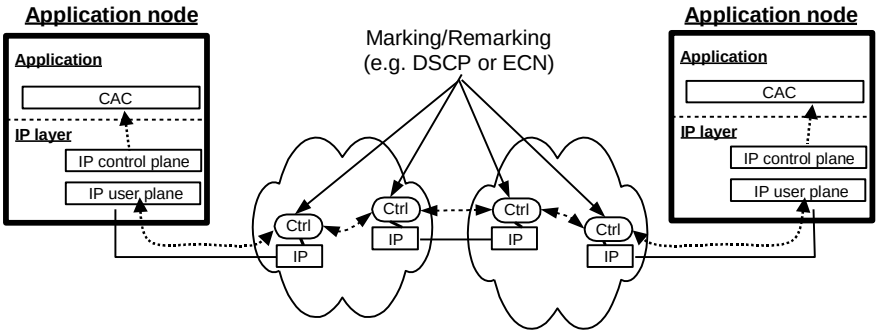


Figure 5.5.4.1: Feedback based QoS provisioning

The CAC function uses feedback information to check for congestion based on an operator-specific threshold. When sessions for outgoing calls are established, the current congestion conditions for the path to the destination network is checked before the session is finalized. In case of resource constraints, the call can be blocked depending on policy. This mechanism can also be used to allow more urgent sessions to be established in place of the normal sessions, this decision depends on the policy in place at the decision points.

Diffserv remarking can be applied locally within domains and between domains (within SLAs) if operators agree, but having end-to-end usage of Diffserv marking will be beneficial, as recommended by Diffserv Service Classes [13]. ECN has end-to-end semantics, since ECN's function is to indicate congestion, the segments of the end-to-end bearer path that wants to have its network congestion information be used will need to support ECN functionality. For each network segment it is possible to document in the SLA between adjacent administration domains, whether ECN indication is used. Network segments that do not use ECN indications will need to guarantee that congestion will not occur when the offered traffic conforms to the SLA. For further description of Diffserv remarking see RFC 2475 [9] and RFC 3260 [28].

When Feedback based Call Admission Control is used, the Call Admission Control can be done using information from the bearer path network layer.

5.5.5 NSIS

The Next Steps in Signalling (NSIS) working group of the IETF is currently working on the standardization of an IP signalling protocol, with QoS as the first use case. The set of requirements can be found in RFC 3726 [35], whilst the framework for the protocol design is given in RFC 4080 [19].

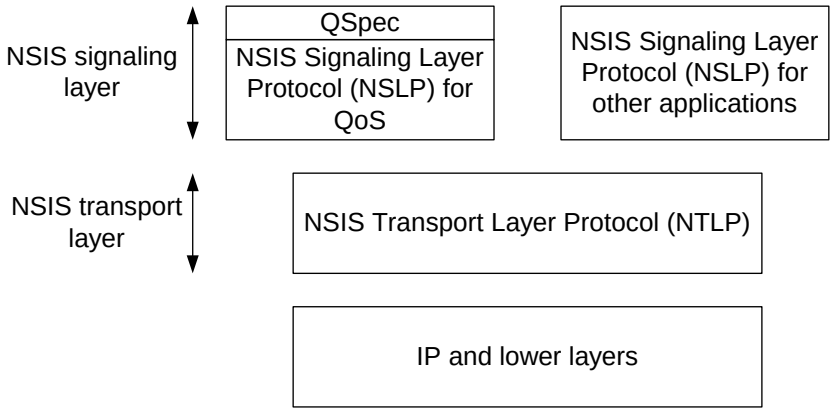


Figure 5.5.5.1 – NSIS Protocol Stack

The NSIS QoS solution consists of a pair of protocols, where one protocol encodes the transaction semantics and the other protocol manages transport and routing, including routing in complex topologies and automatic adaptation to topology changes. Many of the basic design principles of the combination are similar to RSVP. These protocols provide a control signalling protocol that installs "soft" state into devices in the network. Admission control and policy control conditions need to be met before a reservation can be applied.

The protocol that defines transaction semantics for QoS within the NSIS protocol suite is the QoS NSLP (NSIS Signalling Layer Protocol), and is described in [20].

The QoS NSLP is able to have defined interactions with a variety of QoS models (i.e. it is not restricted to IntServ). It is also compatible with a variety of resource management mechanisms, whether they be per micro-flow-based, tunnelled or using DiffServ aggregation.

The QoS Specification (QSpec) is used to provide the resource description, related resource management control information, etc, and is described in [22]. This has some similarities to the functionality provided in RSVP by using similar parameters. A base set of elements for describing a reservation are provided, with the scope to augment these with additional objects for specific QoS models. The working group has recently adopted work to describe how specific QoS models can be supported by the QoS NSLP, e.g. for RMD (Resource Management for DiffServ) [31].

The QoS NSLP has a variety of deployment models, which is a significant distinction from RSVP. Whereas RSVP supports only receiver initiated signalling, QoS NSLP also provides for sender initiation. In addition, it allows an (on-path) proxy to initiate signalling, and so does not require the data sender and/or receiver to support the QoS signalling protocol. The QoS NSLP also allows for reservations to not necessarily be end-to-end and allows in-call bandwidth modification. The protocol is capable of working in scenarios where it is not supported at every node along the path, and will have the capability of detecting QoS-unaware regions. The QoS NSLP can also provide part of the solution for two phase commit reservation operations.

The QoS NSLP provides strong security for signalling messages. Because this functionality is built on standard protocols (such as TLS and IPsec), standard key management mechanisms can be used.

The QoS NSLP works with the NTLP to provide a complete signalling solution for on-path scenarios. However, nothing prevents the QoS NSLP being used in other scenarios where the same transaction semantics and QoS models are required. Indeed, the standardised QoS NSLP could be used as part of an off-path solution. The transport functions could be provided by an adaptation of the NTLP. The advantage of such a solution is that it would have consistent interactions with the on-path protocol as part of an end-to-end solution, and would avoid the need to support different protocols for QoS reservation transactions.

This protocol provides facilities for reuse of standard mechanisms for signalling security (e.g. TLS, IPsec). The NTLP is designed to be robust, and provides efficient mechanisms for signalling reliability and resistance to denial of service attacks. The NTLP can support a variety of signalling applications in addition to QoS, such as firewall control and metering. The NSIS protocols are designed to operate in both IPv4 and IPv6 networks.

5.6 Architecture for hybrid-path IP QoS interaction between UMTS network and external IP network

5.6.1 General

Gw reference point is defined as an interface between the PEP or IP-CAN Gateway (i.e. GGSN) and resource controller element (such as BCF) in the backbone IP network. To provide IP QoS end-to-end, PEP or GGSN would be extended functionally to initiate QoS negotiation signalling to BCF and handle the response of QoS signalling from BCF.

5.6.2 Description of functions

5.6.2.1 QoS negotiation functions for hybrid-path end-to-end IP QoS

Policy Enforcement Point (PEP) or IP-CAN Gateway (GGSN) is responsible for initiating, receiving and handling QoS signalling messages to be used for hybrid-path negotiation with the external network. To that end, it may operate as:

- a signalling initiation node on the hybrid-path. This needs the PEP to collect or acquire necessary QoS negotiation information; such as BCF IP Address, the peer PEP or GGSN IP address, and QoS parameter etc. SBLP may be useful for PEP to get session information, so PEP should better send the signalling to BCF after acquiring the SBLP if PDF is available; without PDF in the UMTS network, if the GGSN know the next hop in the backbone network based on some IP-CAN bearer information, e.g. APN for GPRS, GGSN still can initiate QoS signalling to BCF.

- a signalling handling node on the hybrid-path. This means that PEP or GGSN should handle the response signalling from BCF after finishing QoS negotiation in the backbone IP network. This function may include accept the successful response, and renegotiate with the BCF if requirements cannot be satisfied completely.

Resource controller (i.e. BCF) is responsible for the management and control for resource in the backbone IP network. BCF should be able to receive and response the QoS signalling from and to the PEP or GGSN. More details on BCF is described in sections on off-path mode.

5.6.2.2 QoS management functions for hybrid-path end-to-end IP QoS

Policy Enforcement Point (PEP): except for the definition in TS 23.207 [4], PEP(GGSN) is extended functionally to be able to initiate, finish and modify the QoS negotiation with BCF. The QoS and session related information would be stored in PEP(GGSN).

Policy Decision Function (PDF): as defined in TS 23.207 [4], PDF provide SBLP to PEP for police based control. The SBLP information may be useful for the signalling from PEP to BCF. After the negotiation, PEP will return RPT message to PDF via Go interface, and the message indicates the results of Session Admission Control in the backbone IP networks.

Resource Controller in the backbone IP network: an example of resource controller is the BCF in the off-path mode. This controller is in charge of the management and assignment of resource in the backbone IP network.

5.6.2.3 Selection of external network

If more than one backbone networks exist, PEP(GGSN) would inherently have capabilities to select one of them depending on the routing and traffic information, because these information have been profiled in the PEP (GGSN). This function will offer more guarantees for E2EQoS. Operator's policy may be applied into the PEP(GGSN) as a reference for network selection.

5.6.3 Reference point between functional elements

5.6.3.1 Go reference point (PDF - GGSN)

The functionality is the same as defined in TS 23.207 [4].

Editor's Note: The conclusions for PCC [i.e. TR 23.803] should be taken into account once it is finalized.

5.6.3.2 Gw reference point

The Gw reference point is used for exchange of QoS information between PEP or GGSN and BCF element in backbone IP network. The information exchanged via Gw interface would be same as the information via Gu interface.

5.7 Characteristics of different IP QoS architectures

5.7.1 Overview

This section depicts the main characteristics of the possible alternative solutions that can be used for end-to-end QoS.

5.7.2 Characteristics of feedback based QoS solution

5.7.2.1 Characteristics of the feedback based call admission control with continuous monitoring

The main characteristic of the feedback based QoS solution is its simple implementation and low processing requirement. The nodes supporting the function in the network only have to be configured to support the Diffserv remarking function. Alternatively, the links to nodes not configured for Diffserv remarking have to be e.g. over-dimensioned so that no congestion occurs.

For an interdomain solution, the usage of feedback based solution has to be agreed between the domains as a domain not supporting this mechanism cannot be detected. The SLAs between operators can be used both to indicate if Diffserv remarking is supported as well as the Diffserv codepoints to use. If Diffserv remarking is not supported then over-provisioning can be applied. Intermediate networks using overprovisioning needs to have SLAs supporting DiffServ remarking with the same set of DSCPs.

The feedback solution is an on-path method, so it responses to changes in topology such as on-path signalling. Expected bandwidth efficiency of the method is similar to aggregated on-path signalling solutions.

The feedback based QoS solution with continuous monitoring relies on packet filtering, traffic conditioning and DSCP remarking features of routers supporting DiffServ. Therefore, no new functionality needs to be implemented in current routers when feedback based QoS solution is based on continuous monitoring.

The functionality needed in nodes performing admission control based on background monitoring consists of packet filtering, counting remarking rate for filtered aggregates and deciding on admission per aggregate. Therefore, this method is well suited to bandwidth based SLAs, that need to be configured in edge routers. If admission control is based on background traffic monitoring, session setup is fast because admission control nodes decide on local information that has been collected prior to the session establishment.

5.7.2.2 Characteristics of the feedback based call admission control using RT-ECN probing with continuous ECN monitoring

The main characteristic of this feedback based QoS solution is its simple implementation and low processing requirement. The nodes supporting the function in the network only have to be configured to support the ECN remarking function. Alternatively, the links to nodes not configured for ECN remarking have to be e.g. over-dimensioned so that no congestion occurs.

For an interdomain solution, the usage of feedback-based solution has to be agreed between the domains, as a domain not supporting this mechanism cannot be detected. The SLAs between operators can be used to indicate if ECN remarking is supported. If ECN remarking is not supported then over-provisioning can be applied. Intermediate networks needs to support Diffserv Service Classes as indicated in [13].

RT-ECN probing with continuous ECN monitoring is a dynamic solution that responds to changes in topology such as network failure.

RT-ECN probing is performed with every session setup and provides a real-time congestion information input into the call admission control decision.

Continuous ECN monitoring allows congestion to be detected mid-call providing a stimulus for reactive measures to be taken.

5.7.3 Characteristics of off-path signalling using Gu interface

Off-path signalling usually involves an independent resource management system, which communicates via standardized interfaces (COPS [11], SNMP, or other protocols) with the IP layer. It provides unified operation, maintenance and administration of the resources.

