3GPP TSG-SA#18 **Tdoc ⌘ SP-020819**
New Orleans, USA, December 09th – 12th, 2002

CR-Form-v7

CHANGE REQUEST

⌘	**TS 23.207**	**CR**	**44**	⌘**rev**	**4**	⌘	Current version:	**5.5.0**	⌘	

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Combined CR on alignement with stage-3 on end-to-end QoS		
Source:	⌘	Nortel, Ericsson, Nokia		
Work item code:	⌘	E2EQoS	***Date:*** ⌘	10.12.2002
Category:	⌘	**F**	***Release:*** ⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	This contribution aligns TS 23.207 with the stage 3 specification TS 29.207.
Summary of change:	⌘[H	QoS information is only provided for the combined set of flows requested by the GGSN. Clarification of the Diffserv Edge Function Functional Components that can be installed on the basis of PDP Context parameters and on the basis of static configuration is added. A definition for QoS class is provided.
Consequences if not approved:	⌘	The stage 2 specification is not aligned with the stage 3 specification. The Diffserv edge functions in the GGSN would remain unclear. The terminology "QoS class" would remain unclear.

Clauses affected:	⌘	5.1.1.3, 5.2.1, 5.2.3, 5.3.1, 5.3.2, 6.1.1, A.2.3, A.2.5, C				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	This CR is combined from 3 different WG-approved CRs: CR#50 (S2-023063), CR#44rev3 (S2-023064), and CR#52 (S2-023535).				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First amended section

5.1.1.3 Interaction to 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 IP 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.

In addition, where the UMTS network is also using external IP network resources as part of the UMTS bearer service (for example for the backbone bearer service), it may also be necessary to interwork with that network.

The GGSN shall support DiffServ edge functionality~~ and be able to shape upstream traffic~~. There are a number of other mechanisms provided to support interoperator interworking, some of which are given below.

NOTE: This list is not exhaustive. Other options are possible.

- Signalling along the flow path: In this scenario, resource requirements are explicitly requested and either granted or rejected through the exchange of signalling messages between network elements along the path of the IP packet flow. Signalling may be performed on a per-flow basis (e.g. using end to end RSVP) or it may be performed for an aggregate set of flows. In the latter case, it is expected that signalling exchanges would only be required when there are changes required in the resources allocated to an aggregate set of flows.

- Interaction between network management entities: In this scenario, resource requirements need to be explicitly negotiated and provisioned through network management entities. The results of this exchange are then enforced in the border nodes separating DiffServ administrative domains.

- Service Level Agreements enforced by the border routers between networks: In this scenario, resources are allocated along the path based on agreements between the network operators. The border routers along the path flow are provisioned with the characteristics of the aggregated traffic that is allowed to flow between systems.

Next amended section

5.2.1 GGSN

This clause provides functional descriptions of capabilities in GGSN. The capabilities are part of IP BS Manager (see 5.1.1.1) or corresponding user plane functions. Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

The **DiffServ Edge Function** shall be compliant to the IETF specifications for Differentiated Services [6]. The IETF Differentiated Services architecture will be used to provide QoS for the external bearer service.

Parameters for the Diffserv Edge Function (i.e. classifiers, meters, packet handling actions) may be statically configured on the GGSN, derived from PDP Context parameters and/or derived from RSVP signalling.

Diffserv functions configured on the basis of PDP Context parameters consist of marking user packets. The DSCP to be used is derived from the PDP Context parameters according to statically configured rules.

Statically configured Diffserv functions may include classifiers, meters, markers, droppers and shapers acting on uplink traffic.

RSVP/IntServ Function

[Editor's note: Detailed functional description of RSVP/IntServ Function is FFS]

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a combined set of IP flows~~packets (or IP "flows") defined by a packet classifier~~. The policy enforcement function includes policy-based admission control that is applied to the ~~IP ~~bearer~~s~~ associated with the flows, and configuration of the ~~packet handling and ~~policy based "gating" functionality in the user plane.   Service-based local policy decisions are either "pushed" to or requested by the GGSN via the Go interface.

Policy-based admission control ensures that the resources that can be used by a particular set of IP flows are within the "authorized resources" specified via the Go interface. The authorized resources provide an upper bound on the resources that can be reserved or allocated for ~~an~~the set of IP flows. The authorized resources are~~may be~~ expressed as a maximum authorised bandwidth and QoS class~~an Intserv-style Flowspec~~. The QoS class identifies a bearer service (which has a set of bearer service characteristics associated with it). The PDF generates a maximum authorized QoS class for the set of IP flows. This information is mapped by the **Translation/mapping function** in the GGSN to give the authorized resources for UMTS bearer admission control.

In the user plane, policy enforcement is defined in terms of a "gate" implemented in the GGSN. A gate is a policy enforcement function that interacts through Go interface with PCF as the Policy Decision Point for QoS resource authorisation at the IP BS level for a unidirectional flow of packets. Gate operations as defined in TS23.228 are to ~~define the ~~control and ~~to ~~manage media flows based on policy, and are under the control of PCF. A gate operates on a unidirectional flow of packets, i.e., in either the upstream or downstream direction. A gate consists of a packet classifier, and a gate status (open/closed)~~, a traffic metering function, and user plane actions to be taken for the set of packets matching the classifier~~.   When a gate is open, the packets in a flow are accepted, and are thus subject to the Diffserv edge treatment~~ (policing or marking) as determined by traffic metering and user plane actions~~. When a gate is closed, all of the packets in the flow are dropped.

The gate shall be applied to the PDP contexts where SBLP applies, and for such PDP contexts the information received in the TFT is ignored. In the downlink direction, packets are processed against each gate in turn until a match is found. If a match is not found, packet processing shall then continue against filters installed from UE supplied TFTs for PDP contexts where SBLP is not applied according to specification TS 23.060.

In the uplink direction, packets received on a PDP context with SBLP based filters shall be matched against those filters. If a match is found, the packet shall be passed if the gate associated with that filter is open processed according to the gate functions. If the gate is closed, or if the packet does not match any of the packet filters, the packet shall be silently discarded.

The packet classifier associated with a gate is a micro-flow classifier including the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow.

