Prototyping of an Interconnection Border Gateway Function (IBGF) in Next Generation Networks (NGN) Using Open Source Software Tools

Stephan Massner and Michael Maruschke

Institute of Telecommunication and Information Technology
Hochschule für Telekommunikation Leipzig (HfTL) Gustav-Freytag Str. 43-45,
Leipzig, 04277, Germany
Phone: +49 (0) 341 3062-238; Fax: +49 (0) 341 3062-245
{massner,maruschke}@hftl.de

Abstract. This paper illustrates both the detailed theoretical setup of the Interconnection Border Gateway Function (IBGF) and its technical implementation using Open Source Software components. Moreover, a model is proposed to handle different traffic classes according to their corresponding Quality of Service (QoS) requirements while also forwarding "best effort" data traffic. The functionality is verified by evaluating data streams with varying QoS parameters, which are identified by an adequate packet marking method.

Keywords: Next Generation Network (NGN), Interconnection Border Gateway Function (IBGF), IP-Multimedia Network, Resource and Admission Control Subsystem (RACS), IP-Multimedia Subsystem (IMS), Quality of Service (QoS).

1 Introduction

In Next Generation Networks (NGNs), IBGFs are used to connect IP-Multimedia Subsystem (IMS) networks and IP Multimedia networks on the transport layer, utilizing transport functionality at network borders. Its tasks are specified in standards by the European Telecommunications Standards Institute - Telecoms & Internet converged Services & Protocols for Advanced Network (ETSI-TISPAN) [1][2][3]. These may vary in descriptions by the 3rd Generation Partnership Project (3GPP). The IBGF has a horizontal interface (Ds) to the transport layer below the IMS network, and another to the transport layer of other IP-Multimedia networks (Iz). Between both transport layers the IBGF manages media streams to meet given QoS parameters of forwarded data. Utilizing the vertical interface (Ia), the IBGF is managed by transport control functionalities, like the Service Policy Decision Function (SPDF) located in the Resource and Admission Control Subsystem (RACS).

T. Magedanz et al. (Eds.): TridentCom 2010, LNICST 46, pp. 739–752, 2011.

2 General IBGF Description

2.1 IBGF Tasks

The standardized[3] tasks an IBGF fulfills are:

- opening/closing gates
- allocating/translating IP addresses/port numbers
- IPv4/IPv6 interworking
- hosted NAT traversal
- packet marking
- resource allocation/bandwidth reservation
- policing
- QoS/usage metering
- transcoding
- detection of inactive bearer connections
- specific call-independent procedures
- BGF overload control

With its functionality, the IBGF represents a domain with integrated service classes, due to the fact that QoS resources have to be provided for transmitted data streams (See Figure 1). The control of these QoS resources is managed by functionalities on the Transport Control Sublayer, in this case the SPDF[1]. It sends information to the IBGF about the allocation of QoS resources, data stream handling (classification, Topology Hiding, marking, policies,...), and rules about traffic classes. The IBGF on the other hand informs the SPDF about currently used, reserved, and free resources (QoS/usage), based on individual or bundled streams. Furthermore, it provides information about currently configured as well as policies used.