BCF is a critical node in the network since it holds information about the network logical topology and controls the service resources.

It can be implemented within a single administrative domain and multi-domain as well. The standardization of the protocol to support inter-domain solutions is depending on the progress in other standardization body (IETF, ITU-T or others).

With this solution there is no need to implement a scalable reservation protocol in each router.

This solution complements existing IP networks with QoS control functions without affecting traditional services. It adopts a layered network structure consisting of the logic bearer layer, bearer control layer and service control layer. Logic bearer layer can be e.g. an MPLS-based bearer layer that is separated from traditional IP services in terms of resources.

It requests resources before the use of services, guarantees the resources during the use and releases of resources after the use.

It fulfils the QoS requirements as long the resource management server reflects the real logical topology information (routing and link loads).

If the backbone is based on MPLS, only the edge routers need to provide flow classification functions.

5.7.4 Characteristics of on-path signalled QoS solution

In on-path QoS signalling methods (RSVP and future NSIS QoS application), the signalling messages follow the data path and make reservations for the data flow or aggregate in each network element along the path. RSVP and NSIS are able to inter-work with general routing protocols; therefore additional signalling is not needed.

The resource management is simple: based on Intserv [5] or Diffserv [9], advanced resource management may be implemented in some nodes, e.g. edge nodes. Both RSVP and NSIS utilize soft state principle. This results in more robust design than hard states, ensuring that abandoned reservations are removed automatically after time-out. Both RSVP and NSIS are able to give fast and automatic response to changing network topology, e.g. reservations are automatically moved in the new data-path after rerouting.

On-path signalling methods have distributed architectures, which is very desirable from network resilience and robustness point of view. Intserv requires storing per flow reservation state in each router, which can cause scalability issues. This can be avoided by RSVP extensions for aggregated reservation, summary refresh, which are supported also by NSIS.

6 Procedures

Editor's Note: This section will describe the procedures for the functional elements contained in the different enhanced E2E QoS architectures.

6.1 QoS procedures in functional elements

6.1.1 General

This section describes the main procedures for each involved network element that is used for the end-to-end QoS management. Procedures to ensure end-to-end QoS may be required. Various scenarios and architectures need to be

studied in order to determine if new procedures would be needed to be added to the existing functional elements in order to meet the requirements of end-to-end QoS management.

6.1.2 Procedures in the off-path model

6.1.2.1 Procedures in the PDF

When the PDF received the bearer authorization request from the GGSN, the PDF shall authorize the bearer resources by checking the stored SBLP for the session.

After this, for some services with strict end-to-end QoS requirement, it is necessary for the PDF to check if there are enough resources. The PDF shall send the authorized QoS request signalling to the BCF when interacting with the external IP network. One way in which the PDF can discover the BCF is by using a static configuration mechanism in the PDF. For example the PDF can find the appropriate BCF through static configuration of the FQDN or IP address of the BCF(s) which manages the external gateway router which interacts with the GGSN.

The PDF receives the response from the BCF, containing the information that the requested QoS can be guaranteed, that only lower QoS can be guaranteed, or that no QoS can be guaranteed.

Finally, the PDF shall send the authorization decision to the GGSN containing the QoS negotiated with the external IP network. This informs the UE about the QoS available on the end-to-end path for the concerned flow(s).

Editor's Note: It is FFS how to signal to the UE that no QoS can be guaranteed, e.g. the QoS class could be reduced to the lowest value indicating best effort.

If, during the established session, the BCF detects that the negotiated QoS cannot be maintained in the external IP network (link failure, congestion …) for some of the media flows, the BCF reports the information to the PDF. The PDF sends an unsolicited authorization decision to the GGSN that triggers a GGSN initiated bearer modification. This informs the UE about the fact that the QoS is decreased or even no more guaranteed for the concerned flow(s).

When the PDF received update or revoke request from the AF, the PDF shall send the appropriate update and revoke request to the GGSN and the BCF if needed. The original resource may be modified or released.

Editor's Note: The static configuration mechanism may only work with a single BCF. Other mechanisms to select BCF are FFS. This includes selecting BCF in an external IP network with multiple BCFs.

6.1.3 Procedures in the feedback based call admission control on-path model

6.1.3.1 General

As part of session establishment, the current congestion condition of the external backbone IP network shall be obtained by the media function (e.g. GGSN or another node in the IMS core).

The congestion condition indication is then provided to the CAC function which could be allocated to the media function (e.g. GGSN, MRF) or to another IMS core node (e.g. PDF).

6.1.3.2 Procedures for feedback based call admission control with continuous monitoring

6.1.3.2.1 Overview

There are two main procedures for the Feedback based Call Admission Control:

- provision of the feedback of the resource situation in the network;
- doing call admission control based on the collected information.

Two optional procedures can also be used in connection to this model:

- monitoring support in intermediate domains;

- providing feedback for rate control in case of persistent congestion.

6.1.3.2.2 Provision of feedback on resource situation

This feedback procedure is run continuously and it is done independently of any particular session. That is, packets from any session can be used to carry information on the resource situation.

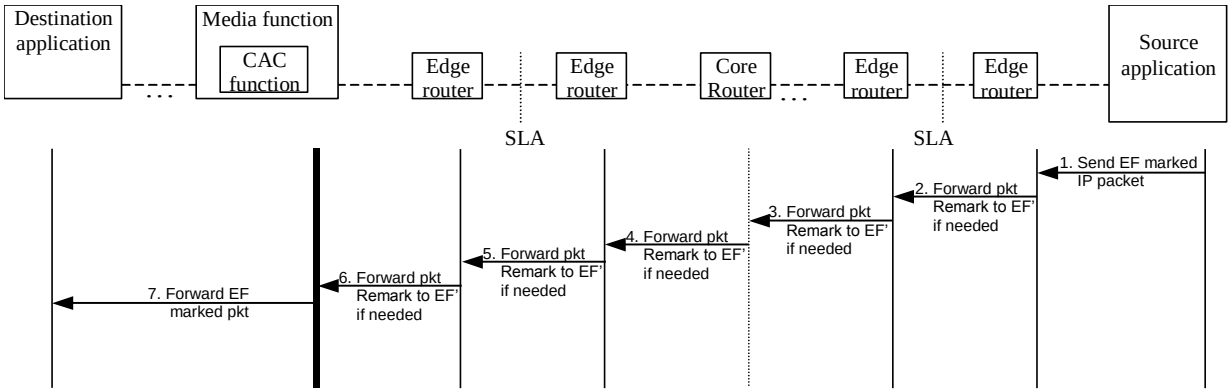


Figure 6.1.3.2.2.1: Provision of feedback on resource situation

1) An IP packet is sent from the source application. The packet is DiffServ marked for guaranteed QoS, e.g. with Expedited Forwarding (EF).
The packet is received by an edge router. The edge router is configured with a policing function that remarks packets - that are out of a preconfigured traffic profile (token bucket rate and size) for a corresponding flow aggregate - to provide indication of potential resource limitation to the Media function. The traffic profile can be set according to an engineered bandwidth limitation based SLAs or a capacity limitation of specific links. Indication is generated before actual congestion is reached. Out-of-profile packets are marked to a second DSCP (denoted in this example as EF') that is associated with EF.
The traffic profile of this policing function should be lower than the bandwidth agreed in the SLA or bandwidth available for EF traffic on links. The difference between the two profiles provides an interval where feedback on resource limitation is already sent but actual resource limitation is not reached, which allows Media function nodes to interpret the feedback and block new calls before reaching congestion.
The remarked packet is forwarded to next node.

2) The packet is received by the edge router of the next domain (new DiffServ domain and new backbone operator). The next operator may have a different DiffServ mapping scheme, so remarking EF' packets to another DSCP may be necessary (packets are still denoted by EF' in the figure). Same policing function as described in 1. could be executed by this edge router too. That is, if congestion is experience by this edge router then EF packets could be remarked to EF' in this node too.
The packet is forwarded towards the destination.

3) A core router receives the packet.
It forwards the packet towards its destination using the scheduling queue indicated by the DSCP in the packet. The DiffServ scheduler in routers are configured to use the same queue for packets marked with the original DSCP (EF) and with the DSCP indicated resource limitation (EF'). These routers may implement polices to remark packet so as edge routers. However, configuring policing function is not necessary in core nodes if resource provisioning is solved within the domain with another method than feedback based admission control (e.g. traffic engineered tunnels, overprovisioning).

4) The packet is received by an egress edge router. Procedures are the same as in step 1.

5) The packet is received by an ingress edge router. Procedures are the same as in step 2.

6) The remarked packet is received by the media function holding a Call Admission Control function. The amount of remarked packets (EF') is counted in this node to provide the basis of call admission decisions for new flows. Amount of remarked packets is counted separately for flow aggregates, which are defined by source IP address ranges.
Note that the size of the aggregates should be selected such that IP addresses belonging to different routes within the inter-domain backbone IP network should belong to different aggregates. On the other hand, the size of aggregates should preferably be large enough to ensure that new calls belong to aggregates where ongoing calls

provide feedback for admission control decision.
Configuration of aggregates could be made easier by using automatic aggregate creation based on a default prefix value (or a set of default prefix values for different IP address ranges). The automatic operation would mean that whenever a packet is received with source IP address that do not belong to any aggregate for which remarking measurement is ongoing, then a new aggregate is created with the size of the default prefix value.

7) The packet is marked back to the original EF class and forwarded towards its destination.
Note that additional IP routers, DiffServ domains and Media functions may reside between the given Media function and the destination.

NOTES:

- The provision of feedback on resource situation as described in figure 6.1.3.2.2.1 and in the text above, is done bi-directional. The figure only shows one direction, The call admission control is done in the destination or receiving ends of each uni-directional path.

- A domain that does not support DiffServ or does not support marking for providing feedback information should convey DSCP information without any modification.

- A domain that applies tunnelling techniques (MPLS or IP tunnel) and does not support marking for providing feedback information should use the DiffServ marking of the inner header when the header of the tunnel is removed.

- A domain that applies tunnelling techniques (MPLS or IP tunnel) and does support marking for providing feedback -information to Media functions should set the outer header at the entry of the tunnel based on the DS field of the IP packet (i.e. in MPLS, EF of EF' should be mapped to different EXP codepoint (Experimental field of MPLS header); and in IP, EF or EF' should be written to DS field of outer header) and map the outer header to the DS field of the IP packet at the end of the tunnel.

6.1.3.2.3 Performing Call Admission Control based on resource situation

The media function (e.g. GGSN, MRF) receives a request to establish a media path. As part of the procedure, the media function obtains the IP address for the requested source (e.g. as a filter from the PDF, in a H.248 request, etc). The media function uses this IP address to check the resource situation along the path between source and the media function.

As a first step the admission control looks for an aggregate that includes the source IP address of the new flow.

If a corresponding aggregate is found and the current frequency of remarked packets for the aggregate is higher than a preconfigured threshold, then the path in the network for the new flow is considered close to, or at its maximum limit. Hence the request to setup the media path is rejected. If the remarking rate is below the preconfigured limit then the flow is admitted.

If no corresponding aggregate is found then the flow is admitted. Proper provisioning (difference between traffic profile for remarking and total agreed traffic profile in SLAs) should make possible to admit calls in these situations. By proper sizing of the aggregates the probability of this situation should be minimized.

Note that admission control decision is always related to the upstream part of the end-to-end path. That is, Media function decides on resource availability along path from the source. In the case of bi-directional flows, two Media functions are required: one in the source and another one in the destination domain.

Remarking and the usage of the feedback information shall be done separately for each DiffServ class. It may be done only for high prioritized traffic, e.g. EF marked traffic, or for several or all used classes. Typically it is only done for EF marked traffic. This separation ensures that high priority traffic is admitted even if there is a congestion situation for low priority traffic along the path.

6.1.3.2.4 Monitoring support in inter-mediate domains

Support of this method should not be monitored on a per-call basis. Monitoring on a per-route basis (i.e. route in the transit part of the end-to-end path) is sufficient, that should be done in the management layer.

Whether or not inter-mediate domains convey feedback information can be monitored by sending EF' marked packets regularly but at a very low rate. In that case, a completely zero rate of EF' packets means that inter-mediate networks do not convey remarking information.

Another means to check this capability is to send ping packets with EF' field (to be configured via pingCtlDSField management object, see RFC 2925 [10]).