Elements of the 5-tuple that cannot be derived from the SDP according to a set of rules shall be wild-carded.~~ It is possible for a set of packets to match more than one classifier.   When this happens, the sequence of actions associated with the gates are executed in sequence.   Packets that are marked by a gate may not be (re)marked by a subsequent gate to a Diffserv Code Point corresponding to a better service class.~~

The **Binding Mechanism Handling** associates the PDP context bearer with one or more IP flows in order to support service-based local policy enforcement.   Binding information is included in PDP Context Activation or Modification messages to associate the PDP context bearer with SBLP policy decision information provided by the PCF associated with the IP flow(s). In order to allow SBLP policy information to be "pulled" from the PCF, the binding information shall allow the GGSN to determine the address of the PCF to be used.

When binding information is received, the GGSN shall ignore any UE supplied TFT, and the filters in that TFT shall not be installed in the packet processing table. When sending the binding information to the network, the Ue shall populate the TFT filters with wildcard values.

Next amended section

5.2.3 P-CSCF(PCF)

This clause provides functional descriptions of capabilities in P-CSCF(PCF). Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.

Service-based Local Policy Decision Point

- Authorize QoS resources (bandwidth, etc.) for the session. The P-CSCF (PCF) shall use the SDP contained in the SIP signaling message to calculate the proper authorization. The authorization shall be expressed in terms of the IP resources to be authorized. The authorization shall include limits on QoS for the set of IP ~~packet~~ flows and restrictions on individual IP flows (eg. destination address and port).

–For bi-directional media flows, the P-CSCF(PCF), according to operator policy, may assume that the 64-bit IPv6 address prefix of the source address for downstream packets is the same as the prefix of the destination address for upstream packets of the same media flow. The implementation of this P-CSCF(PCF) assumption would be determined by operator policy in order to reduce the possibilites of bearer misuse In the filters supplied by the PCF for bi-directional flows, the source address prefix for downstream packets may be identified as the same as the destination address prefix for the upstream. Similarly, the source address prefix for the upstream packets may be identified as the same as the destination address prefix for the downstream.

- The P-CSCF (PCF) shall be able to enforce the behaviour of the UE in respect to the assignment of IMS media components to the same PDP Context or to separate PDP Contexts. This behaviour of the UE is controlled by the IMS network using the indications described in Sections 4.2.5.1 of [4]. In case the UE violates this indication, and attempts to carry multiple IMS media components in a single PDP context despite of an indication that mandated separate PDP contexts, the P-CSCF/PCF shall take care that such a PDP context would be rejected by the GGSN. To do so, the P-CSCF/PCF uses the Go interface.

- The P-CSCF (PCF) shall be able to decide if new QoS authorization (bandwidth, etc.) is needed due to the mid-call media or codec change. A new authorization shall be required when the resources requested by the UE for a flow exceeds previous authorization, or a new flow is added, or when elements of the packet classifier(s) for authorized flows change.

- The PCF functions as a Policy Decision Point for the service-based local policy control.

- The PCF shall exchange the authorization information with the GGSN via the Go interface.

- PCF provides final policy decisions controlling the allocated QoS resources for the authorized media stream. The decision shall be transferred from the PCF to the GGSN.

- At IP multimedia session release, the PCF shall revoke the QoS resource authorization for the session.

Binding Mechanism Handling

- The PCF generates an authorization token for each SIP session and the P-CSCF sends the authorization token to the UE in SIP signalling. The authorization token may contain information that identifies its generator. The authorization token shall be unique across all PDP contexts associated with an APN. The authorization token conforms to the IETF specification on SIP Extensions for Media Authorization.

Next amended section

5.3.1 Go Functional Requirements

The Go interface allows service-based local policy and QoS inter-working information to be "pushed" to or requested by the GGSN from a Policy Control Function (PCF). The Go interface provides information to support the following functions in the GGSN:

~~– Control of Diffserv inter-working~~

–

- Control of service-based policy "gating" function in GGSN
- UMTS bearer authorization
- Charging correlation related function

The Common Open Policy Service (COPS) protocol supports a client/server interface between the Policy Enforcement Point in the GGSN and Policy Control Function (PCF). The Go interface shall conform to the IETF COPS framework as a requirement and guideline for Stage 3 work.

The COPS protocol allows both push and pull operations. For the purpose of the initial authorisation of QoS resources the pull operation shall be used. Subsequently the interactions between the PCF and the GGSN may use either pull or push operations.

Policy decisions may be stored by the COPS client in a local policy decision point allowing the GGSN to make admission control decisions without requiring additional interaction with the PCF.

Next amended section

5.3.2 Information Elements Exchanged via Go Interface

- The COPS protocol supports several messages between a client and server.

Additional 3GPP Go-specific information elements must be included in COPS messages to support the SBLP control functions identified in Section 5.3.1. Consistent with the COPS framework, the Go interface is identified by a "client type" allocated for a 3GPP Go COPS client (GGSN).

All of the information described in the remainder of this section applies specifically to the 3GPP Go COPS client type. The events specific to the UMTS or IP bearer service would trigger the request messages from the GGSN PEP to the PCF.   The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the PCF and the GGSN.

A **Request** (REQ) message from the GGSN to the PCF shall allow the GGSN to request SBLP policy information for ~~the~~a set of IP flow~~(s)~~ identified by binding information (described below).

Binding information associates the PDP context to the IMS session and IP flows, and is used by the GGSN to request SBLP policy information from the PCF. The binding information includes 1) an authorization token sent by the P-CSCF to the UE during SIP signalling, and 2) one or more flow identifiers used by the UE, GGSN and PCF to uniquely identify the IP media flow(s).

The authorization token shall be unique within the scope of the operator's domain. The authorization token conforms to relevant IETF standards on SIP Extensions for Media Authorization.

A flow identifier identifies an IP media flow associated with the SIP session. Flow identifiers are based on the ordering of media components (media description structure defined by a single 'm=' line), and port numbers within that media component in the SDP. A flow identifier combined with the authorization token shall be sufficient to uniquely identify an IP media flow.

A **Decision** (DEC) message from the PCF to the GGSN contains decision objects. A Decision object shall include one of the following commands:

- Install (Admit request/Install configuration, Commit)
- Remove (Remove request/Remove configuration)

These commands are used to:

- Authorize QoS/Revoke QoS authorization for one or more IP flows
- Control forwarding for one or more IP flows

The **responses** from the PEP to the PCF include an acknowledgement and/or an error response to commands received by the PEP. The following response messages shall be supported:

- Report State (Success/Failure/Accounting) (RPT)

The **Delete Request State (DRQ)** message from the PEP to the PCF indicates that the request state of a previously authorised bearer resource is no longer available/relevant at the GGSN so the corresponding COPS policy state shall likewise be removed at the PCF. The DRQ message includes the reason why the request state was deleted.