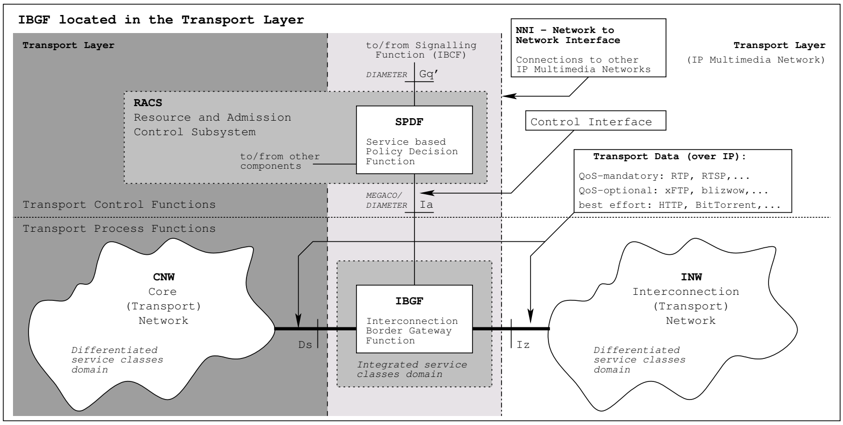
IBGF located in the Transport Layer
Transport Layer
to/from Signalling Function (IBCF)
DIAMETER
Gq'
NNI - Network to Network Interface
Connections to other IP Multimedia Networks
Transport Layer
(IP Multimedia Network)
RACS
Resource and Admission Control Subsystem
SPDF
Service based Policy Decision Function
to/from other components
Control Interface
Transport Data (over IP):
QoS-mandatory: RTP, RTSP,...
QoS-optional: xFTP, blizwow,...
best effort: HTTP, BitTorrent,...
MEGACO/ DIAMETER
Ia
Transport Control Functions
Transport Process Functions
CNW
Core (Transport) Network
Differentiated service classes domain
Ds
IBGF
Interconnection Border Gateway Function
Integrated service classes domain
Iz
INW
Interconnection (Transport) Network
Differentiated service classes domain

Fig. 1. IBGF located in the Transport Layer

The IBGF is located between domains with differentiated service classes, because it handles data streams according to their classification, identified by their individual marking. The latter is also edited by the IBGF according to guidelines.

2.2 IBGF Interfaces

Vertical Interface to the Transport Control Sublayer (Ia). The connection to the RACS[2] can basically be divided into two different types. In the first case, a direct connection can exist between the SPDF and the IBGF[4]. In the second case, multiple SPDFs and IBGFs can communicate with each other. The latter requires a reporting framework as specified in ETSI TR 182 022[5].
If a point to point connection exists between the SPDF and the Transport Control Sublayer (first case), information to be exchanged can generally be categorized into:

- Policy Push, Audit Request (SPDF to IBGF) and
- Usage Metering, QoS-Reporting (IBGF to SPDF)

However, in the second case, this data transfer is realized by introducing a sublayer and thus changing the topology. A functional division into Reporting Source, Reporting Collector, and Reporting Sink is necessary, as illustrated in Figure 2. Thereby, entities appear both as transport sources and sinks in the Transport Control Sublayer and Transport Process Sublayer, depending on the flow of information. The entity inside the sublayer acts as a reporting controller, which aggregates, filters, and delivers received data to the destination. Moreover, it can introduce modifications, if this meets the destination's requirements.