6.1.3.2.5 Providing feedback for rate control in case of persistent congestion

In parallel to blocking new calls, Media functions could also send notification to ongoing sessions to enforce rate control when remarking rate of a given aggregate exceeds a preconfigured threshold.

6.1.3.3 Procedures for feedback based call admission control with RT-ECN probing and continuous ECN monitoring

6.1.3.3.1 General

RT-ECN probe packets are sent as part of every call setup in order to check for congestion in the bearer path. RT-ECN probe packets are only sent during call setup and until the call is answered or aborted in order to check for route congestion. After call setup, route congestion is checked by continuous ECN monitoring of media packets.

For GPRS it is envisaged that RT-ECN probes will be sent between the caller's and the callee's GGSN. For GPRS, congestion in the access network is already controlled via standard GPRS QoS mechanisms.

For non GPRS it is envisaged that RT-ECN probes will be sent between the caller's and the callee's terminal (UE). For non GPRS access networks where the access network's QoS mechanisms can be used to reach the caller's/callee's terminal (UE) the RT-ECN probe can alternatively be sent between the caller's and callee's Gateway (GGSN equivalent).

For GPRS to non GPRS calls (and vice-versa) it is envisaged that the RT-ECN will be sent between the caller's GGSN and the callee's terminal (UE) or between the caller's GGSN and the callee's Gateway (GGSN equivalent).

Note: GPRS is the only IP-CAN currently in scope of TS 23.207 [4].

The ECN indications (in the IP header within the TOS byte) provided by the external backbone IP network shall be used to indicate current congestion conditions in the backbone IP network.

All packets marked with that DSCP and ECN capable will be measured and marked according to the congestion level. The marking of packets with RT-ECN does not care what session and what kind of packet it is. The RT-ECN router marking process just looks at the DSCP, the ECN capability and the traffic levels when deciding whether to mark the ECN field. This means that ECN marking can provide feedback based congestion information continuously during a session as well as at call setup time.

For GPRS, a check for available resource in Backbone Network using RT-ECN probe can be an additional step in the GGSN before the UE-to-UE flow related to a specific PDP-Context is allowed and charged for. The CAC functionality will need to be integrated to the PDP-Context processing in the GGSN wrt Gating function and its interface to the CSCF functions.

For non GPRS, a check for available resource (end to end) using RT-ECN can be an additional step in the call setup procedure of the UE's or Gateway (GGSN equivalent).

Note: GPRS is the only IP-CAN currently in scope of TS 23.207 [4].

Continuous monitoring of congestion can provide a trigger for reactive measures.

Each domain (intermediate IP network) must engineer how much VoIP traffic it wants to handle (this is governed by its business, how much VoIP has it charged its customers for, how many VoIP SLA it has made with its peering domains, etc). So each domain will have its own settings for the RT-ECN traffic levels.

One domain's RT-ECN traffic level DOES NOT need to be the same as another domain's. And most likely they are totally different. When setting the RT-ECN traffic level, the largest possible AF session and the likelihood of multiple simultaneous requests for AF sessions should be taken into consideration such that congestion should not occur.

6.1.3.3.2 Procedures in the GGSN

As part of session establishment to a GPRS connected UE, the current congestion condition of the external backbone IP network shall be obtained by sending a RT-ECN probe packet from the caller's GGSN, over the Gi interface, to the

callee's GGSN using the callee's IP address. The terminating GGSN intercepts the RT-ECN probe packet and responds with the current congestion condition.

Note: The choice of transport protocol for the RT-ECN probe packet needs to consider the monitoring of incoming packets at the GGSN for detecting the RT-ECN probe packet. In this respect the choice of RT-ECN probe transport protocol shall not lead to a large processing impact to the GGSN.

For calls to a non GPRS connected UE, the current congestion condition of the external backbone IP network and terminating access network shall be obtained by sending a RT-ECN probe packet from the caller's GGSN, over the Gi interface, to the callee's UE using the callee's IP address and port number. The UE or terminating Gateway responds with the current congestion condition.

Note: GPRS is the only IP-CAN currently in scope of TS 23.207 [4].

The congestion condition indication (ECN marking) that is returned can be used for making application flow admission control decisions. The result of this admission control decision is then provided to the UE using existing GPRS signalling.

Continuous monitoring of congestion at the GGSN can provide a trigger for reactive measures.

7 Message flows

Editor's Note: This section will describe the message flows between functional elements contained in the different enhanced E2E QoS architectures.

7.1 Message flows for the off-path IP QoS model

Editor's Note: The procedures in this section should be aligned with PCC [i.e. TR 23.803] once it is finalized.

7.1.1 Authorize QoS resources, AF session establishment

Same as 6.3.1 in TS 23.207 [4].

7.1.2 Authorize QoS resources, bearer establishment

This section provides the flows for bearer establishment, resource reservation and policy control with PDP Context setup and external network interworking.

The following figure is applicable to both the Mobile Originating (MO) side and the Mobile Terminating (MT) side.

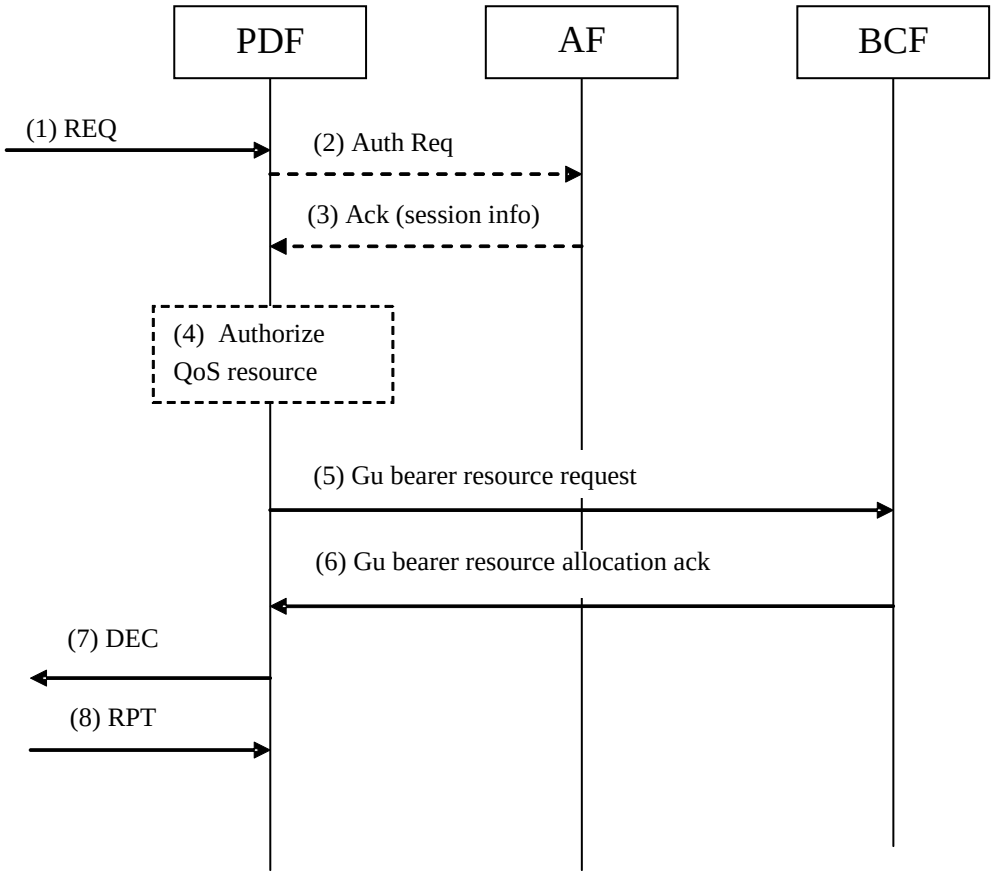


Figure 7.1.2.1: Authorize QoS resources, bearer establishment

1) The GGSN sends a REQ message with the Binding Information to the PDF in order to obtain relevant policy information.

2) A PDF generated authorization token enables the PDF to identify the authorisation status information. If the previous PDF interaction with that AF had requested this, or if the previous interaction with the AF did not include service information, the PDF sends an authorisation request to that Application Function.

3) The AF sends the service information to the PDF.

4) The PDF shall authorize the required QoS resources for the AF session if the session description is consistent with the operator policy rules defined in the PDF, and install the IP bearer level policy in its internal database. This is based on information from the Application Function.

5) The PDF sends a request for QoS resources of the external IP network to the BCF with service information, which may include session description information based on the AF session signalling.

6) The PDF will receive the result of allocation resources from the BCF.

7) The PDF sends a DEC message back to the GGSN.

8) The GGSN sends a RPT message back to the PDF, which may also trigger a report message to be sent from the PDF to the AF.

7.1.3 Enable media procedure

Same as section 6.3.3 in TS 23.207 [4].

7.1.4 Disable media procedure

Same as section 6.3.4 in TS 23.207 [4].

7.1.5 Revoke authorization for GPRS and IP resources

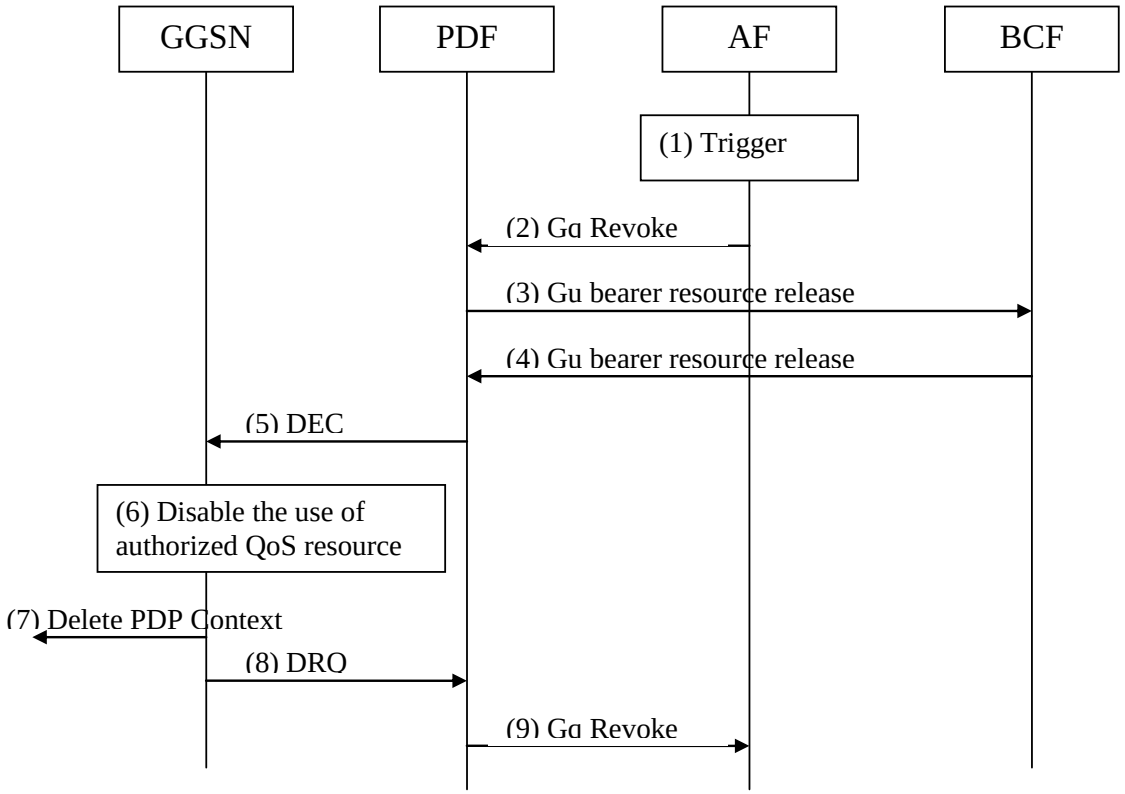


Figure 7.1.5.1: Revoke authorization for GPRS and IP resources

1) AF session signalling message exchanges for e.g. AF session release or internal action at the AF triggers the need to revoke the authorization.

2) The Application Function sends a message to the PDF to indicate the revocation.

NOTE: Steps 3 and 5 may be initiated in parallel.

3) The PDF sends a bearer resource release request message to the BCF to release the resources of the external network.

4) The BCF responses with a bearer resource release ack message to the PDF.

5) The PDF shall send a DEC (Decision) message containing revoke command to the GGSN.

