Technical Specification Group Services and System Aspects
Meeting #21, Frankfurt, Germany, 22-25 September 2003

TSGS#21(03)0378

Source: **TSG SA WG2**
Title: **CRs on 23.207**
Agenda Item: **7.2.3**

The following Change Request has been approved by TSG SA WG2 and is requested to be approved by TSG SA plenary #21.
Note: the source of all these CRs is now S2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

Tdoc #	Title	Spec	CR #	cat	Version in	REL	WI	S2 meeting
S2-033214	Functional additions for the Gq interface	23.207	060r1	B	5.8.0	6	QoS1	S2-34

CR-Form-v7

CHANGE REQUEST

⌘ **23.207** **CR** **60** ⌘ **rev** **1** ⌘ Current version: **5.8.0** ⌘

*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:	⌘	Functional additions for the Gq interface
Source:	⌘	Nokia, Nortel Networks, Siemens, Ericsson
Work item code:	⌘	QoS1
Date:	⌘	18/08/2003
Category:	⌘	**B**
Release:	⌘	Rel-6

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: ⌘

TS 23.207 currently describes a Policy Decision Function (PDF) that is only applicable for IMS and is tightly linked to SIP session control. As a result, PDF is currently shown as being a logical entity of the P-CSCF.
Such an architecture does not enable a generic service policy to be applied to both IMS and non-IMS services.

TR 23.917 has studied the feasibility of standardising the interface between the PDF and Application Functions (e.g. P-CSCF in the IM domain), and has developped functional descriptions and procedures. These new functionalities and procedures shall be reflected in the correspondng Technical Specification, i.e. TS 23.207.

Summary of change: ⌘

The description of functionalities and procedures has been updated to reflect the new functions of generalized service based policy control.

Consequences if not approved: ⌘

Clauses affected: ⌘ 1, 2, 3.1, 3.2, 5.1, 5.1.1.1, 5.1.2.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 6.1.1, 6.1.2, 6.1.3, 6.2
New clauses: 5.2.4, 5.3a, 6.1.4

Other specs affected: ⌘

Y	N		
X		Other core specifications	⌘ TS 23.002
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘

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.

1 Scope

The present document provides the framework for end-to-end Quality of Service involving GPRS and complements TS23.107 which describes the framework for Quality of Service within UMTS. –The end-to-end QoS architecture is provided in Figure 1. –The document describes the interaction between the TE/MT Local Bearer Service, the GPRS Bearer Service, and the External Bearer Service, and how these together provide Quality of Service for the End-to-End Service. –The document also describes IP level mechanisms necessary in providing end-to-end Quality of Service involving GPRS networks, including possible interaction between the IP level and the GPRS level, as well as the application level and the IP level.

In contrast to the TS23.107, the present document is only applicable to GPRS packet switched access services, and includes aspects of interworking to the IM subsystem as well as PSTN and other networks. –The document does not cover the circuit switched access services.