The Install command used to Authorize QoS contains the following policy information associated with the IP flow(s):

- Packet classifier(s)

- Authorized QoS information
- Packet handling action
- Event generation information (e.g. charging identity)

The packet classifier includes the standard 5-tuple: (source IP address, destination IP address, source port, destination port, protocol), identifying a set of packets associated with a unidirectional flow. Elements of the 5-tuple may be wild-carded.

The authorized QoS information provides an upper bound on the resources that can be reserved or allocated for the combined set of IP flow~~(s)~~. The authorized QoS information shall contain the DiffServ class and Data rate parameter. The DiffServ class is used only to identify the maximum allowed traffic class.

NOTE: Further elements and details of the authorized QoS information are defined in 29.207.

The packet handling action defines the packet handling that should be accorded to ~~in-profile and out-of-profile~~ packets matching the packet classifier. ~~In-profile traffic is defined as traffic that is within the authorized QoS information. The packet handling action may be ignored by the GGSN.~~ The packet handling action (gate status) shall result in packets being passed (gate open), or silently discarded (gate closed).

Event generation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with IMS session records from the P-CSCF. The PCF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision. The GGSN shall send the GCID of the PDP context and the GGSN address to the PCF as part of the authorisation report (RPT).

The messages which revoke QoS authorisation or remove configuration information provide only the information that is needed to perform the action (e.g., the COPS handle element, which is used as a way of identifying the installed decision information).

Next amended section

6.1.1 Procedures in the GGSN

The QoS procedures in the GGSN are triggered by the QoS signaling messages from the UE, i.e., PDP Context Activation message or the RSVP messages. The exact QoS procedures in the GGSN depend on the GGSN and UE QoS capabilities. The GGSN is required to support Diffserv edge function. Other QoS capabilities that may be supported at the GGSN are RSVP functions and service-based local policy enforcement functions.

For UEs that do not support RSVP, the GGSN may use the PDP context~~IP~~ level information ~~(e.g., addressing 5-tuple) provided by service based local policy according to the authorization token~~ to configure the DiffServ edge~~classifier~~ functionality and provide internetworking between PDP context and backbone IP network. The authorization token is included in the PDP context activation/modification messages.

For UEs that support RSVP, the GGSN may also support RSVP and use RSVP rather than the PDP context to control the QoS through the backbone IP network. ~~The GGSN may use IP level information provided by service based local policy according to authorization token to authorize the RSVP session and configure the DiffServ classifier functionality.~~ The authorization token may be included in the RSVP signaling and the PDP context activation/modification messages. Alternatively, the RSVP messages may pass transparently through the GGSN.

If SBLP is implemented in the operator's network, the GGSN shall authorize the PDP context activation/modification messages ~~and optionally (dependent on operator policy) RSVP messages~~ that are subject to service based local policy by sending an authorization request to the PCF. Alternatively, the GGSN may authorize PDP context activation/modification messages ~~and optionally (dependent on operator policy) RSVP messages~~ that are subject to service based local policy using the cached policy in the Local Decision Point. The GGSN shall map the received IP flow based policy information into PDP context based policy information.

Next amended section

A.2.3 Scenario 3

The UE performs an IP BS function which enables end-to-end QoS using IP layer signalling towards the remote end. There is no IP layer signalling between the IP BS Managers in the UE and the GGSN. However, the GGSN may make use of information regarding the PDP context which is signalled between the UMTS BS managers and provided through the translation/mapping function.

This scenario assumes that the UE and GGSN support DiffServ edge functions, and that the backbone IP network is DiffServ enabled. In addition, the UE supports RSVP signalling which interworks within the UE to control the DiffServ.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS requirements. The QoS requirements from application layer (e.g. TS23.228 describes interworking from SIP/SDP to QoS requirements) are mapped down to create an RSVP session. The UE shall establish the PDP context suitable for support of the RSVP session. The authorisation token from the application layer when included shall be mapped to ~~the corresponding RSVP signalling parameters as well as~~ the PDP context parameters, and may also be mapped to the RSVP signalling.

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. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060).

In this scenario, the terminal supports signalling via the RSVP protocol to control the QoS at the local and remote accesses, and DiffServ to control the IP QoS through the backbone IP network. The RSVP signalling protocol may be used for different services. It is expected that only RSVP using the Integrated Services (IntServ) semantics would be supported, although in the future, new service definitions and semantics may be introduced. The entities that are supporting the RSVP signalling should act according to the IETF specifications for IntServ and IntServ/DiffServ interwork.

The QoS for the wireless access is provided by the PDP context. The UE may control the wireless QoS through signalling for the PDP context. The characteristics for the PDP context may be derived from the RSVP signalling information, or may use other information.

QoS for the IP layer is performed at two levels. The end-to-end QoS is controlled by the RSVP signalling. Although RSVP signalling can be used end-to-end in the QoS model, it is not necessarily supported by all intermediate nodes. Instead, DiffServ is used to provide the QoS throughout the backbone IP network.

At the UE, the data is also classified for DiffServ. Intermediate QoS domains may apply QoS according to either the RSVP signalling information or DiffServ mechanisms. In this scenario, the UE is providing interworking between the RSVP and DiffServ domains. The GGSN may override the DiffServ setting from the UE. This GGSN may use information regarding the PDP context in order to select the appropriate DiffServ setting to apply, as shown in the figure below.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and DiffServ in the remote access network in the scenario shown in the figure below. The RSVP signalling may control the QoS at both the local and remote accesses. This function may be used to determine the characteristics for the PDP context, so the UE may perform the interwork between the RSVP signalling and PDP context.

The UE provides control of the DiffServ (although this may be overwritten by the GGSN), and in effect, determines the appropriate interworking between the PDP context and DiffServ.