6) The GGSN receives the DEC message, and disables the use of the authorized QoS resources.

7) The GGSN initiates deactivation of the PDP context used for the AF session, in case the UE has not done it before.

8) Upon deactivation of the PDP Context, the GGSN sends a DRQ (Delete Request State) message back to the PDF.

9) The PDF indicates the successful execution of the revoke indication.

7.1.6 Indication of PDP context release

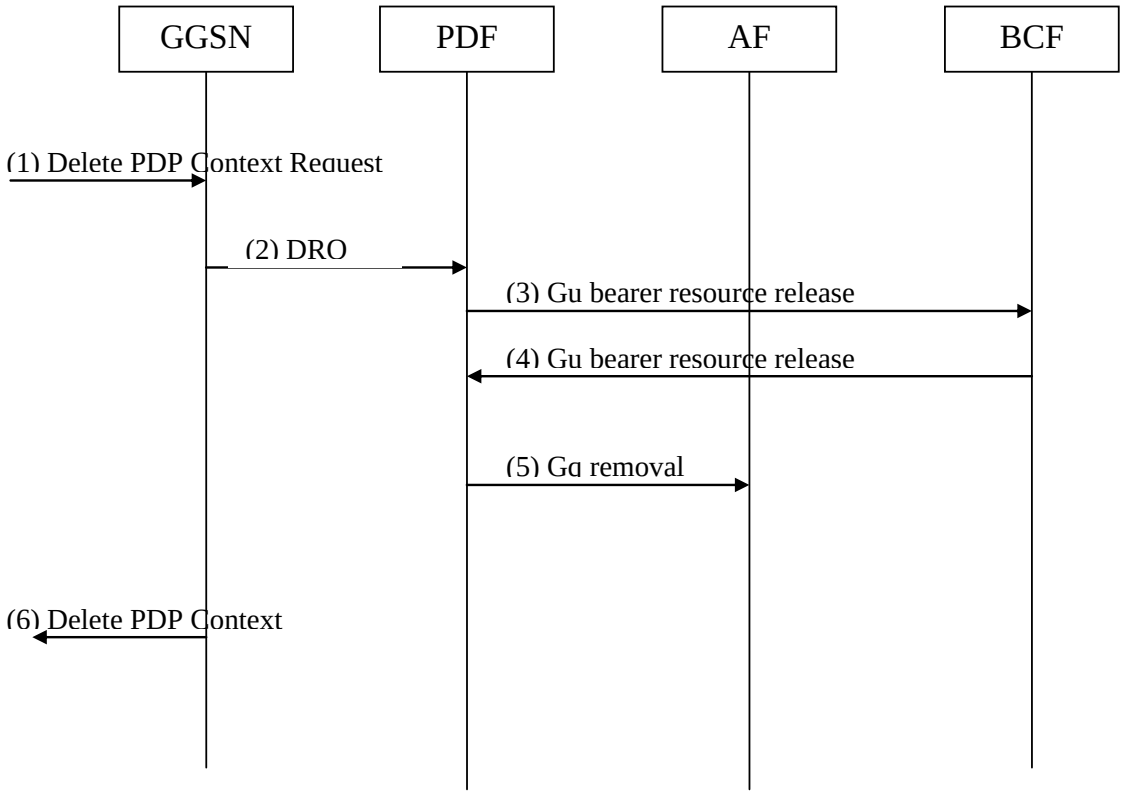


Figure 7.1.6.1: Indication of PDP context release

1) The GGSN receives a Delete PDP Context request for the PDP context related to the media flow.

2) The GGSN sends a DRQ message to the PDF.

NOTE: Steps 3 and 5 may be initiated in parallel.

3) The PDF sends a bearer resource release request message to the BCF to release the resources of the external network.

4) The BCF responses with a bearer resource release ack message to the PDF.

5) The PDF indicates the bearer removal to the AF.

6) The GGSN sends the Delete PDP Context Response message to the SGSN to acknowledge the PDP context deletion.

7.1.7 Authorization of PDP context modification

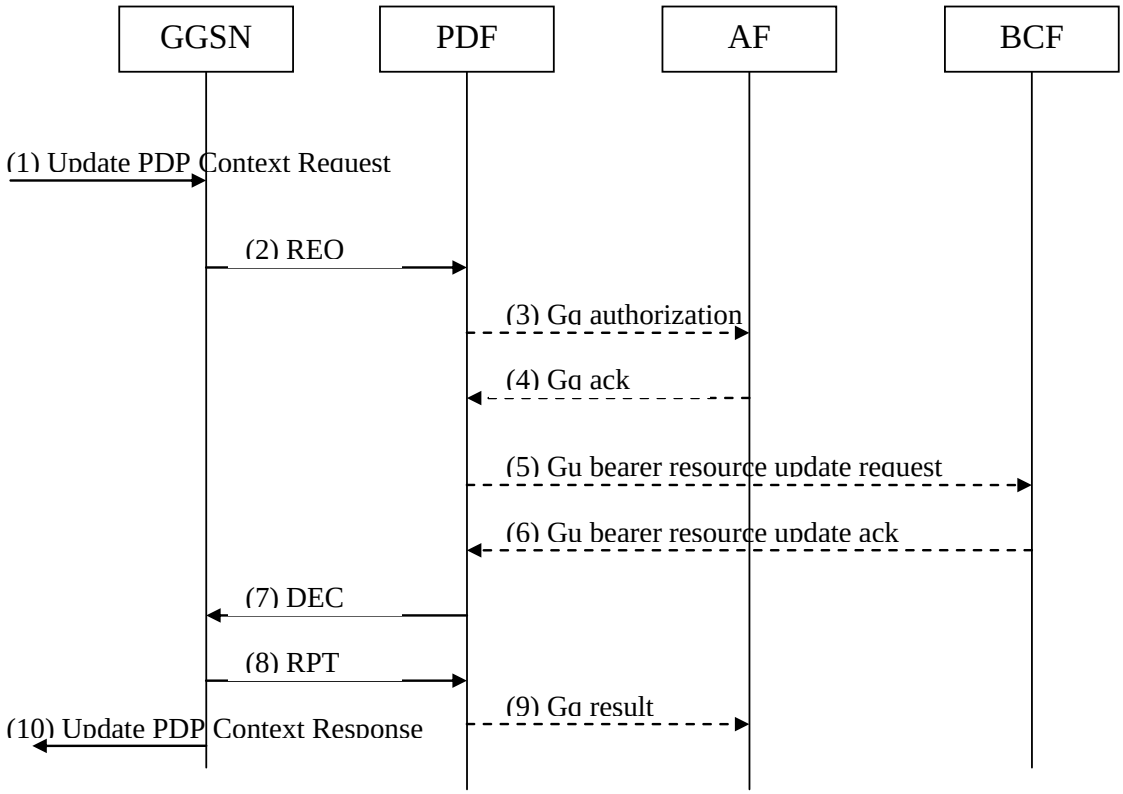


Figure 7.1.7.1: Authorization of PDP context modification

1) A request to modify the PDP context related to the media flow is indicated by sending the Update PDP Context Request message to the GGSN.

2) The GGSN sends a REQ message to the PDF. If the GGSN has sufficient information to authorize this PDP context modification request, then the GGSN does not send a REQ message to the PDF.

3) The PDF may send an authorization request to the Application Function. This may be the case if this was requested from the AF at initial authorisation, and if PDF requires more information from the AF before authorising the network resources modification.

4) The AF shall send service information for authorization of the bearer modification.

5) The PDF sends a bearer resource update request message to the BCF to update the resources of the external network if necessary.

6) The BCF responses with a bearer resource update ack message to the PDF.

7) The PDF receives the REQ message, notes the requested modification and informs the GGSN of the authorization decision.

8) The GGSN sends a RPT message back to the PDF.

9) In case the PDF had contacted the AF in step 3), then the successful installation of the decision is reported to the AF.

10) If the PDF accepted the modification, the GGSN sends the Update PDP Context Response message to the SGSN to acknowledge the PDP context modification.

7.1.8 Indication of PDP context modification

Same as section 6.3.7 in TS 23.207 [4].

7.1.9 Update authorization procedure

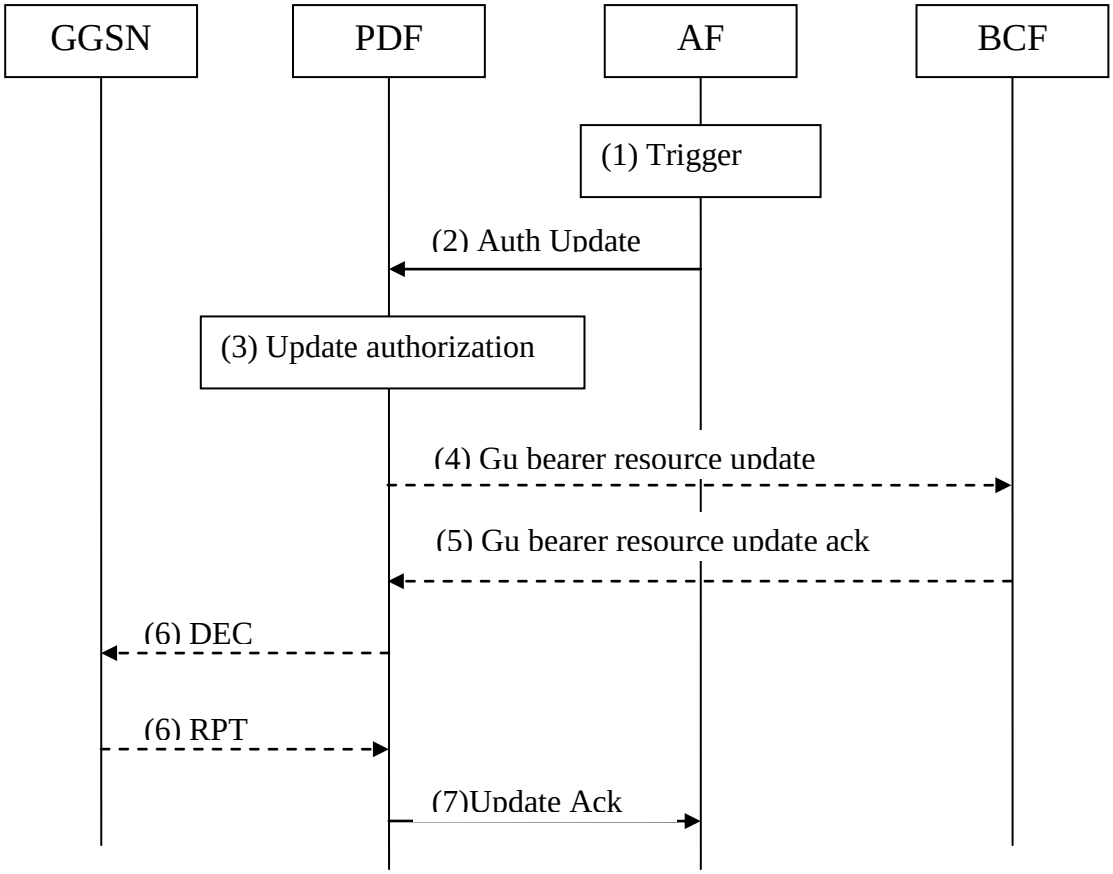


Figure 7.1.9.1: Update authorization procedure

1) The AF is triggered to give updated service information to the PDF (e.g. as a result of the modification of the session at session control level).

2) The AF gives the updated service information to the PDF.

3) The PDF updates the authorization for the session if the session description is consistent with the operator policy rules defined in the PDF. In case the session modification requires enhancing the reserved resources, the PDF may decide not to send an updated decision authorizing the enhanced QoS to the GGSN, but would rather wait for a new authorization request from the GGSN.

4) In case the session modification affects the authorized resources, the PDF sends the resource update request message to the BCF if necessary.

5) The BCF responses with a resource update ack message to the PDF.

6) In case the session modification affects the authorized resources, the PDF sends a DEC message to the GGSN to enforce authorization according to the session modification. The GGSN updates the authorization. If the QoS of the PDP context exceeds the updated authorized QoS and the UE does not modify the PDP context accordingly, the GGSN shall perform a network initiated PDP context modification to reduce the QoS to the authorized level. The GGSN sends a RPT message back to the PDF.

7) The PDF sends an acknowledgement to the AF.

7.2 Message flows for the on-path signalling IP QoS model

7.2.1 Authorize QoS resources, AF session establishment

Same as section 6.3.1 in TS 23.207 [4].