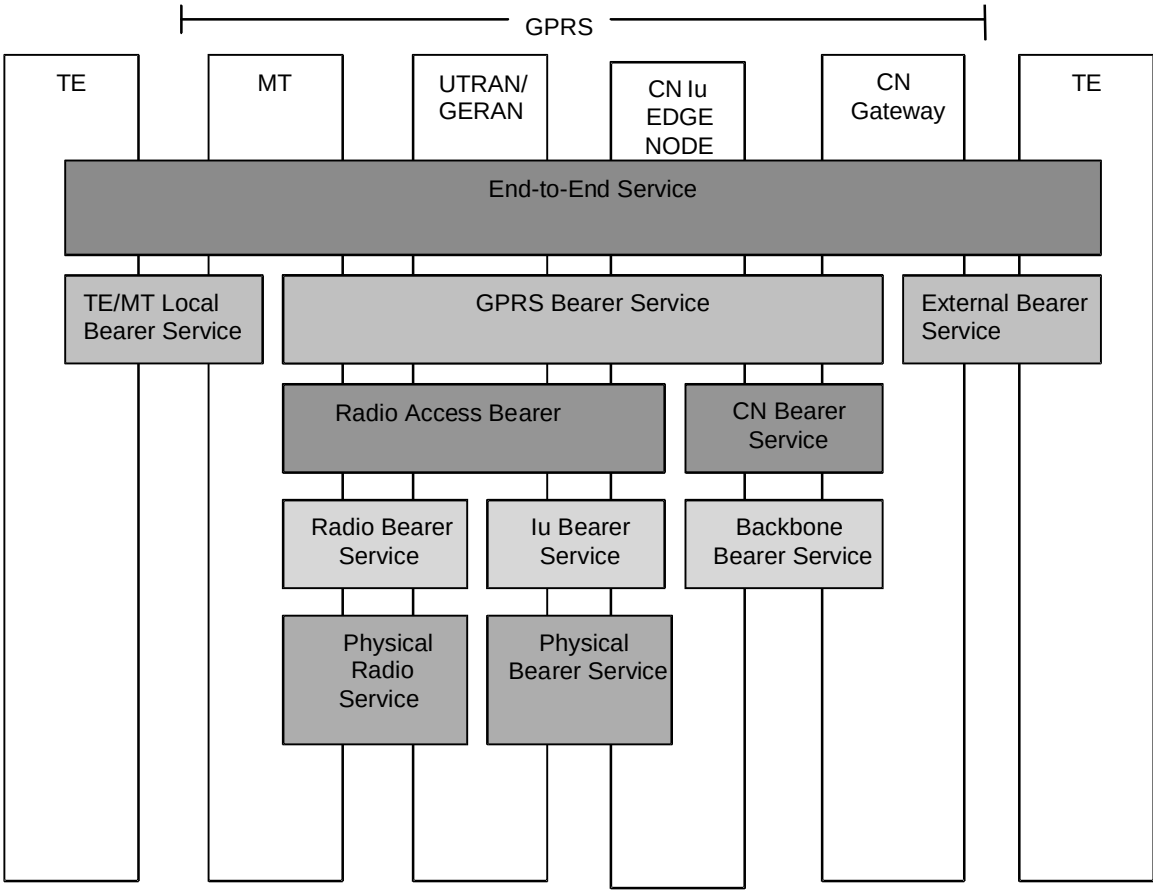

Figure 1: End-to-End QoS Architecture

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 TS 22.288: "Service requirements for the IP Multimedia – stage 1".

[2] 3GPP TS 23.002: "Network Architecture".

[3] 3GPP TS 23.107: "QoS Concept and Architecture".

[4] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – stage 2".

[4a] 3GPP TS 29.207: " Policy control over Go interface ".

[4b] 3GPP TS 29.208: " End to end Quality of Service (QoS) signalling flows".

[4c] 3GPP TS 29.xxx: "Policy control over Gq interface".

[5] 3GPP TS 22.105: "Vocabulary for 3GPP Specifications".

[6] RFC 2475: "An Architecture for Differentiated Services (Diffserv)".

[7] RFC 2753: "A Framework for Policy-based Admission Control ".

[8] RFC 2748: "Common Open Policy Service protocol (COPS)".

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

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

[11] RFC 2210: "The use of RSVP with IETF integrated Services".

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

[13] RFC 3261: "SIP: Session Initiation Protocol".

[14] RFC 2327: "Session Description Protocol".

[15] RFC 2998: "A Framework For Integrated Services Operation Over DiffServ Networks".

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

[17] RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[18] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions and Abbreviations

3.1 Definitions

RSVP - Resource ReSerVation Protocol: The RSVP protocol [9] is used by a host to request specific qualities of service from the network for particular application data streams or flows. The network responds by explicitly admitting or rejecting RSVP requests.

DiffServ: Diffserv networks classify packets into one of a small number of aggregated flows or "classes", based on the Diffserv codepoint (DSCP) in the packet's IP header. This is known as behavior aggregate (BA) classification [6]. At each Diffserv router, packets are subjected to a "per-hop behavior" (PHB), which is invoked by the DSCP [17].