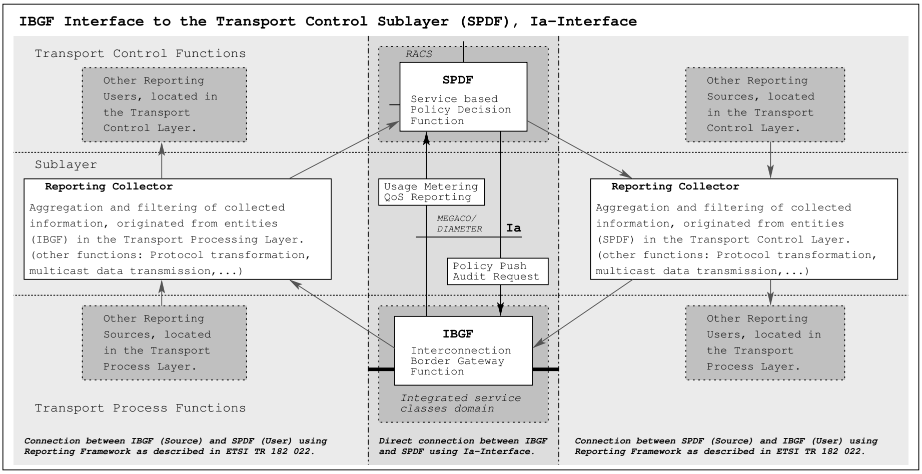
IBGF Interface to the Transport Control Sublayer (SPDF), Ia-Interface
Transport Control Functions
Other Reporting Users, located in the Transport Control Layer.
RACS
SPDF
Service based Policy Decision Function
Other Reporting Sources, located in the Transport Control Layer.
Sublayer
Reporting Collector
Aggregation and filtering of collected information, originated from entities (IBGF) in the Transport Processing Layer. (other functions: Protocol transformation, multicast data transmission,...)
Usage Metering QoS Reporting
MEGACO/ DIAMETER
Ia
Policy Push Audit Request
Reporting Collector
Aggregation and filtering of collected information, originated from entities (SPDF) in the Transport Control Layer. (other functions: Protocol transformation, multicast data transmission,...)
Other Reporting Sources, located in the Transport Process Layer.
IBGF
Interconnection Border Gateway Function
Integrated service classes domain
Other Reporting Users, located in the Transport Process Layer.
Transport Process Functions
Connection between IBGF (Source) and SPDF (User) using Reporting Framework as described in ETSI TR 182 022.
Direct connection between IBGF and SPDF using Ia-Interface.
Connection between SPDF (Source) and IBGF (User) using Reporting Framework as described in ETSI TR 182 022.

Fig. 2. Ia-Interface

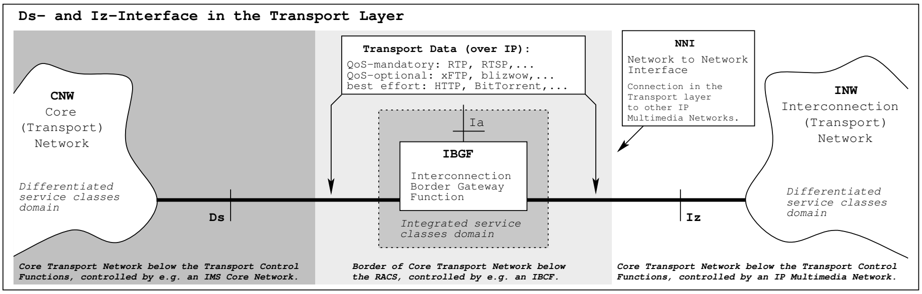
Ds- and Iz-Interface in the Transport Layer
Transport Data (over IP):
QoS-mandatory: RTP, RTSP,...
QoS-optional: xFTP, blizwow,...
best effort: HTTP, BitTorrent,...
NNI
Network to Network Interface
Connection in the Transport layer to other IP Multimedia Networks.
CNW
Core (Transport) Network
Differentiated service classes domain
Ia
IBGF
Interconnection Border Gateway Function
Integrated service classes domain
INW
Interconnection (Transport) Network
Differentiated service classes domain
Ds
Iz
Core Transport Network below the Transport Control Functions, controlled by e.g. an IMS Core Network.
Border of Core Transport Network below the RACS, controlled by e.g. an IBCF.
Core Transport Network below the Transport Control Functions, controlled by an IP Multimedia Network.

Fig. 3. Ds- and Iz-Interface

Horizontal Interface to the Transport Process Sublayer (Ds and Iz). Both interfaces terminate traffic from IPv4 and/or IPv6 networks (See Figure 3). Here, data streams from different traffic classes are received and sent. Upon receiving, data packets are sorted into traffic classes, which are distinguished by QoS characteristics (roughly: QoS, non-QoS). Packets, for example, can be classified in the following way:

- non-QoS: "best effort" - e.g.: Hypertext Transfer Protocol (HTTP), BitTorrent, ...
- QoS: "QoS-mandatory" - e.g.: Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), ...
- "QoS-optional" - e.g.: x File Transfer Protocol (xFTP), blizwow, ...