7.2.2 Authorize QoS resources, bearer establishment

This section provides the flows for bearer establishment, resource reservation and policy control with PDP Context setup and external network interworking.

The following figure is applicable to the case where the GGSN supports on-path signalling proxy functionality.

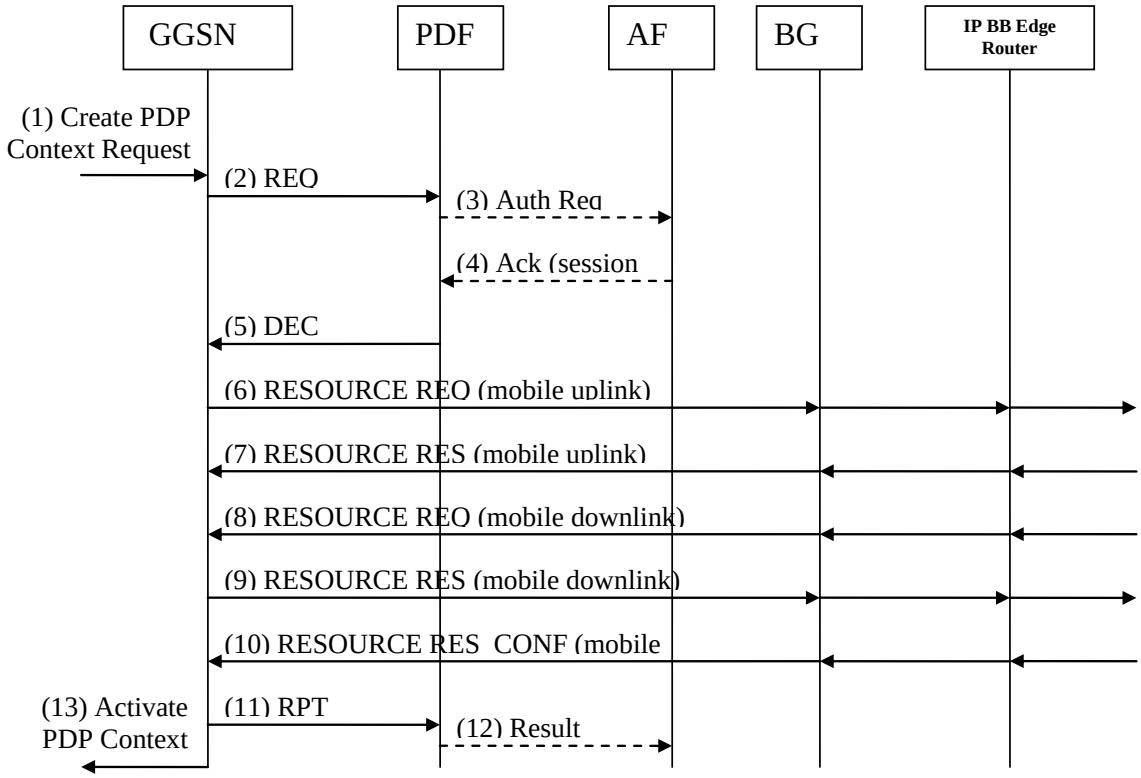


Figure 7.2.2.1: Authorize QoS resources, bearer establishment

1) A request to establish a PDP context is indicated by sending the Create PDP Context Request to the GGSN.

2) The GGSN sends a COPS REQ message with the Binding Information to the PDF in order to obtain relevant policy information.

3) The PDF may send an authorization request to the Application Function. This may be the case if this was requested from the AF at initial authorization, and if the PDF requires more information from the AF before authorising the modification of network resources.

4) The AF shall send back service information for authorization of the bearer modification.
The PDF shall authorize the required QoS resources for the AF session if the session description is consistent with the operator policy rules defined in the PDF, and install the IP bearer level policy in its internal database. This is based on information from the Application Function.

5) The PDF sends a COPS DEC message back to the GGSN.

6) If the Packet Classifier includes a mobile up-link flow, the GGSN sends a RESOURCE REQ message towards the flow receiver.
The GGSN uses authorized QoS and Packet Classifier information received DEC message to populate the QoS parameters in the generated on-path signalling message .When multiple flows are multiplexed over the same

PDP context, one on-path signalling reservation per flows belonging to the same session is maintained by the GGSN. This message travels hop-by-hop (through every on-path signalling-enabled network element) towards the flow originator.

7) The flow receiver, or an on-path signalling receiver proxy acting on behalf of the receiver, responds with a RESOURCE RES message reserving resources for the mobile up-link flow.

Note: the RESOURCE RES CONF message sent by the GGSN has been omitted for simplicity.

8) If a mobile down-link flow needs to be reserved, the down-link flow originator, (or an on-path signalling receiver proxy acting on behalf of the originator, such as the GGSN on the remote side), sends an RESOURCE REQ message for the mobile down-link.

9) The GGSN, acting as on-path signalling receiver proxy on behalf of the UE, responds with a RESOURCE RES message reserving resources for the mobile down-link flow and requesting a confirmation.

10) The down-link flow originator, (or an on-path signalling receiver proxy acting on behalf of the originator, such as the GGSN on the remote side), sends a RESOURCE RES CONF message confirming resources have been reserved for the mobile down-link.

Note: Steps 6 and 8 may be initiated in parallel.

The GGSN, BG or IP Backbone Edge Router may be configured to perform aggregation of on-path signalling reservations (e.g., RFC 3175 [16] or draft-lefaucheur-rsvp-dste [17] for RSVP).
When the aggregate reservation is not yet established or when the aggregate reservation needs resizing to reflect the cumulative resource requirements of all the micro-flows aggregated over it, on-path signalling messages associated with the aggregate reservation are exchanged between the on-path signalling aggregation point and the de-aggregation point.

11) The GGSN sends a RPT message back to the PDF.

12) In case the PDF had contacted the AF in step3), then the successful installation of the decision is reported to the AF.

13) The GGSN responds with a PDP Context Accept message to the SGSN.

7.2.3 Enable media procedure

Same as 6.3.3 in TS 23.207 [4].

7.2.4 Disable media procedure

Same as 6.3.4 in TS 23.207 [4].

7.2.5 Revoke authorization for GPRS and IP resources

The section provides the flows for revoking the authorization of GPRS and IP Resources with external network interworking.

The following figure is applicable to the case where the GGSN supports on-path signalling proxy.

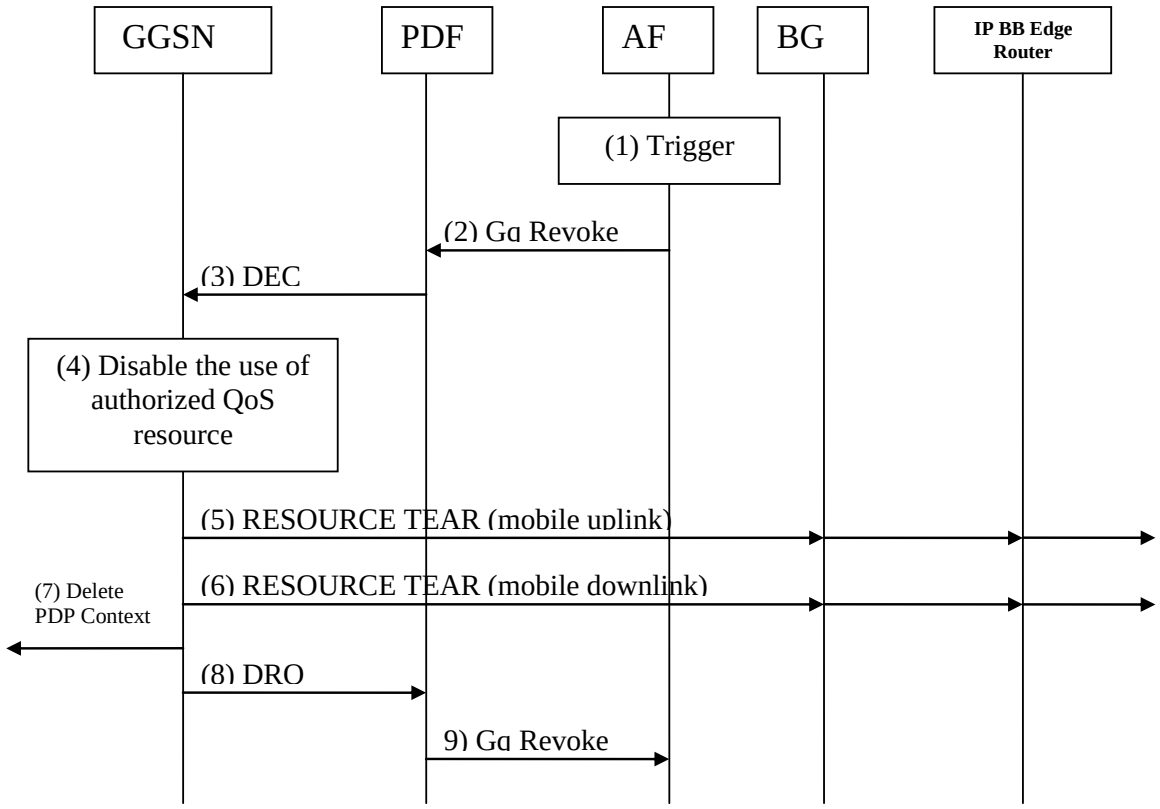


Figure 7.2.5.1: Revoke authorization for GPRS and IP resources

1) AF session signalling message exchanges for e.g. AF session release or internal action at the AF triggers the need to revoke the authorization.

2) The Application Function sends a message to the PDF to indicate the revocation.

3) The PDF shall send a DEC (Decision) message containing revoke command to the GGSN.

4) The GGSN shall disable the use of authorized QoS resources.

5) If resources were reserved in the mobile uplink direction, the GGSN sends a RESOURCE TEAR message towards the flow originator to release the resources.

6) If resources were reserved in the mobile downlink direction, the GGSN, acting as on-path signalling receiver proxy on behalf of the UE, sends a RESOURCE TEAR message releasing resources for the downlink flow. The GGSN, BG or IP Backbone Edge Router may be configured to perform aggregation of on-path signalling reservations (e.g., RFC 3175 [16] or draft-lefaucheur-rsvp-dste [17] for RSVP).
When the releasing of resources triggers a re-sizing of the aggregate reservation, on-path signalling messages associated with the aggregate reservation are exchanged between the on-path signalling aggregation point and the de-aggregation point.

7) The GGSN initiates deactivation of the PDP context used for the AF session, in case the UE has not done it before.

NOTE: Steps 5, 6 and 7 may be initiated in parallel.

8) Upon deactivation of the PDP Context, the GGSN sends a DRQ (Delete Request State) message back to the PDF.

9) The PDF indicates the successful execution of the revoke indication.

7.2.6 Indication of PDP context release

The "Indication of PDP Context Release" procedure is used upon the release of a PDP Context that was established based on authorisation from the PDF.

The following figure presents the "Indication of PDP Context Release" procedure for the case where the GGSN supports on-path signalling proxy.

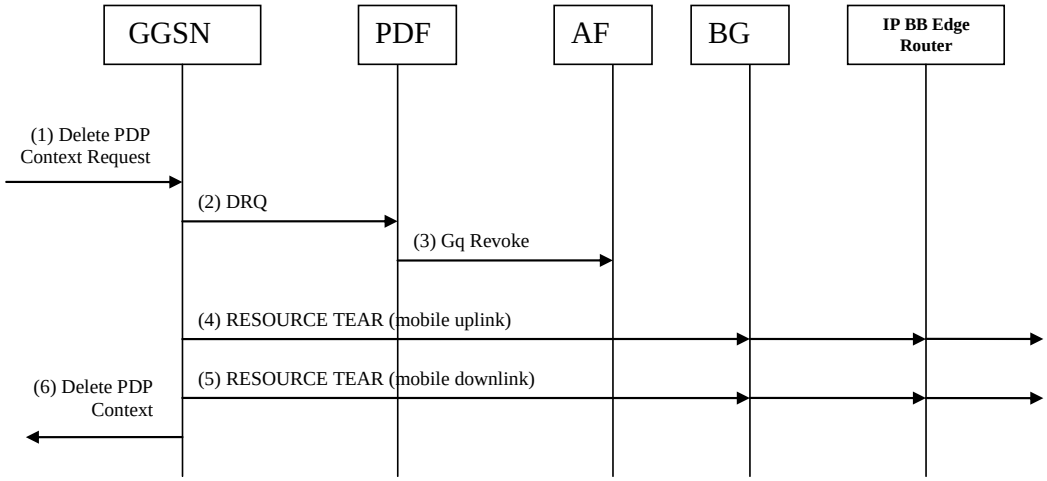


Figure 7.2.6.1: Indication of PDP context release

1) The GGSN receives a Delete PDP Context request for the PDP context related to the media flow.
2) The GGSN sends a DRQ message to the PDF.
3) The PDF indicates the bearer removal to the AF.
4) If mobile uplink resources were reserved, the GGSN sends a RESOURCE TEAR message to the flow receiver to release the resources of the external network.
5) If mobile downlink resources were been reserved, the GGSN sends a RESOURCE TEAR message to the flow receiver to release the resources of the external network.
6) The GGSN sends the Delete PDP Context Response message to the SGSN to acknowledge the PDP context deletion.