IntServ - The integrated services architecture [12] defined a set of extensions to the traditional best effort model of the Internet with the goal of allowing end-to-end QOS to be provided to applications. One of the key components of the architecture is a set of service definitions; the current set of services consists of the controlled load and guaranteed services. The architecture assumes that some explicit setup mechanism is used to convey information to routers so that

they can provide requested services to flows that require them. –While RSVP is the most widely known example of such a setup mechanism, the Intserv architecture is designed to accommodate other mechanisms.

COPS - Common Open Policy Service: The COPS protocol [8] is a simple query and response protocol that can be used to exchange policy information between a policy server (Policy Decision Point or PDP) and its clients (Policy Enforcement Points or PEPs).

Application Function: The Application Function (AF) is an element offering applications that require the control of IP bearer resources. The AF is capable of communicating with the PDF to transfer dynamic QoS-related application information. One example of an AF is the P-CSCF of the IM CN subsystem.

AF session: An AF session is established by an application level signaling protocol offered by the AF that requires a session set-up with explicit session description before the use of the service. One example of an AF session is an IMS session.

AF session signalling: AF session signalling is used to control the AF session. One example of AF session signalling is SIP/SDP.

3.2 Abbreviations

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

AF	Application Function
APN	—Access Point Name (*)
COPS	Common Open Policy Service protocol
DiffServ	Differentiated Services
DSCP	Diffserv Code Point
GERAN	GSM/EDGE Radio Access Network (*)
GGSN	Gateway GPRS Support Node (*)
HTTP	Hypertext Transfer Protocol (*)
IMS	—IP Multimedia Subsystem
IntServ	Integrated Services
LAN	—Local Area Network
LDP	—Label Distribution Protocol
MPLS	Multiprotocol Label Switching Architecture
PDF	—Policy Decision Function
PEP	—Policy Enforcement Point
PHB	—Per Hop Behavior
RNC	—Radio Network Controller (*)
SDP	—Session Description Protocol
SIP	—Session Initiation Protocol (*)
SNMP	Simple Network Management Protocol (*)
TFT	—Traffic Flow Template (*)

* this abbreviation is covered in 21.905v 4.2.0

********** Next change **********

5 End-to-End QoS Architecture

5.1 QoS Management Functions in the Network

To provide IP QoS end-to-end, it is necessary to manage the QoS within each domain. An IP BS Manager is used to control the external IP bearer service. Due to the different techniques used within the IP network, this communicates to the UMTS BS manager through the Translation function.

At PDP context setup the user shall have access to one of the following alternatives:

- Basic GPRS IP connectivity service: The bearer is established according to the user's subscription, local operator's IP bearer resource based policy, local operator's admission control function and GPRS roaming agreements. In this case, IP bearer resource based local policy decisions may be applied to the bearer.

- Enhanced GPRS based services: The bearer is used to support an enhanced application-layer service, such as IM. In this case, service-based local policy decisions (e.g., authorization and policy based control) are also applied to the bearer.

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. The IP policy architecture does not mandate the policy decision point to be external to the GGSN.

Whenever 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. Interworking may be realised in a number of ways, including:

- signalling along the flow path (e.g. RSVP, LDP).
- packet marking or labelling along the flow path (e.g. DiffServ, MPLS)
- interaction between Policy Control and/or Resource Management elements.
- Service Level Agreements enforced by the border routers between networks.

For the policy control the following should apply:

- The IP policy framework employed in UMTS should, as far as possible, conform to IETF "Internet Standards". The IETF policy framework may be used for policy decision, authorization, and control of the IP level functionality, at both user and network level.
- There should be separation between the scope and roles of the UMTS policy mechanisms and the IP policy framework. This is to facilitate separate evolution of these functions.

5.1.1 Description of functions

5.1.1.1 QoS management functions for end-to-end IP QoS in UMTS Network

NOTE: The end-to-end QoS management functions do not cover the cases of a circuit switched service, or an IP service interworking with an ATM service at the gateway node.