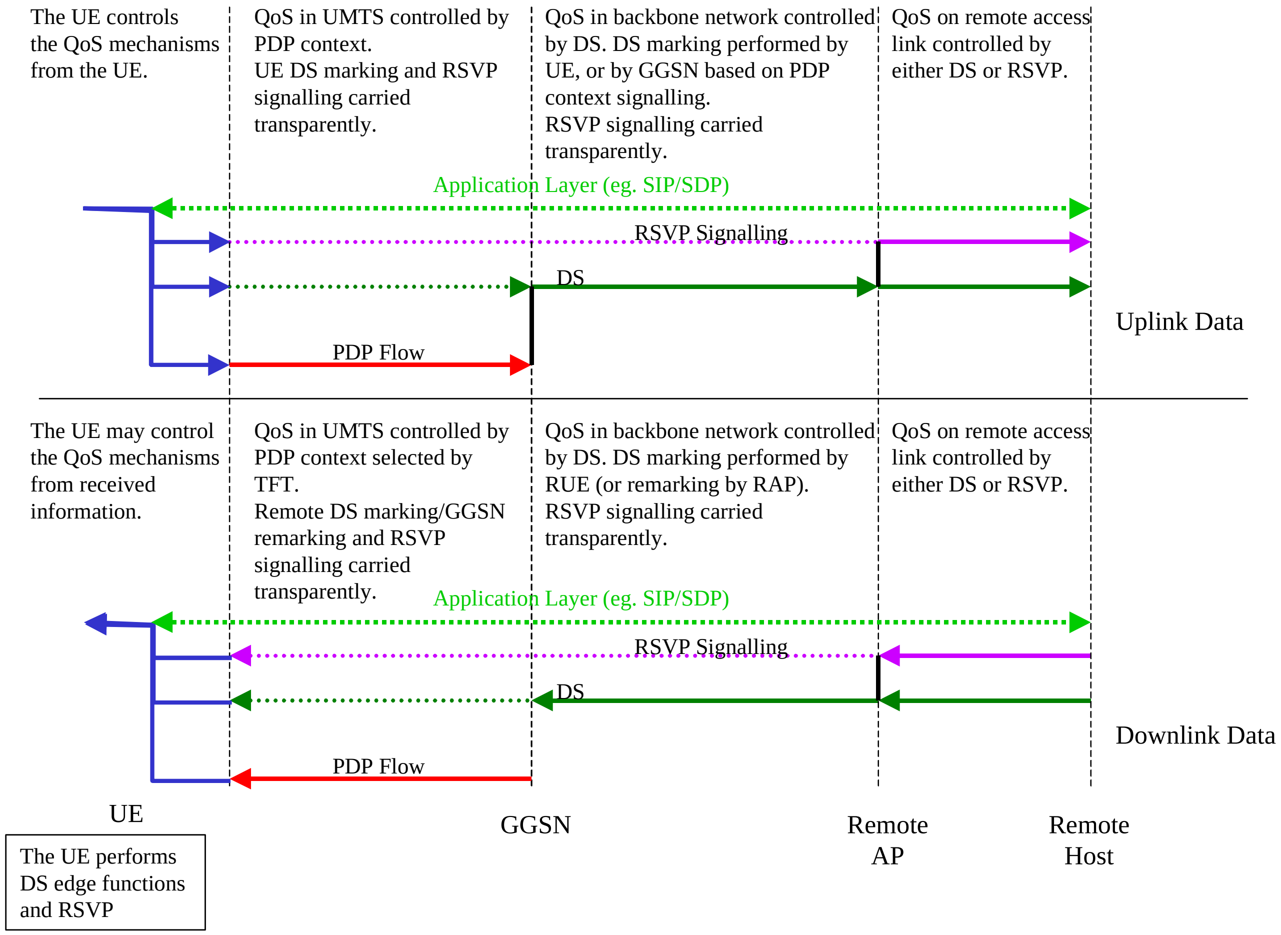
The UE controls the QoS mechanisms from the UE.
QoS in UMTS controlled by PDP context. UE DS marking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by UE, or by GGSN based on PDP context signalling. RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
PDP Flow
Uplink Data
The UE may control the QoS mechanisms from received information.
QoS in UMTS controlled by PDP context selected by TFT. Remote DS marking/GGSN remarking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by RUE (or remarking by RAP). RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
PDP Flow
Downlink Data
UE
GGSN
Remote AP
Remote Host
The UE performs DS edge functions and RSVP

Figure A.4: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; without service based policy

~~When the authorisation token is included in the PDP context establishment/modification (as per section 5.1.1.2.3), the GGSN may use IP level information provided by service based local policy according to the authorisation token to configure the DiffServ classifier functionality. The information can also be used for DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point.~~The GGSN provides the interworking between the PDP context and the DiffServ function

The application layer signaling may be processed in the local network at an application server such as the P-CSCF in the case of SIP signaling. Interworking between the GGSN and the application layer is shown as a vertical line where applicable. This interworking is for policy control and is between the GGSN and the PCF policy function co-located in the P-CSCF, as shown in the figure below.