NOTE: Steps 2, 4, 5 and 6 may be initiated in parallel.

7.2.7 Authorization of PDP context modification

The "Authorization of PDP Context Modification" procedure is used when a PDP Context is modified such that the requested QoS falls outside of the limits that were authorized at PDP context activation (or last modification) or such that new binding information is received. In this case, the GGSN communicates with the PDF as described below. The following figures present the "Authorization of PDP Context Modification" procedure with a GGSN acting as on-path signalling proxy.

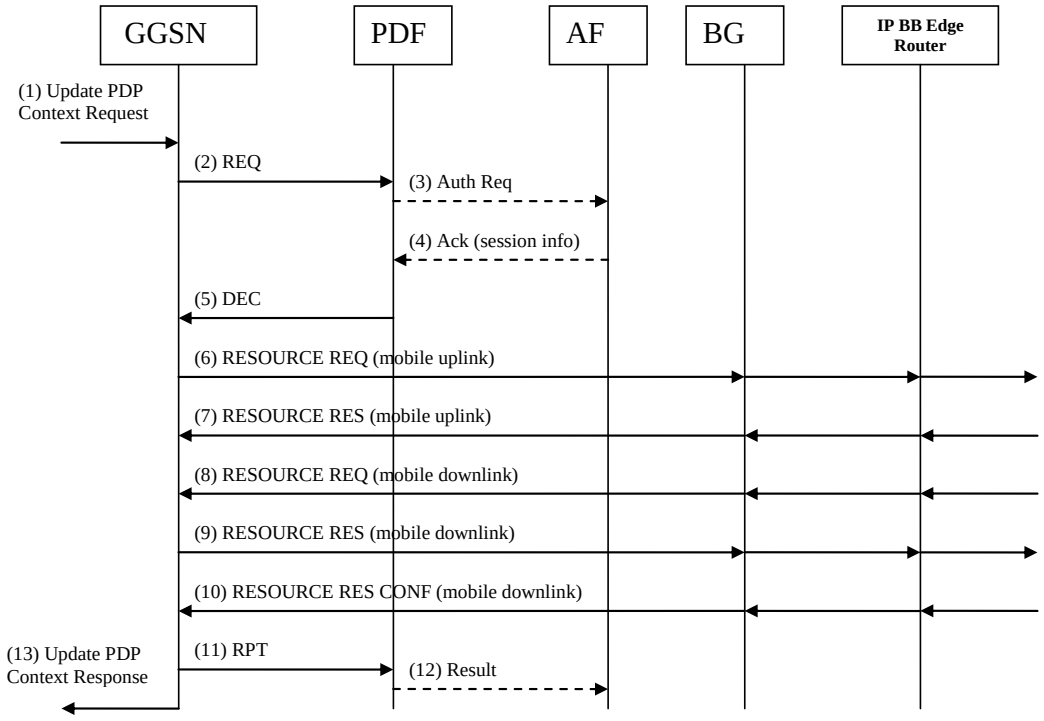


Figure 7.2.7.1: Authorization of PDP context modification

1) A request to modify a PDP context related to the media flow is indicated by sending the Update PDP Context Request to the GGSN.

2) The GGSN sends a REQ message to the PDF. If the GGGSN has sufficient information to authorize this PDP context modification request, then the GGSN does not send a REQ message to the PDF.

3) The PDF may send an authorization request to the Application Function. This may be the case if this was requested from the AF at initial authorization, and if the PDF requires more information from the AF before authorising the modification of network resources.

4) The AF shall send back service information for authorization of the bearer modification.

5) The PDF receiving the REQ message, notes the requested modification and informs the GGSN of the authorization decision.

6) If the modified media flow updates a component for the mobile up-link direction, the GGSN sends a RESOURCE REQ message towards the flow receiver.
The GGSN uses authorized QoS and Packet Classifier information received DEC message to populate the QoS parameters in the generated RESOURCE REQ message .When multiple flows are multiplexed over the same PDP context, one on-path signalling reservation per flows belonging to the same session is maintained by the GGSN. This message travels hop-by-hop (through every on-path signalling-enabled network element) towards the flow originator.

7) On receiving the RESOURCE REQ message, the flow receiver, or an on-path signalling proxy acting on behalf of the receiver, responds with a RESOURCE RES message reserving resources for the mobile uplink flow.

NOTE 1: The RESOURCE RES CONF message sent by the GGSN has been omitted for simplicity.

8) If the modified media flow updates a component in the mobile-downlink, the flow originator, (or an on-path signalling proxy acting on behalf of the originator, such as the GGSN on the remote side), sends an RESOURCE REQ message for the mobile downlink flows.

9) The GGSN, acting as on-path signalling receiver proxy on behalf of the UE, responds with an RESOURCE RES message reserving resources for the mobile down-link flow and requesting a confirmation.

10) The down-link flow originator, (or an on-path signalling receiver proxy acting on behalf of the originator, such as the GGSN on the remote side), sends an RESOURCE RES CONF message confirming resources have been reserved for the mobile down-link.

NOTE 2: Steps 6 and 8 may be initiated in parallel.

The GGSN, BG or IP Backbone Edge Router may be configured to perform aggregation of on-path signalling reservations (e.g., RFC 3175 [16] or draft-lefaucheur-rsvp-dste [17] for RSVP).
When the aggregate reservation is not yet established or when the aggregate reservation needs resizing to reflect the cumulative resource requirements of all the micro-flows aggregated over it, on-path signalling messages associated with the aggregate reservation are exchanged between the on-path signalling aggregation point and the de-aggregation point.

11) The GGSN sends a RPT message back to the PDF.

12) In case the PDF had contacted the AF in step3), then the successful installation of the decision is reported to the AF.

13) The GGSN responds with an Update PDP Context Response message to the SGSN.

NOTE 3: Steps 11 and 13 may be initiated in parallel.

7.2.8 Indication of PDP context modification

Same as section 6.3.7 in TS 23.207 [4].

7.2.9 Update authorization procedure

When a session is modified, an update for a previous authorization of the session may be given to the PDF and possibly to the GGSN. The figure below presents the "Update Authorization" procedure upgrading the resources for a GGSN acting as on-path signalling Proxy.

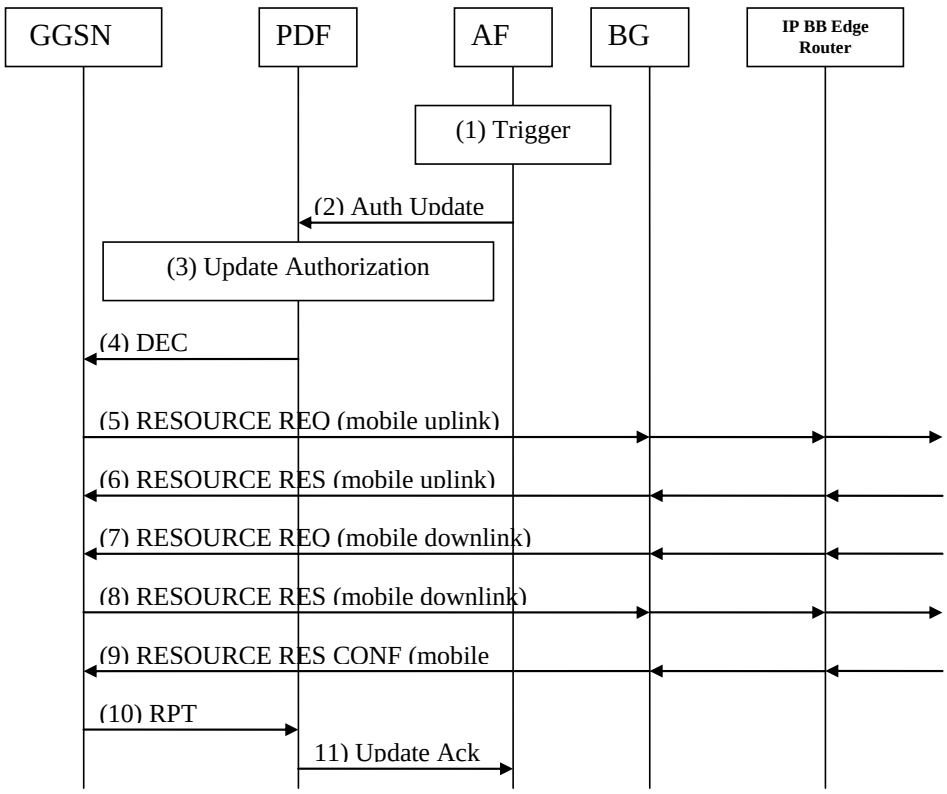


Figure 7.2.9.1: Update authorization procedure

1) The AF is triggered to give updated service information to the PDF (e.g. as a result of the modification of the session at session control level).

2) The AF gives the updated service information to the PDF.

3) The PDF updates the authorization for the session if the session description is consistent with the operator policy rules defined in the PDF. In case the session modification requires enhancing the reserved resources, the PDF may decide not to send an updated decision authorizing the enhanced QoS to the GGSN, but would rather wait for a new authorization request from the GGSN.

4) In case the session modification affects the authorized resources, the PDF sends a DEC message to the GGSN to enforce authorization according to the session modification.

5) If the modified session affects a component in the mobile uplink direction, the GGSN sends a RESOURCE REQ message towards the flow receiver with the updated description.

6) On receiving the RESOURCE REQ message, the flow receiver, or an on-path signalling proxy acting on behalf of the receiver, responds with a RESOURCE RES message reserving resources for the mobile up-link.

NOTE 1: The RESOURCE RES CONF message sent by the GGSN has been omitted for simplicity.

7) If the modified media flow affects a component in the mobile down-link, the flow originator, (or an on-path signalling proxy acting on behalf of the originator, such as the GGSN on the remote side), sends a RESOURCE REQ message for the mobile downlink flows.

8) The GGSN, acting as on-path signalling proxy on behalf of the UE, responds with a RESOURCE RES message reserving resources for the mobile downlink flow.

9) The down-link flow originator, (or an on-path signalling receiver proxy acting on behalf of the originator, such as the GGSN on the remote side), sends a RESOURCE RES CONF message confirming resources have been reserved for the mobile down-link.

NOTE 2: Steps 5 and 7 may be initiated in parallel.

10) If the QoS of the PDP context exceeds the updated authorized QoS and the UE does not modify the PDP context accordingly, the GGSN shall perform a network initiated PDP context modification to reduce the QoS to the authorized level. The GGSN sends a RPT message back to the PDF.

11) The PDF sends an acknowledgement to the AF.

8 Security aspects

Editor's Note: This section will describe the security aspects that may need to be considered when providing E2E QoS across networks not managed by 3GPP operators.

Editor's Note: The security of on-path and off-path models needs to be explored in more detail or possibly removed from this technical report.

8.1 Security aspects for the off-path model

The PDFs may authenticate with the BCFs mutually using authentication information in the SLA endorsed between those entities when signalling connection being established between them to improve the security.

The signalling for IP QoS is out-of-band and path-decoupled, which can be delivered on the dedicated link to avoid the influences of the media flows.

Logical Bearer Network (LBN) may be planed and configured to separate real time service (voice and video service etc.) flows from Internet data traffics in the external IP network.

8.2 Security aspects for the RSVP on-path model

RSVP includes a complete security framework for secure operation of RSVP. This includes:

- message integrity and node authentication. Corrupted and/or spoofed reservation requests could lead to theft of service by unauthorized parties or to denial of service caused by reserving up network resources. RSVP protects against such attacks with a hop-by-hop authentication mechanism using an encrypted hash function. The mechanism is supported by INTEGRITY objects that may appear in any RSVP message as specified in RFC 3097 [33]. These objects use a keyed cryptographic digest technique, which rely on RSVP neighbours sharing a secret.