IP BS Manager uses standard IP mechanisms to manage the IP bearer services. These mechanisms may be different from mechanisms used within the UMTS, and may have different parameters controlling the service. When implemented, the IP BS Manager may include the support of DiffServ Edge Function and the RSVP function. The **Translation/mapping function** provides the inter-working between the mechanisms and parameters used within the UMTS bearer service and those used within the IP bearer service, and interacts with the IP BS Manager. In the GGSN, the IP QoS parameters are mapped into UMTS QoS parameters, where needed. In the UE, the QoS requirements determined from the application layer (e.g., SDP) are mapped to either the PDP context parameters or IP layer parameters (e.g., RSVP).

If an IP BS Manager exists both in the UE and the Gateway node, it is possible that these IP BS Managers communicate directly with each other by using relevant signalling protocols.

The required options in the table define the minimum functionality that shall be supported by the equipment in order to allow multiple network operators to provide interworking between their networks for end-to-end QoS. Use of the optional functions listed below, other mechanisms which are not listed (e.g. over-provisioning), or combinations of these mechanisms are not precluded from use between operators.

The IP BS Managers in the UE and GGSN provide the set of capabilities for the IP bearer level as shown in Table 1. Provision of the IP BS Manager is optional in the UE, and required in the GGSN.

Table 1: IP BS Manager capability in the UE and GGSN

Capability	UE	GGSN
DiffServ Edge Function	Optional	Required
RSVP/IntServ	Optional	Optional
IP Policy Enforcement Point	Optional	Required (*)

(*)Although the capability of IP policy enforcement is required within the GGSN, the control of IP policy through the GGSN is a network operator choice.

Figure 2 shows the scenario for control of an IP service using IP BS Managers in both possible locations in the UE and Gateway node. The figure also indicates the optional communication path between the IP BS Managers in the UE and the Gateway node.

Policy Decision Function (PDF) is a logical policy decision element which uses standard IP mechanisms to implement Service Based Local Policy (SBLP) in the IP bearer layer. –These mechanisms may be conformant to, for example, the framework defined in IETF [RFC2753] "A Framework for Policy-based Admission Control" where the PDF is effectively a Policy Decision Point (PDP). –The PDF makes decisions in regard to SBLP using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP).

~~The Policy Decision Function (PDF) is a logical entity of the P-CSCF. If the PDF is implemented in a separate physical node, t~~The interface between the PDF and ~~P-CSCF~~ the Application Function (AF) is ~~not standardized~~ the Gq interface specified in 3GPP TS 23.002 [2].

The interface between the PDF and GGSN is specified within 3GPP, named Go interface, and is included in the Reference Architecture depicted in TS23.002. –The ~~protocol~~ interface between the PDF and GGSN supports the transfer of information and policy decisions between the policy decision point and the IP BS Manager in the GGSN.

The PDF makes policy decisions based on information obtained from the ~~P-CSCF~~AF. The PDF maps the policy set-up information received from the AF via the Gq interface ~~In the P-CSCF(PDF), the application level parameters (e.g., SDP) are mapped~~ into IP QoS parameters. –The ~~P-CSCF(~~PDF~~)~~ is in the same domain as the GGSN. The AF may either be in the same domain as the PDF or may be in a different domain than the PDF.

NOTE: Currently in IETF, inter-domain policy interactions are not defined.

Application Function (AF) offers services that require the control of IP bearer resources. The AF maps QoS-related application level parameters (e.g. SDP) into policy set-up information, and sends this information to the PDF via the Gq interface.

********** Next change **********

5.1.2 Allocation of QoS management functions

5.1.2.1 QoS management functions for end-to-end IP QoS

The QoS management functions for controlling the external IP bearer services and how they relate to the UMTS bearer service QoS management functions are shown in Figure 2.