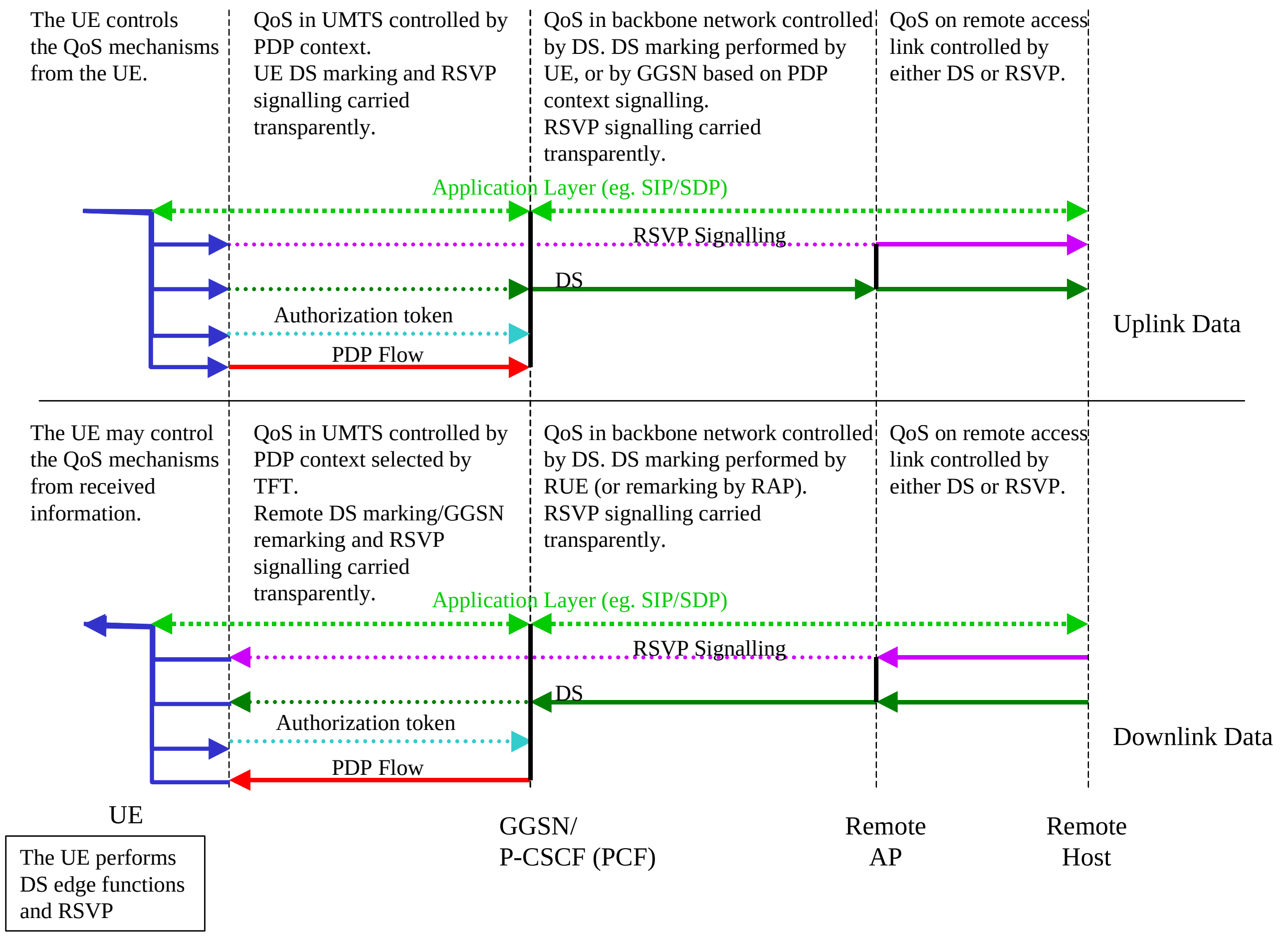
The UE controls the QoS mechanisms from the UE.
QoS in UMTS controlled by PDP context. UE DS marking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by UE, or by GGSN based on PDP context signalling. RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Authorization token
PDP Flow
Uplink Data
The UE may control the QoS mechanisms from received information.
QoS in UMTS controlled by PDP context selected by TFT. Remote DS marking/GGSN remarking and RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by RUE (or remarking by RAP). RSVP signalling carried transparently.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Authorization token
PDP Flow
Downlink Data
UE
The UE performs DS edge functions and RSVP
GGSN/ P-CSCF (PCF)
Remote AP
Remote Host

Figure A.5: Local UE supports RSVP signalling with IntServ semantics, and DiffServ; where service based policy is applied

Next amended section

A.2.4 Scenario 4

The UE performs an IP BS function which enables end-to-end QoS using IP layer signalling towards the remote end. However, the UE relies on this end-to-end communication being utilised by at least the access point (GGSN) in order to provide the end-to-end QoS.

This scenario assumes that the UE and GGSN support RSVP signalling which may control the QoS directly, or interwork with DiffServ. The backbone IP network is RSVP and/or DiffServ enabled.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS requirements. The QoS requirements from application layer (e.g. TS23.228 describes interworking from SIP/SDP to QoS requirements) are mapped down to create an RSVP session. The UE shall establish the PDP context suitable for support of the RSVP session. The authorisation token from the application layer shall be mapped to ~~the corresponding RSVP signalling parameters and~~ the PDP context parameters, and may also be mapped to the RSVP signalling.

In this scenario, the terminal supports signalling via the RSVP protocol to control the QoS across the end-to-end path. The GGSN also supports the RSVP signalling, and uses this information rather than the PDP context to control the QoS through the backbone IP network. The control of the QoS through the core is expected to be supported through interworking with DiffServ at the GGSN, although it may optionally be supported by per flow resource reservation. The RSVP signalling protocol may be used for different services. It is only expected that only RSVP using the Integrated Services (IntServ) semantics would be supported, although in the future, new service definitions and semantics may be introduced. The entities that are supporting the RSVP signalling may fully support the specifications for IntServ and IntServ/DiffServ interwork. If not, they are expected to set the break bit.

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. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060).

QoS for the IP layer is performed at two levels. The end-to-end QoS is controlled by the RSVP signalling. Although RSVP signalling occurs end-to-end in the QoS model, it is not necessarily supported by all intermediate nodes. DiffServ is used to provide the QoS throughout the backbone IP network, although optionally each node may support RSVP signalling and allocation of resources per flow. An authorisation token may be included in the RSVP signalling and the PDP context establishment/modification. The GGSN may ~~use IP level information provided by service based local policy according to the authorisation token to~~ authorise the RSVP session and configure the Diffserv classifier functionality.~~ The information may also be used in conjunction with a Diffserv aggregate to enable DiffServ class admission control, e.g., the requested end-to-end bandwidth from the UE for a particular flow may be informed to the GGSN beforehand for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point.~~

The GGSN supports the RSVP signalling and acts as the interworking point between RSVP and DiffServ. Intermediate QoS domains may apply QoS according to either the RSVP or DiffServ mechanisms.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and RSVP in the remote access network in the scenario shown in the figure below. The RSVP signalling may control the QoS at the local access. This function may be used to determine the characteristics for the PDP context, so the UE may perform the interwork between RSVP and the PDP context.