- secure identification of end-user. In environments where host based RSVP signalling is supported, positive authentication of the user responsible for each reservation request is possible through the capability of RSVP to convey identity information as specified in RFC 3182 [34] inside RSVP messages.

In addition:

- In environments where RSVP signalling from the UE is allowed, the GGSN may be configured to rate limit the number of RSVP messages received from a UE. This protects against denial of service attacks associated with sending an excessive amount of signalling towards the GGSN and the rest of the network.

- In environments where RSVP signalling from the UE is not allowed, the GGSN may be configured to discard or to ignore RSVP messages, in order to protect against potential denial of service attacks.

9 Charging aspects

Editor's Note: This section will describe the charging aspects that may need to be considered when providing E2E QoS between operators and networks not managed by 3GPP operators.

10 Conclusions and recommendations

10.1 Conclusions

The current interconnection model for 3GPP networks is described in GSMA PRD IR.34 [36] and this model takes a pragmatic approach to QoS, relying simply on overprovisioning and marking of User Plane IP packets (using DiffServ) to exchange QoS information (i.e. as per Release 99).

According to GSMA, IMS deployment in the near term will rely on this approach, together with SLAs, to deliver QoS on inter-PLMN networks. Such solution is described in Annex A.2.1 and A.2.2 of TS 23.207 [4] and presented in Section 5.2.3 of the TR.

It is generally recognized that in the future new interconnection models may be needed, e.g., to accommodate increased adoption of IP based services and/or support interfacing to other Next Generation Networks and/or when the committed SLAs cannot be met, although the timing and the details of such need is not currently well understood.

10.2 Recommendations

The current interconnection model required by GSMA for 3GPP networks does not require the enhancement of the current specification in TS 23.207 [4].

NOTE: TS 23.207 [4] may require to be enhanced as a result of other ongoing specification work in 3GPP related to IMS and QoS issues.

It is recommended that this work item be frozen until the timing and the details of the need of new interconnection models become clear.

Annex A (informative): QoS conceptual models

A.1 Scenarios

These scenarios give examples of concatenating QoS mechanisms in different parts of the network which together can deliver an end-to-end QoS when UMTS network interacts with the external IP network. These scenarios are not intended to describe the details of the interworking between the QoS mechanisms.

The scenario assumes that the GGSN supports label edge router (LER) functions, and the backbone IP network is MPLS enabled. The UE may either provide an IP BS Manager or not.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS requirements. The QoS requirements determined from the application layer (e.g. TS 23.228 [2] describes interworking from SIP/SDP to QoS requirements) are mapped down to PDP context parameters in the UE.

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed either from the terminal using the PDP context signalling, or from the SGSN by subscription data.

The IP QoS for the downlink direction is controlled by the remote terminal up to the GGSN which may use the service based policy decided by the PDF or the TFT.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, MPLS LSP through the backbone IP network, and the same mechanism in the remote access network in the scenario shown in the figure below. The GGSN provides the interworking between the PDP context and the MPLS LSP function. However, the interworking may use information about the PDP context which is established, or be controlled from static profiles, or dynamically through other means such as proprietary HTTP based mechanisms. The UE is expected to be responsible for the control of the PDP context, but this may instead be controlled from the SGSN by subscription.

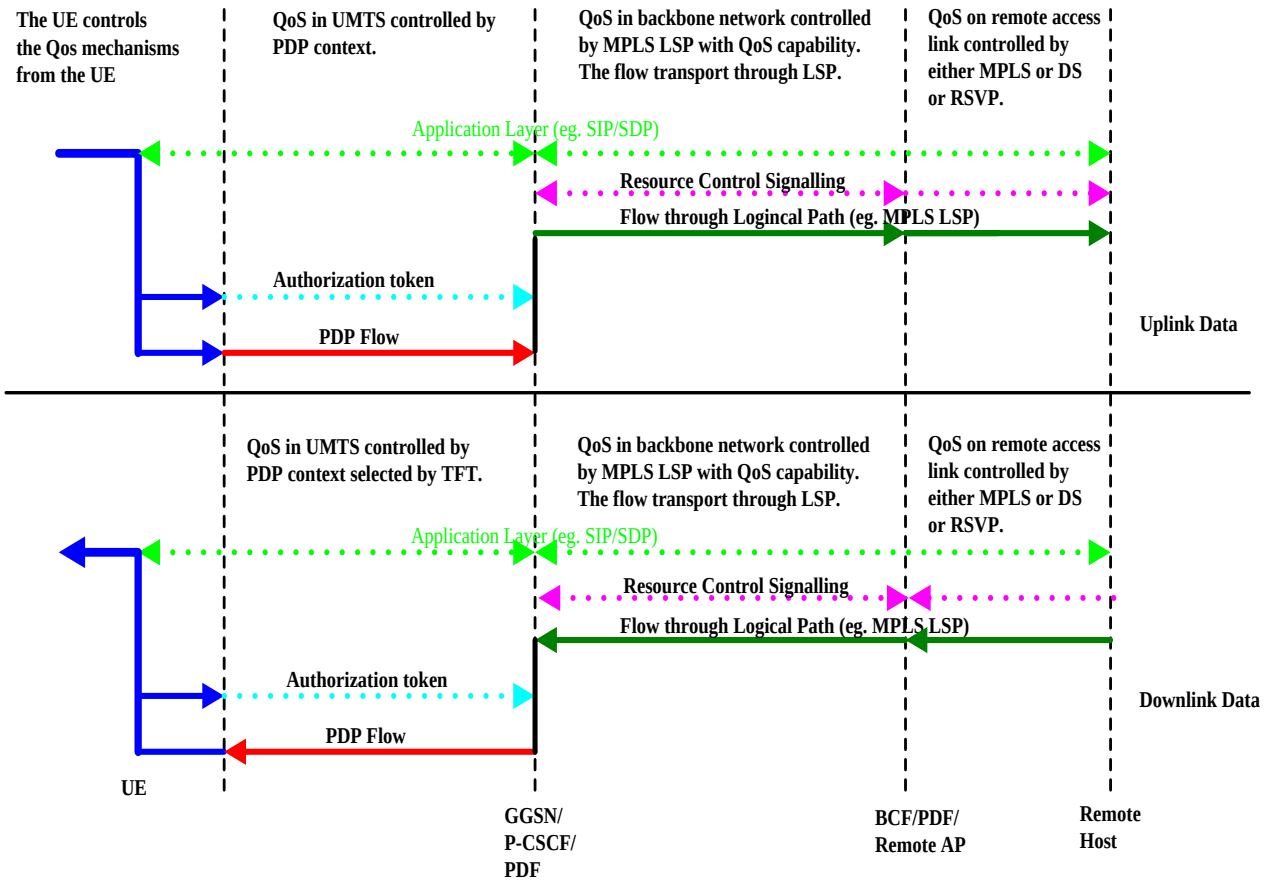


Figure A.1.1: QoS Control Based on Independent Resource Control of IP Backbone Network

NOTES:

- The solid horizontal lines indicate the mechanism that is providing QoS for the flow of data in the direction indicated.
- The dashed horizontal lines indicate where QoS control information is passed that is not directly controlling the QoS in that link/domain.
- The arrows on the horizontal lines indicate nodes that receive information about QoS from that mechanism, even if that mechanism is not used to control the QoS over that link/domain.
- The solid vertical lines indicate interworking between the different mechanisms.
- In the figure, the term RAP refers to the Remote Access Point, and RUE is the Remote UE.

The TFT and UMTS QoS profile determines the QoS applicable over the UMTS access. However, the configuration of the TFT or SBP may use the QoS profile to select the Diffserv, so there may be interworking between MPLS LSP flow and the PDP Flow via the TFT filters.

Annex B (informative): Examples of QoS provisioning schemes

B.1 Description of QoS provisioning schemes

B.1.1 General

The IP technology supports a flexible scheme to provision QoS. Many different provisioning schemes are possible and have been described to try to solve the QoS problem. QoS provisioning is done in each domain along the end-to-end path. The overall goal is to meet a specific contract (e.g. in terms of bitrate, delay, jitter) in delivering a stream of IP packets from one host to another over multiple IP domains. This description tries to give an overview over the most accepted QoS provisioning schemes. It should be noted that some of these provisioning schemes are already deployed in commercial service provider networks (e.g., over-provisioning, DiffServ based provisioning).

B.1.2 Functionality of the application node to backbone interface

The possible QoS methods can be categorized according to the required functionality at the application node to backbone interface. Forwarding of IP packets is a mandatory functionality of the IP backbone network, but additional control functions can support QoS provisioning. Control functions must be supported on the both sides of the application node to backbone interface. For example, assume that IP backbone network supports some kind of resource reservation protocol then this functionality can only be used if the application node part also supports it, i.e. the application node should be able to request resources from the backbone network and it should be able block new sessions if there are no available backbone resources.

Possible information exchange methods between application node and IP backbone network are:

- no information exchange exists: Neither IP level resource reservation nor marking of user plane IP packets is used;
- indirect control information is provided from the backbone to the application node via marking user plane IP packets (ECN, DSCP field marking);
- explicit control function: resource reservation protocol for traffic aggregates; and
- explicit control function: per-flow resource reservation.

Information exchange methods can also be possibly combined for optimal performance.

B.1.3 Over-provisioning

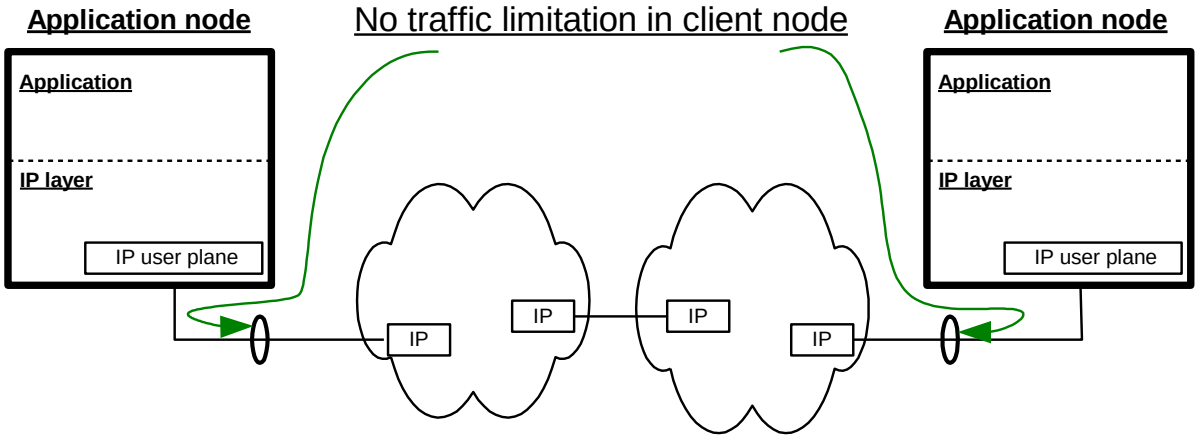


Figure B.1.3.1: Over-provisioning

Over-provisioning uses the connection model described in subclause 5.2.3.

The over-provisioning model of ensuring QoS can work in networks with a low fraction of real-time traffic. An over-provisioned network has a performance monitoring driven provisioning, re-dimensioning and extension of the network. The network/path or link is extended when the utilization is reaching a certain level. There is no need to limit the traffic in the application nodes. A well-managed and over-provisioned network should never be overloaded. However, un-expected network conditions may require additional QoS mechanisms to be handled in an appropriate way.

The advantage with over-provisioning is that it is simple – it is the Internet model. The drawbacks are that over-dimensioning is needed, which may result in lower resource utilization. Another drawback is that over-subscription by someone will affect everyone.

With an end-to-end view on QoS where often several network domains are involved, over-provisioning should have a role for ensuring QoS in sub-networks within different domains, rather than as a model ensuring it end-to-end.