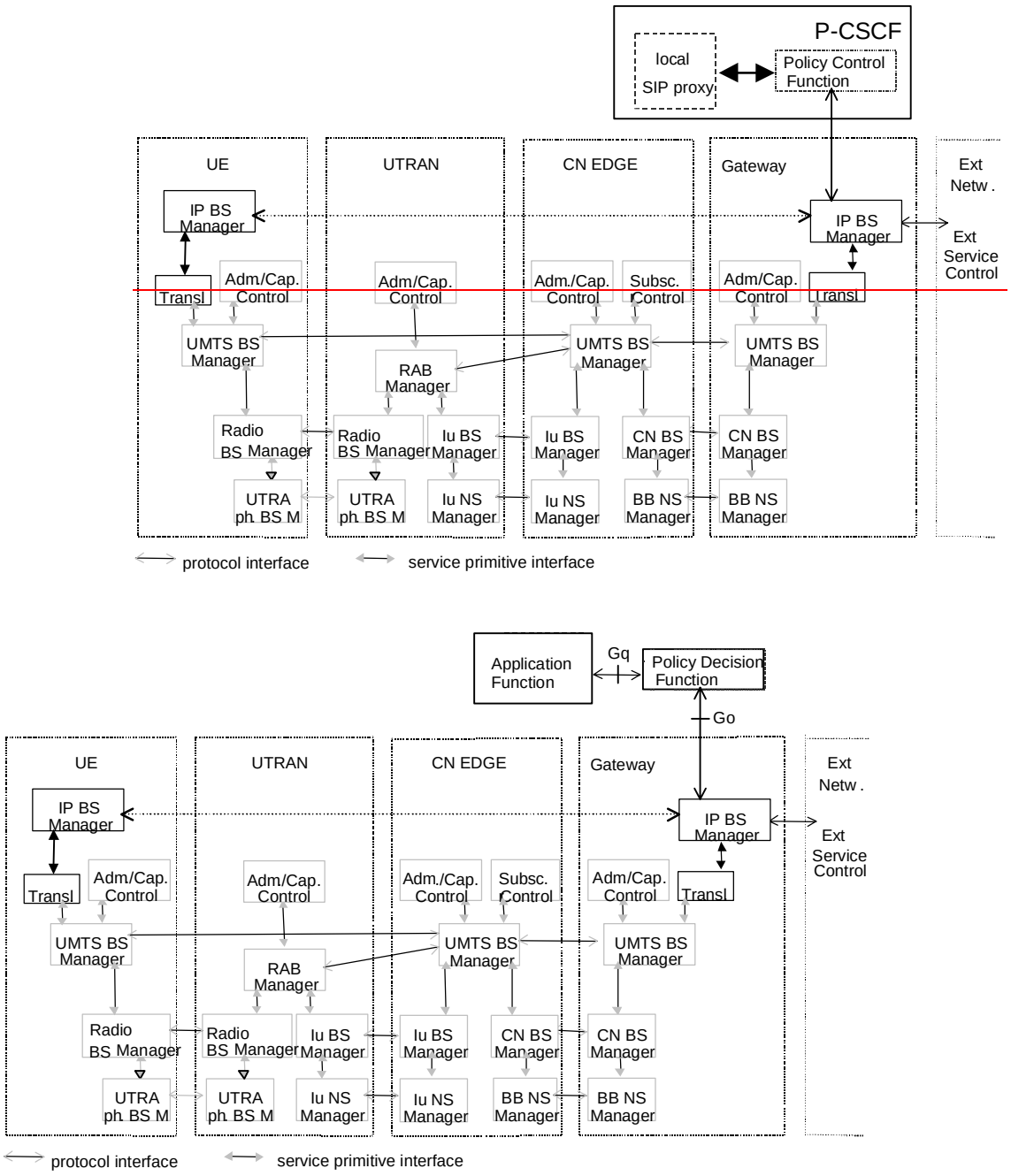

Figure 2: QoS management functions for UMTS bearer service in the control plane and QoS management functions for end-to-end IP QoS

NOTE: The dimmed boxes in Figure 2 are clarified in TS23.107.

~~NOTE: The following will be revisited in the Release 6 timeframe: - the possible reuse of the protocols in the Go interface between the GGSN and other application servers, and possible interfaces between the PDF and the P-CSCF, and between the PDF and other application servers.~~

Note: The UE is only shown as a combined element, but it may also consist of a split TE/MT. Standardization of the interface and operation within a split UE is outside the scope of this TS.

5.2 Capabilities of Functional Elements

This section provides functional descriptions of capabilities in GGSN, UE, ~~and P-CSCF~~(PDF~~)~~, and AF.