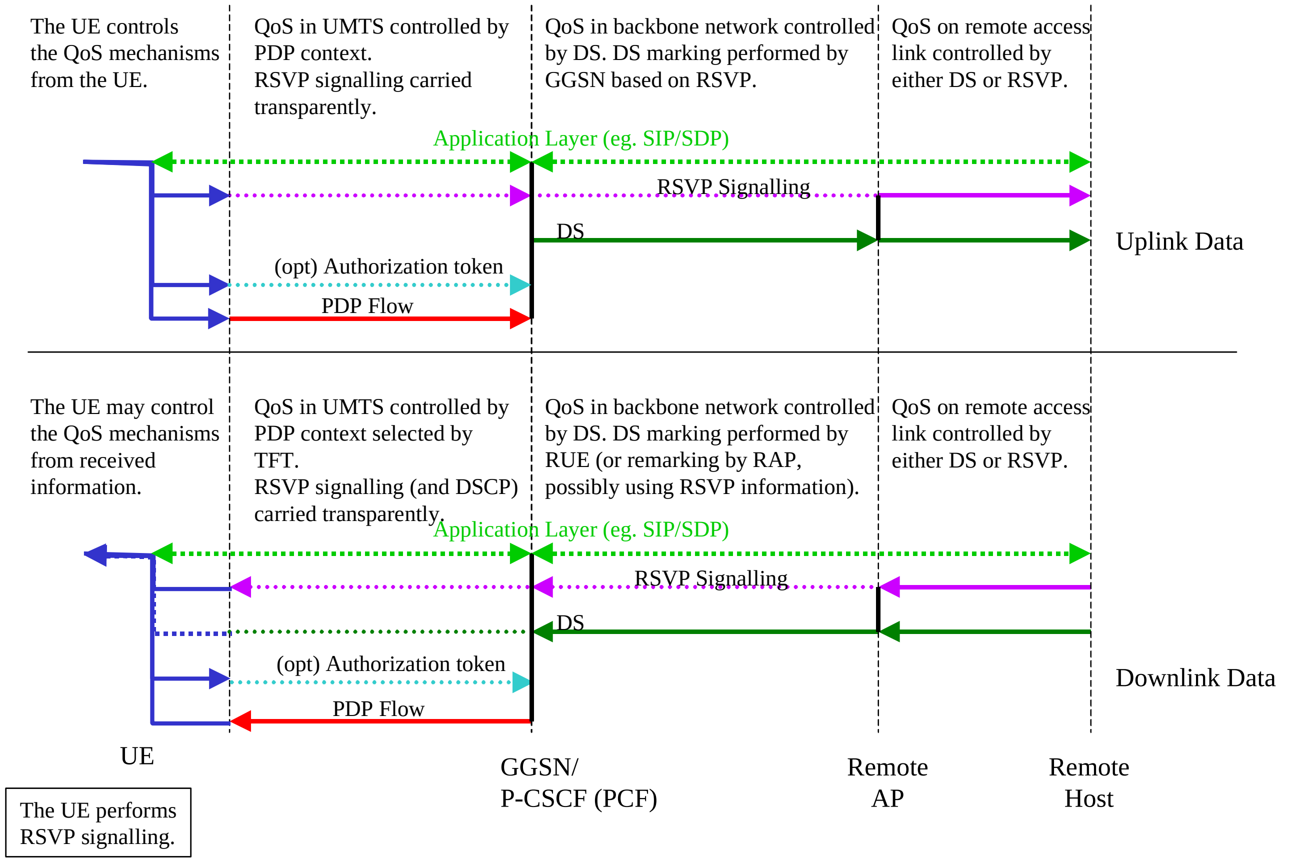
The UE controls the QoS mechanisms from the UE.
QoS in UMTS controlled by PDP context. RSVP signalling carried transparently.
QoS in backbone network controlled by DS. DS marking performed by GGSN based on RSVP.
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
Uplink Data
(opt) Authorization token
PDP Flow
The UE may control the QoS mechanisms from received information.
QoS in UMTS controlled by PDP context selected by TFT. RSVP signalling (and DSCP) carried transparently.
QoS in backbone network controlled by DS. DS marking performed by RUE (or remarking by RAP, possibly using RSVP information).
QoS on remote access link controlled by either DS or RSVP.
Application Layer (eg. SIP/SDP)
RSVP Signalling
DS
(opt) Authorization token
PDP Flow
Downlink Data
UE
GGSN/ P-CSCF (PCF)
Remote AP
Remote Host
The UE performs RSVP signalling.

Figure A.6: Local UE supports RSVP signalling using IntServ Semantics

Next amended section

A.2.5 Scenario 5

The UE performs an IP BS function which enables end-to-end QoS without IP layer signalling and negotiation towards the IP BS function in the GGSN, or the remote host. The P-CSCF provides the authorization token to the UE during the SIP session setup process, and the UE provides the authorization token to the GGSN in the PDP context activation/modification message~~, to enhance the interworking options to the DiffServ edge function of the GGSN~~. The GGSN uses the authorization token to obtain a policy decision from the P-CSCF(PCF)~~ which will be used to derive IP level information~~. This is done via the standardized interface between the PCF and GGSN. Even if the interface is an open interface where all information elements are standardized, the actual usage of the information is operator specific.

~~In addition, IP level information may also be derived from PDP context (e.g. QoS parameters).~~

The scenario assumes that the GGSN support DiffServ edge functions, and that the backbone IP network is DiffServ enabled.

The application layer (e.g. SIP/SDP) between the end hosts identifies the QoS needs. The QoS requirements from application layer (e.g. TS23.228 describes interworking from SIP/SDP to QoS requirements) are mapped down to the IP layer and further down to the PDP context parameters in the UE. The authorisation token from the application layer is included in the PDP context parameters by the UE.

~~The GGSN DiffServ edge function may use the IP level information (e.g., 5-tuple combination of source and destination IP address, source and destination port number, and the protocol identifier) provided by service based local policy according to the authorisation token to configure the DiffServ classifier functionality. The information can be used for DiffServ class admission control, e.g., for the GGSN DiffServ edge to determine if the flow can be allowed to a certain DiffServ class or to/from an ingress/egress point. As a result, the GGSN may select the appropriate DiffServ setting to apply. This is shown in the figure below.~~

In this scenario, the control of the QoS over the UMTS access network (from the UE to the GGSN) may be performed from the terminal using the PDP context signalling. Alternatively, subscription data accessed by the SGSN may override the QoS requested via signalling from the UE (according to the procedures specified in TS 23.060).

The QoS for the downlink direction is controlled by the remote host from the remote network to the GGSN. The PDP context controls the UMTS level QoS between the GGSN and the UE. The QoS in the uplink direction is controlled by the PDP context up to the GGSN. The GGSN configures the DiffServ Edge function~~uses the IP level information~~ to interwork with~~ DiffServ in~~ the backbone IP network and ~~-~~control the IP QoS bearer service towards the remote -host.

The end-to-end QoS is provided by a local mechanism in the UE, the PDP context over the UMTS access network, DiffServ through the backbone IP network, and DiffServ in the remote access network. Note that DiffServ control at the Remote Host is shown in this example. However, other mechanisms may be used at the remote end, as demonstrated in the other scenarios.