QoS characteristics for classifications can be structured into single criteria (parameters) like jitter, delay, bandwidth, packet loss or any combination of the above. Moreover, a dynamic division of different classes into subclasses is performed, depending on respective parameter values as deciding criteria. Therefore it is possible to allocate resources dynamically, which affect a respective stream dedicated to a QoS class. Policing is applied depending on each QoS class and is not further divided into subclasses (e.g.: Stochastic Fairness Queuing (SFQ), Class Based Queuing (CBQ) with / without Token Bucket Filter (TBF), etc.). QoS marking is also executed according to corresponding QoS classes, which is identical for respective subclasses.

2.3 Detailed Description of IBGF Function Blocks

The IBGF functional blocks (see Figure 4) are divided into:

① **IPv4/IPv6 termination** of the inbound data stream, including the termination of layers 1-3.

② **Gate** for the inbound stream and its examination according to **filter** criteria like origin (source address : source port) and destination (inbound interface; destination address : destination port). For "best effort" data streams, dedicated port ranges can be reserved (e.g. HTTP) which are not managed

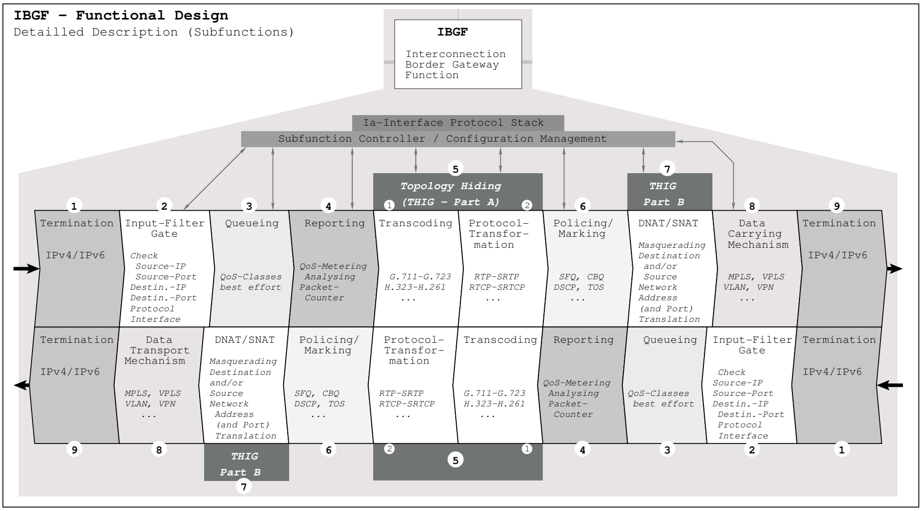
IBGF - Functional Design
Detailled Description (Subfunctions)
IBGF
Interconnection Border Gateway Function
Ia-Interface Protocol Stack
Subfunction Controller / Configuration Management
Topology Hiding (THIG - Part A)
THIG Part B
1 Termination IPv4/IPv6
2 Input-Filter Gate Check Source-IP Source-Port Destin.-IP Destin.-Port Protocol Interface
3 Queueing QoS-Classes best effort
4 Reporting QoS-Metering Analysing Packet-Counter
5 Transcoding G.711-G.723 H.323-H.261 ...
Protocol-Transformation RTP-SRTP RTCP-SRTCP ...
6 Policing/Marking SFQ, CBQ DSCP, TOS ...
7 DNAT/SNAT Masquerading Destination and/or Source Network Address (and Port) Translation
8 Data Carrying Mechanism MPLS, VPLS VLAN, VPN ...
9 Termination IPv4/IPv6
Data Transport Mechanism MPLS, VPLS VLAN, VPN ...

Fig. 4. IBGF - Functional Design

separately by the Transport Control Sublayer, but instead follow common rules. Thus, ”best effort” traffic is treated with network neutrality principles. Both the process of blocking and releasing the corresponding gate is subject to policy guidelines (bandwidth limitation etc.) set by the SPDF.