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.

The **Service-based Local Policy Enforcement Point** controls the quality of service that is provided to a combined set of IP flows. —The policy enforcement function includes policy-based admission control that is applied to the bearer associated with the flows, and configuration of the 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 the set of IP flows. The authorized resources are expressed as a maximum authorised bandwidth and QoS class. 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 PCDF 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 control and 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). —When a gate is open, the packets in a flow are accepted, and are thus subject to the Diffserv edge treatment. –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.

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..

5.2.2 UE

This clause provides functional descriptions of capabilities in UE. 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.

DiffServ Edge Function acts as a DiffServ (DS) boundary for the traffic from applications running on the UE. As specified in RFC2475, DS boundary node must be able to apply the appropriate PHB to packets based on the DS code point. In addition, DS boundary nodes may be required to perform traffic conditioning functions. When GGSN DiffServ marking is used, the DiffServ edge function in the UE is not needed.

RSVP/Intserv Function provides the capability for the UE to request end-to-end QoS using RSVP messages as defined in IETF standards. RSVP messages may also be used by the network to inform the DSCP to be used by the UE. ~~–~~RSVP messages shall include the authorization token and flow identifier(s) in a policy data object if the authorization token is available in the UE. RSVP may be used to trigger PDP context activation/modification. ~~–~~The inter-working between MT and TE is FFS.

Binding Mechanism associates the PDP context bearer to the IP flow(s) to support SBLP policy enforcement in the GGSN. The binding information containing the authorization token and flow identifier(s) provides the binding mechanism, and is included by the UE in the PDP Context Activation and Modification messages. The authorization token may also be used to bind a RSVP session with a SIP session by including the authorization token and flow identifier(s) in RSVP messages. The AF provides the authorization token to the UE during AF session set-up. E.g. ~~F~~for IMS services, the authorization token is provided to the UE by the P-CSCF during SIP session establishment.

~~The manner in which QoS preconditions for a SIP session shall be met are as stated in TS 23.228. The functionality shall be compliant to the IETF specification on Integration of Resource Management and SIP.~~

For each bi-directional media flow, the UE shall ensure that the 64 bit IPv6 address prefix of the source address of outgoing packets is the same as the prefix of the destination address supplied for incoming packets.

5.2.3 ~~P-CSCF(~~PDF~~)~~

This clause provides functional ~~–~~descriptions of capabilities in ~~P-CSCF(~~PDF~~)~~. ~~Determination of exactly which functions are required to support interoperator and multi-vendor aspects are not addressed in this clause.~~The PDF makes policy decisions based on policy set-up information obtained from the AF via the Gq interface.

Editor's note: Once the functional split between the AF and the PDF is further clarified, the P-CSCF(PDF) related text shall be accordingly revised, and the AF-related text is to be moved to section 5.2.4.

Service-based Local Policy Decision Point

- Authorize QoS resources (bandwidth, etc.) for the AF session. The ~~P-CSCF (PCF)~~PDF shall use the policy set-up information received from the AF ~~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 flows and restrictions on individual IP flows (eg. destination address and port).

- For bi-directional media flows~~-~~, the P-CSCF(PDF), 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(PDF) assumption would be determined by operator policy in order to reduce the possibilites of bearer misuse. In the filters supplied by the PDF 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 (PDF) shall be able to enforce the behaviour of the UE ~~in~~ with 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~~P-CSCF using the indications described in Section~~s 4.2.5.1~~E.2.2.1 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/PDF shall take care that such a PDP context would be rejected by the GGSN. To do so, the P-CSCF/PDF uses the Go interface.

- The P-CSCF (PDF) 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 PDF functions as a Policy Decision Point for the service-based local policy control.

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

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

- At ~~IP multimedia~~ AF session release, the PDF shall revoke the QoS resource authorization for the AF session.

Binding Mechanism Handling

- ~~—~~The PDF generates an authorization token for each ~~SIP~~AF session on request from the AF.~~and the P-CSCF sends the authorization token to the UE in SIP signalling.~~ The authorization token includes a fully qualified domain name of the PDF. ~~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.