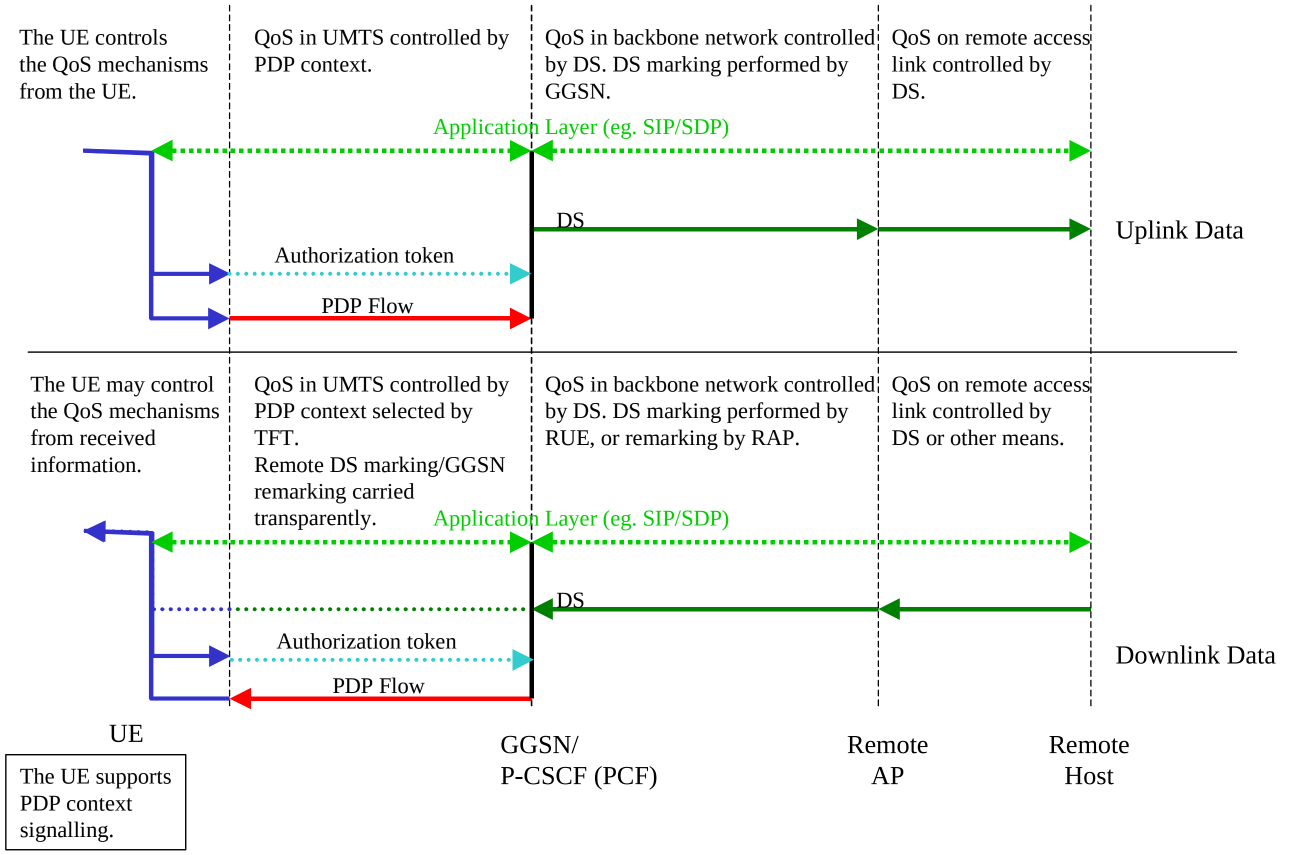
The UE controls the QoS mechanisms from the UE.
QoS in UMTS controlled by PDP context.
QoS in backbone network controlled by DS. DS marking performed by GGSN.
QoS on remote access link controlled by DS.
Application Layer (eg. SIP/SDP)
DS
Uplink Data
Authorization token
PDP Flow
The UE may control the QoS mechanisms from received information.
QoS in UMTS controlled by PDP context selected by TFT.
Remote DS marking/GGSN remarking carried transparently.
QoS in backbone network controlled by DS. DS marking performed by RUE, or remarking by RAP.
QoS on remote access link controlled by DS or other means.
Application Layer (eg. SIP/SDP)
DS
Authorization token
PDP Flow
Downlink Data
UE
The UE supports PDP context signalling.
GGSN/
P-CSCF (PCF)
Remote
AP
Remote
Host

Figure A.7: Local UE provides authorization token in PDP context activation/modification message and GGSN provides interworking with DiffServ

Next amended section

Annex C (informative): Sample Mapping of SDP Descriptions Into QoS Authorization

The QoS requirement for a session depends on the media and codec information for the session. Initial session establishment in the IM Subsystem must determine a common codec (or set of common codecs for multimedia sessions) that will be used for the session. This is done through an end-to-end message exchange to determine the complete set of common codecs, and then the session initiator makes the decision as to the initial set of codecs for the media flows.

The session initiator includes an SDP in the SIP INVITE message that lists every codec that the originator is willing to support for this session. When the message arrives at the destination endpoint, it responds with the subset that it is also willing to support for the session by selectively accept or decline those media types in the original list. When multiple media codecs are listed, the caller and called party's media fields must be aligned—that is, there must be the same number, and they must be listed in the same order. QoS authorization is performed for this common subset. The P-CSCF(PCF) shall use the SDP contained in the SIP signaling to calculate the proper authorization. The authorization shall include limits on IP resources, and restrictions on IP packet flows, and may include restrictions on IP destinations. These restrictions are expressed as a data rate and QoS class for the combined set of IP flows, and a set of~~may take the form of a flowspec and~~ filter specs.

The QoS authorization for a session shall include an Authorization-Token, which shall be assigned by the P-CSCF(PCF). The Authorization-Token shall~~may~~ contain information that identifies the P-CSCF(PCF) that generated the token. Each authorized session may include several flow authorizations. Each flow authorization may include an authorization for one or more flows. The authorization shall contain the following information:

- Filter Specs (IP flow 5-tuples that identify~~ies~~ the set of flows)
- Data rate and QoS class~~FLOWSPEC~~ that describes the authorized resource for the set of flows

~~– DSCP that identifies the assigned DiffServ PHB the flow~~

~~–~~The IP flow 5-tuples includes Source Address, Source Port, Destination Address, Destination Port and Protocol ID. Note that some fields may be wildcarded.~~The FLOWSPEC includes the following elements:~~

~~– Token rate [r]~~

~~– Bucket depth [b]~~

~~– Peak rate [p]~~

~~– Minimum policed unit [m]~~

- ~~Maximum packet size [M]~~

A typical SDP description consists of a session-level description (details that apply to the whole session and all media flows) and the several media-level descriptions (details that apply to a single media flow). The four critical components for mapping an SDP description into a QoS authorization are the media announcements ("m="), the connection data ("c="), the attributes ("a=") and the bandwidth ("b=").