B.1.4 Static provisioning

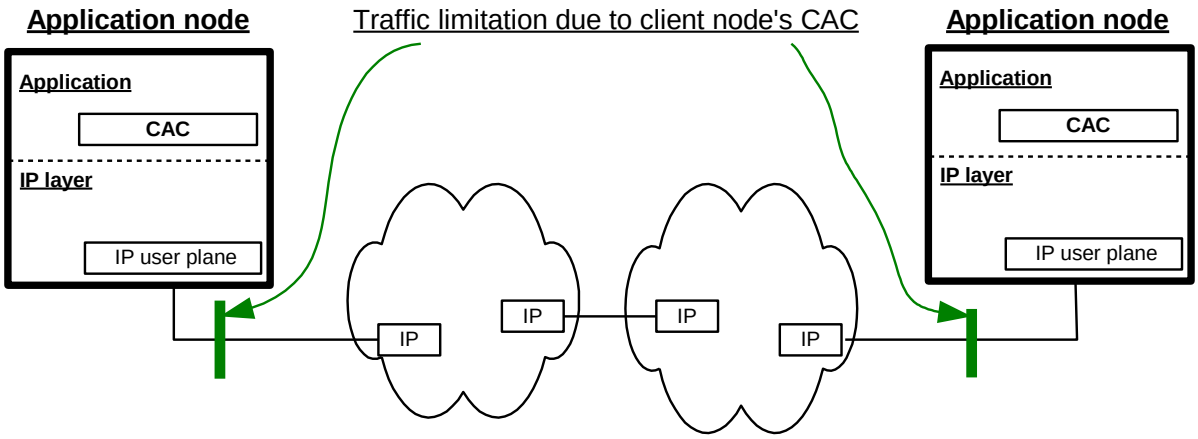


Figure B.1.4.1: Static provisioning

Static provisioning uses the connection model described in subclause 5.2.3.

A Call Admission Control (CAC) function resides in the application part of the application node. The network dimensioning is based on the maximum limits in the application node, i.e. the transport demand of each application node is limited.

In the single operator case, traffic limits of application nodes are considered at dimensioning to avoid congestion in the network, i.e. links are dimensioned to have enough capacity to carry the limited traffic without congestion.

In a multi-domain IP backbone network (see Figure B.1.4.1), operator domains are dimensioned separately. The main task is to derive maximum limits for inter-domain links based on limitations of application nodes (and then the single-domain dimensioning method can be used).

B.1.5 End-to-end measurement based admission control

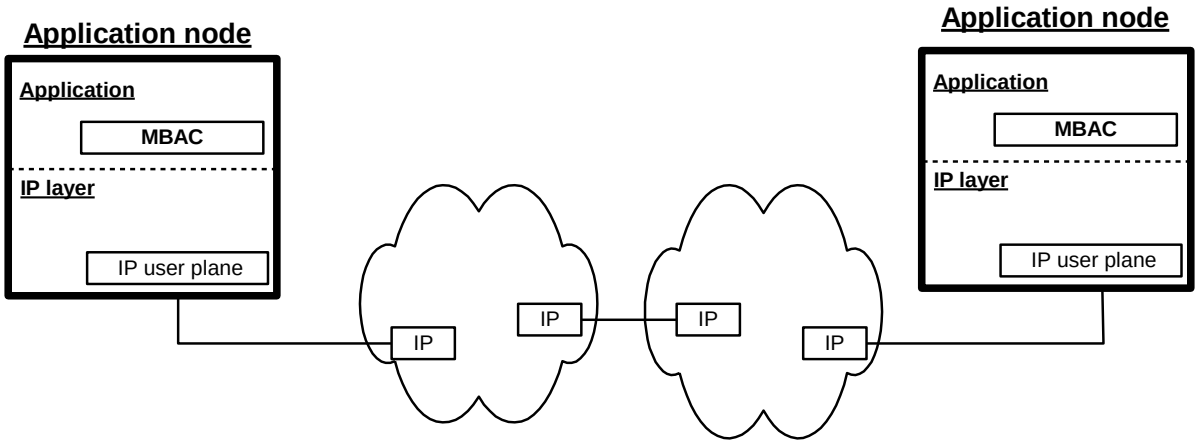


Figure B.1.5.1: End-to-end MBAC

E2E MBAC uses the connection model described in subclause 5.2.3.

Admission control is implemented in the application part of the application nodes, illustrated as "MBAC" entity in figure B.1.5.1. The admission control uses measurement on the payload traffic to predict the availability of bandwidth in the network.

In the multi-domain case (see Figure B.1.5.1), the application of MBAC can be problematic if the MBAC uses measurement on the payload traffic that is for other purposes or if it is not supported by some operator via the path.

B.1.6 Bandwidth broker

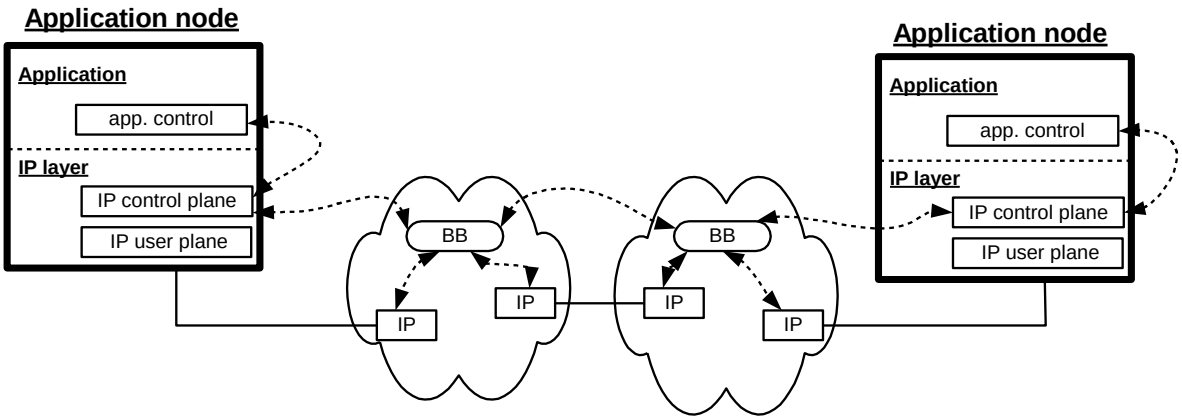


Figure B.1.6.1: Bandwidth broker (BB)

Bandwidth Broker uses the connection model described in subclause 5.2.4 or 5.2.2, depending on if resource requests are initiated from the application node itself or from a policy function external to the application node.

The Bandwidth Broker (BB) solution for QoS, comprises a centralized admission control server for QoS instead of admission control functionality in the network or application nodes. Admission control is made "off-path" e.g. outside

the backbone network. BB can use knowledge of routing to better predict the link-load on the links in the backbone network.

In inter-domain case (see Figure B.1.6.1), the communication of BBs of domains along the path is required. That is, operators involved in the end-to-end backbone service have to be known in advance because this knowledge is required to allocate resources along the path. All changes in the inter-domain routing have to be taken into account in this solution to avoid inconsistency (the path of involved BBs are different from the actual path of the IP traffic).

Editor's Note: The term Bandwidth Broker might not be the final term. If another term such as BCF or Resource Manager is more adequate is FFS.

B.1.7 Signalled provisioning

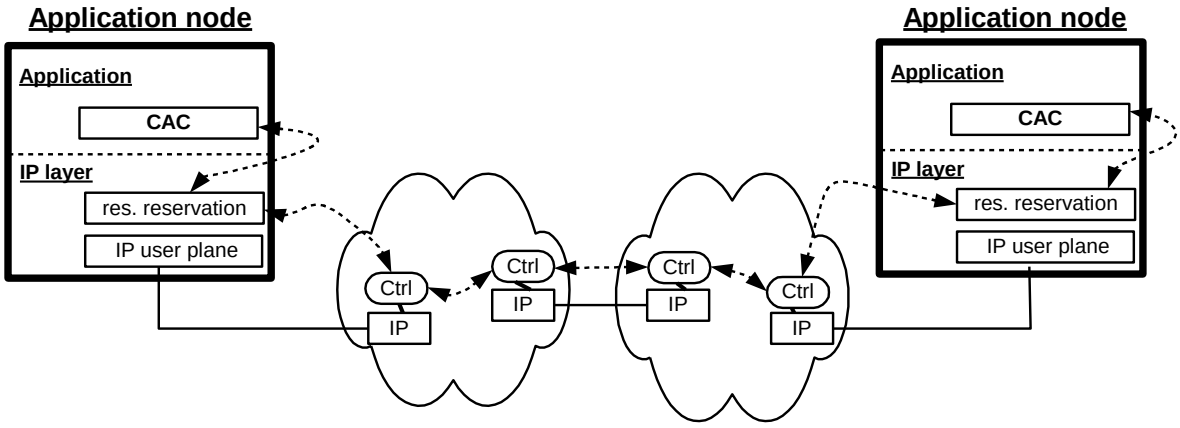


Figure B.1.7.1: Signalled provisioning

Signalled provisioning uses the connection model described in subclause 5.2.4.

A dynamic and protocol driven admission control in the backbone network is the provisioning scheme showed in figure B.1.7.1 above. In inter-domain case, all domains have to support the applied signalling protocol.

The well known signalling protocol RSVP is for example described in RFC 2205 [6], RFC 2209 [7] and RFC 2210 [8]. There have been several areas of concern about the wide-scale deployment of RSVP. This is discussed in RFC 2208 [15]. A way to try to overcome these issues by using a single RSVP reservation to aggregate other RSVP reservations across a backbone IP network or transit routing region is described in RFC 3175 [16]. There is also work in progress on RSVP aggregation over MPLS TE Tunnels [17].

A recent initiative within IETF is NSIS (Next Steps in Signalling). Intention is to standardize an IP signalling protocol with QoS signalling as the first use case. Focus will be on a two-layer signalling paradigm and re-use, where appropriate,
the protocol mechanisms of RSVP, while at the same time simplifying it and applying a more general signalling model. For the latest output from the working group see [19], [20], [21] and [22].

B.1.8 Feedback based provisioning

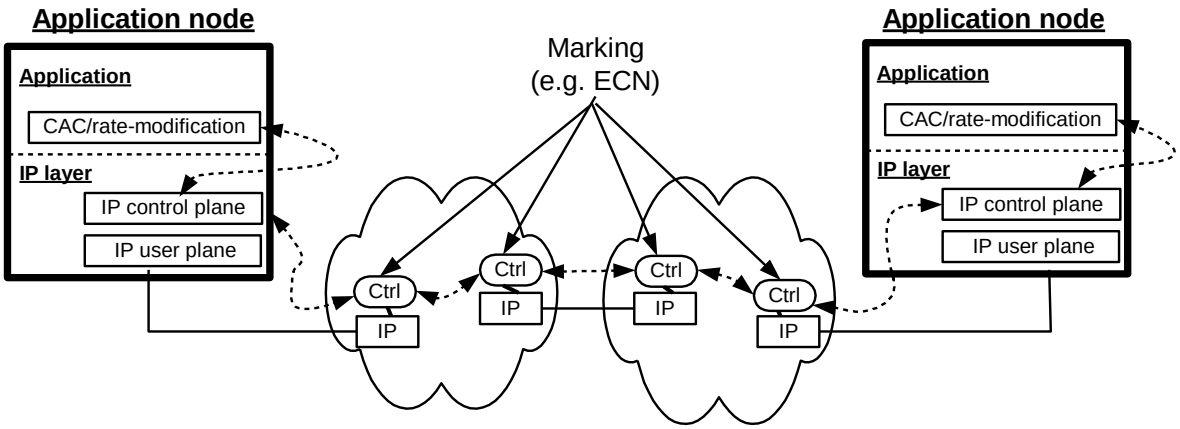


Figure B.1.8.1: Feedback based provisioning

Feedback based provisioning uses the connection model described in subclause 5.2.4.

The feedback-based solution relies on congestion indication from the network and the application node reacts with rate-adaptation of the traffic source or with call blocking. One such method could be the use of Datagram Congestion Control Protocol (DCCP - unreliable UDP with congestion control) and AMR. For more information on DCCP, please refer to work in progress [23].

In inter-domain case (see Figure B.1.8.1), all domains have to support the congestion indication functionality including also the inter-domain connections. See RFC 3168 [14] for further description of Explicit Congestion Notification. There is also recent work in progress on how the usage of ECN markings for real-time flows that use UDP [18].

Annex C (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
09-2005	SA#29	SP-050494	-	-	Presented to TSG SA#29 for Approval	1.2.0	2.0.0
09-2005	-	-	-	-	Updated by MCC for publication as version 7.0.0	2.0.0	7.0.0