5.2.4 Application Function (AF)

The Application Function (AF) is an element offering applications that require the control of IP bearer resources (e.g. UMTS PS domain/GPRS domain resources). One example of an Application Function is the P-CSCF.

Service Based Local Policy related functions

- The AF shall use Gq interface to exchange service based policy set-up information with the PDF.

- The AF shall indicate to the PDF whether or not the PDF should contact the AF at UE resource reservation.

Binding Mechanism Handling

- The AF requests authorization token(s) from the PDF. The following are possible:

    1. The PDF authorizes QoS resources usage for that application for a particular session and user. The authorization token is only valid for the duration of the session for the specific user.
    2. The AF requests multiple authorization tokens. The PDF provides the requested number of authorization tokens. Each of these tokens may later be allocated to a session, and then used for subsequent QoS resource usage authorization procedures for the duration of the session for the specific user.

- The AF sends the authorization token to the UE in AF session signaling.

5.3 Go interface (PDF – GGSN)

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~~Decision Function (PDF). ~~—~~The Go interface provides information to support the following functions in the GGSN:

- 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~~Decision Function (PDF). ~~–~~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 PDF 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 PDF.

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 PDF. ~~—~~The information elements specific to UMTS would be standardized and carried in the 3GPP Go specific interactions between the PDF and the GGSN.

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

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

- Charging information (ICID in case of IMS)

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 flows. 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 packets matching the packet classifier. The packet handling action (gate status) shall result in packets being passed (gate open), or silently discarded (gate closed).

Charging information (ICID) allows the GGSN to be aware of the IMS session level charging identifier of the IMS session that the Install command relates to. The PDF shall send the ICID provided by the P-CSCF as part of the authorisation (Install) decision.

The Report State contains the following information:

- Charging correlation information

Charging correlation information contains information used to correlate usage records (e.g. CDRs) of the GGSN with ~~IMS~~AF session records from the ~~P-CSCF~~AF. For this purpose, the GGSN shall send the GCID of the PDP context and the GGSN address to the PDF 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).

5.3a Gq Interface (PDF - AF)

5.3a.1 Gq Functional Requirements

The Gq interface is used for service-based policy set-up information exchange between the Policy Decision Function (PDF) and the Application Function (AF). This information is used by the PDF for service based local policy decisions.

The Gq interface allows service based QoS information needed for QoS authorisation to be exchanged between the AF and the PDF.

One PDF shall be able to serve more than one Application Function and one given AF may interact with a number of PDFs. On a per-AF-session basis, the AF shall interact with only a single PDF.

5.3a.2 Information Exchanged via Gq interface

Editor's note: The details of the Gq commands are for further study

********** Next change **********

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 level information to configure the DiffServ edge 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 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 that are subject to service based local policy by sending an authorization request to the PDCF. Alternatively, the GGSN may authorize PDP context activation/modification 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.

6.1.2 Procedures in the UE

The QoS procedures in the UE are triggered by the application layer (e.g., SIP/SDP) QoS requirements. The exact QoS procedures in the UE depend on the UE QoS capabilities.

For UEs that support only UMTS QoS mechanism, the application QoS requirements will trigger a PDP Context Activation procedure with the corresponding UMTS QoS parameters.

For UEs that support both IP (e.g., IP BS Manager) and UMTS QoS mechanism, the application QoS requirements are mapped down to the IP layer QoS parameters. The IP layer parameters are further mapped down to the PDP context parameters in the UE.

For UEs that support RSVP, the application QoS requirements are mapped down to create an RSVP session. The UE shall establish a PDP context suitable for support of the RSVP session. In addition in the case of IMS, the following procedures apply: if the UE received the Media Authorization Token in the SIP signalling, the UE shall include the Media Authorization Token in the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the IMS session.

For UEs that support RSVP, if the UE received the Media Authorization Token in ~~SIP~~AF session signalling, the UE shall include the Media Authorization Token in both the PDP Context Activation request for the PDP Context(s) that are activated to carry the media flows of the ~~IMS~~ AF session, and the RSVP messages if the PDP Context/RSVP is associated to the session.