The media announcements field contains information about the type of media session, and is of the form:

m=<media> <port> <transport> <fmt list>

The attributes field contains attributes of the preceding media session, and is of the form:

a=<attribute><value>

The connection data field contains information about the media connection, and is of the form:

c=<network type> <address type> <connection address>

The optional bandwidth field contains information about the bandwidth required, and is of the form:

b=<modifier>:<bandwidth-value>

An example SDP description from the session originator in the SIP INVITE message:

v=0

o=hshieh 2890844526 2890842807 IN IP4 saturn.attws.com

s=-

c=IN IP4 192.141.10.188

t=0 0

b=AS:64

m=audio 29170 RTP/AVP 3 96 97

a=rtpmap:96 G726-32/8000

a=rtpmap:97 AMR

a=fmtp:97 mode-set=0,2,5,7; maxframes=2

m=video 51372 RTP/AVP 34

a=fmtp 34 SQCIF=2/MaxBitRate=500/SAC AP

m=application 32416 udp text_chat

The called party answers the call and returns the following SDP description in the SIP 183 message:

```
v=0
o=johndoe 2890844526 2890842807 IN IP4 uranus.solar.com
s=-
c=IN IP4 204.142.180.111
t=0 0
b=AS:64
m=audio 31160 RTP/AVP 3 97
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; maxframes=2
a=recvonly
m=video 61000 RTP/AVP 31
a=fmtp 34 SQCIF=2/MaxBitRate=500/SAC AP
m=application 33020 udp text_chat
a=sendonly
```

Upon receiving the above SDP, the originator's P-CSCF will authorize QoS resource for the originator UE with the following media flows:

A uplink audio flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
192.141.10.188	*	204.142.180.111	31160	17

~~This audio flow uses either AMR or GSM FR codec and the authorized resource envelope can be expressed as a FLOWSPEC as follow:~~

~~b~~	~~m~~	~~M~~	~~r~~	~~p~~
~~72.5 bytes~~	~~52 bytes~~	~~72.5 bytes~~	~~3625 bytes/s~~	~~3625 bytes/s~~

~~*See Note 1 for the mapping calculation~~

Since the conversational audio is very sensitive to delay, the ~~DiffServ EF class will be used for the flow, e.g., DSCP = 101110~~maximum QoS class corresponding to conversational traffic class would be set. The b parameter is used to determine the maximum authorised data rate.

An uplink video flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
192.141.10.188	*	204.142.180.111	61000	17

~~The video flow uses H.263 SQCIF codec with 15frame/s. Let's assume the average bit rate and peak bit rate for the encoded video are 28kb/s and 40kb/s respectively. The authorized resource envelope can be expressed as a FLOWSPEC as follow:~~

~~b~~	~~m~~	~~M~~	~~r~~	~~p~~
~~373 bytes~~	~~273 bytes~~	~~373 bytes~~	~~4095 bytes/s~~	~~5595 bytes/s~~

~~*See Note 2 for the mapping calculation~~

The video flow may be assigned a ~~DiffServ AF class with DSCP = 001010~~maximum QoS class corresponding to streaming traffic class. The b parameter is used to determine the data rate.

A downlink video flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
204.142.180.111	*	192.141.10.188	51372	17

~~The video flow uses H.263 SQCIF codec with 15frame/s. Let's assume the average bit rate and peak bit rate for the encoded video are 28kb/s and 40kb/s respectively. The authorized resource envelope can be expressed as a FLOWSPEC as follow:~~

~~b~~	~~M~~	~~M~~	~~r~~	~~p~~
~~373 bytes~~	~~273 bytes~~	~~373 bytes~~	~~4095 bytes/s~~	~~5595 bytes/s~~

~~*See Note 2 for the mapping calculation~~

The video flow may be assigned a ~~DiffServ AF class with DSCP = 001010~~maximum QoS class corresponding to streaming traffic class. The b parameter is used to determine the maximum authorised data rate.

A downlink udp flow:

The following IP 5-tuples identify the flow:

SrcAddress	SrcPort	DestAddress	DestPort	ProtocolID
204.142.180.111	*	192.141.10.188	32416	17

~~Assuming a typing speed of 1 char to 50 chars a second, the authorized resource envelope may be expressed as a FLOWSPEC as follow:~~

~~b~~	~~m~~	~~M~~	~~R~~	~~p~~
~~90 bytes~~	~~41 bytes~~	~~90 bytes~~	~~41 bytes/s~~	~~90 bytes/s~~

~~*See Note 3 for the mapping calculation~~

The udp application flow may be assigned a ~~DiffServ AF class with DSCP = 010100~~maximum QoS class corresponding to interactive. The b parameter is used to determine the data rate.

~~Note 1: With AMR or GSM FR codec, the authorization shall use the maximum rate of the two, i.e., 13kb/s. With 20ms frames, there are 50 frames per second and each frame has 260 bits or 32.5 bytes payload. With IP/UDP/RTP overhead of 40 bytes, each packet is 72.5 bytes. The token rate and peak rate for the session (i.e., r and p) are 72.5 x 50 = 3625 bytes /s. The bucket depth and Maximum packet size (i.e., b and M) are 72.5 bytes. The minimum AMR rate of 4.75kb/s is used to calculate the minimum policed unit m. At that rate, each frame has 95 bits or 16 byes. With the overhead of 40 bytes, we have m equals to 52 bytes.~~

~~Note 2: With variable video codec h.263, we assume an average rate at 28kb/s and peak rate at 40kb/s. The average rate is used to calculate r and m. With 15 frames a second, each frame has 1867 bits or 233 bytes. Each packet is 273 bytes, so the r is 273x15=4095 bytes/s and the m is 273 bytes. The peak rate is used to calculate b, M and p. With 40kb/s and 15 frames/s, each frame has 2667 bits or 333 bytes. Each packet is 373 bytes, so the p is 373x15=5595 bytes/s and the b and M are 373 bytes.~~

~~Note 3: The calculation is the same as in Note 2 with average rate of 1 byte/s and peak rate of 50 bytes/s.~~

Note: The sample mappings in this section are for illustration purpose only. The actual mapping of media codec to QoS resource requirement is specified in TS 29.208.

~~[Editorial note: The sample mappings in this section are for illustration purpose only. The actual mapping of media codec to QoS resource requirement, e.g., FLOWSPEC, is for further study.]~~