At the ~~IMS~~AF session release, the UE shall release all QoS resources allocated for the ~~IMS~~ AF session.

NOTE: Service Based Local Policy may restrict the destination of packets to the addresses/ports included in the ~~SIP~~AF session signalling ~~(SDP)~~. Mechanisms such as MIPv6 Route Optimisation which send packets to other addresses/ports may therefore not operate correctly.

6.1.3 Procedures in the ~~P-CSCF(~~PDF~~)~~

Editor's note: There is still some IMS-specific text contained in this clause, this will have to be revised and generalized later on.

In case of ~~IMS with~~applying ~~-~~ Service based local policy:

The QoS procedures in ~~P-CSCF(~~PDF~~)~~ are related to service based local policy control.

The authorize QoS resources procedure can be invoked between PDF and AF at AF session establishment and/or at bearer establishment. When the AF requests the token from the PDF, it indicates whether or not the PDF should contact the AF at UE resource reservation. ~~is triggered by the P-CSCF receiving a SIP message containing SDP information. The SDP contains sufficient information about the session, such as the end-points, bandwidth requirements and the characteristics of the media exchange. The P-CSCF initiates a policy setup in PDF for the IMS session~~. The PDF shall authorize the required QoS resources and install the IP bearer level policy for the ~~IMS~~AF session.

The PDF provides the policy decision based on the information received from the AF.

The Authorization-Token is generated by the PDF and sent to the ~~UE by the P-CSCF~~AF. ~~For the originating UE, the Authorization-Token shall be included in the first available reliable SIP message (e.g. 183 Session Progress)) from P-CSCF to the UE. For the terminating UE, the Authorization-Token shall be included in the SIP Invite message from P-CSCF to the UE.~~

~~The P-CSCF also generates and forwards an indication to the UE to assist the UE in deciding whether it can assign multiple media components to the same PDP Context, or separate PDP Contexts have to be used. This mechanism is described in Section 4.2.5.1 in [4].~~

Upon receiving the bearer authorization request from the GGSN, the PDF shall authorize the request according to the stored SBLP for the session.

The PDF makes a final decision to enable the allocated QoS resource for the authorized IP flows. This may be triggered by ~~the receipt of the SIP 200 OK (Invite Response) message to the P-CSCF~~an instruction from the AF. QoS resources may also be enabled at the time they are authorised by the PDF.

During the mid-call SIP signaling for media or codec change, the PDF shall be able to decide if new QoS authorization is needed. 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 flow changed.

At IMS session release, the PDF shall revoke the resource authorization.

6.1.4 Procedures in the AF

Editor's note: The details are for further study.

6.2 IP Bearer Level / Application Level Binding Mechanism

The *binding mechanism* associates the PDP context bearer with policy information in the GGSN to support service based local policy enforcement. The SBLP policy decision information in the GGSN is based on IP media flows. ~~–~~The binding mechanism identifies the IP media flow(s) associated with a PDP context bearer and uses this information in selecting the policy information to apply.

The UE shall be able to include binding information in PDP Context Activation and Modification messages to associate the PDP context bearer with policy information . The binding information includes 1) an Authorization Token sent by the ~~P-CSCF~~AF to the UE during ~~SIP~~AF session signaling, and 2) one or more Flow Identifiers which are used by the UE, GGSN and PDF to uniquely identify the IP media flow(s). It is assumed that only one binding information is carried within PDP context Activation/Modification messages in this Release.

The authorization token shall be unique within the scope of the operator's domain. The ~~A~~authorization ~~T~~token conforms to relevant IETF standards.

A Flow Identifier identifies an IP media flow associated with the SIP session. Flow Identifiers are based on the sequence of media components (media description structure defined by a single 'm=' line) in the SDP, and IP flow numbers (defined in the order of increasing port numbers) within each media component.

A ~~F~~flow ~~I~~identifier combined with the ~~A~~authorization ~~T~~token shall be sufficient to uniquely identify an IP media flow.

In order to allow SBLP policy information to be "pulled" from the PDF, the authorization token shall allow the GGSN to determine the address of the PDF to be used.

< End of all changes >