③ **Queueing**, i.e. classification of inbound data streams into corresponding QoS classes and their respective subclasses according to QoS requirements.

④ **Reporting and measurement** of current QoS values, including jitter, packet loss, used bandwidth, current delay, packet counting (data volume) for accounting purposes, and determining the current duration of an existing connection. Moreover, measurement results and connection information can be divided into general and QoS connection data.

⑤ **Topology Hiding** (part A) includes both **transcoding** (5.1) and **protocol transformation** (5.2). For optional transcoding, the IBGF acts as a media gateway, whereas it translates e.g. the media codec G.711 to G.723, or H.323 to H.261. Optional protocol transformations include the conversion from RTP to Secure Real-Time Transport Protocol (SRTP) or Real-Time Transport Control Protocol (RTCP) to Secure Real-Time Transport Control Protocol (SRTCP).

⑥ **Policing and marking** is applied by the IBGF by first reading all queues of the corresponding QoS classes and subclasses with their respective adjusted algorithms. These different algorithms can be applied in a parallel and/or serial, as well as interdependent and/or independent fashion. Markings applied to fields like the Differentiated Service Code Point (DSCP)[6], the Type of Service (TOS)[7] etc. depend on their corresponding classes.

⑦ **Topology Hiding** (part B) covers procedures for Destination Network Address (and Port) Translation (DNA(P)T) and/or Source Network Address (and Port) Translation (SNA(P)T), to hide data stream origins and set the next route as the destination accordingly.

⑧ **Data carrying mechanism** describes the grouping of similar streams, for example with similar destinations and QoS parameters, into data stream bundles. These can then be transmitted through Multi Protocol Label Switching (MPLS), Virtual LAN (VLAN), Virtual Private Network (VPN) or with Virtual Private LAN Service (VPLS).

⑨ **IPv4/IPv6 termination** of the outgoing data stream, including layer 1-3 termination.

3 Prototyping and Implementation

The IBGF implementation (see Figure 5) covers the following function blocks:

❶ The position of interfaces, whether considering the Ds- or Iz-interface, is irrelevant to this case. Here, the IPv4/IPv6 termination is applied to an inbound unidirectional data stream of any arbitrary session, consisting of a RTP and RTCP data stream.

❷ Thereafter, individual data packets are checked by examining the origin (source IP : source port), destination (destination IP: destination port), receiving interface, and the protocol used. In case the determined data matches the filter rules, the specified data packet is allowed to pass the gate. This is realized by utilizing the netfilter framework[8].

❸ For further processing, data packets are sorted into their corresponding QoS classes. In this case, a higher prioritized class (Subclass A2) is used for the RTCP data stream and a lower prioritized class (Subclass n1) is used for the RTP stream. The RTCP stream's packet loss should be close to "0" at the expense of the RTP data stream. This was realized by using functionalities already integrated inside the Linux Kernel.

❹ The measurement of bitrate, delay, jitter, and packet loss of both data streams is executed separately and independently for each subclass utilizing functionalities from the netfilter framework. If a substantial bitrate exceedance is detected, by overstepping a predetermined bitrate level, foremost the RTP data stream will be limited.

❺ Topology Hiding (Part A) is implemented separately. For this purpose, the RTP data stream is transcoded first (part 5.1), by converting the media codec type from G.711 to G.723. This requires the termination of the received RTCP data stream and subsequent generation of a new RTP data stream (outgoing termination). Moreover, the RTCP data stream has to be modified. The protocol transformation of the RTP and RTCP which follows (part 5.2) includes embedding in Secure Shell (SSH).

❻ Policy enforcement for data streams of different traffic classes is carried out with different algorithms, which are adjusted to their corresponding QoS. The subclass of a certain traffic class and the "best effort" class are treated with SFQ. Traffic classes amongst each other are processed by CBQ, whereas

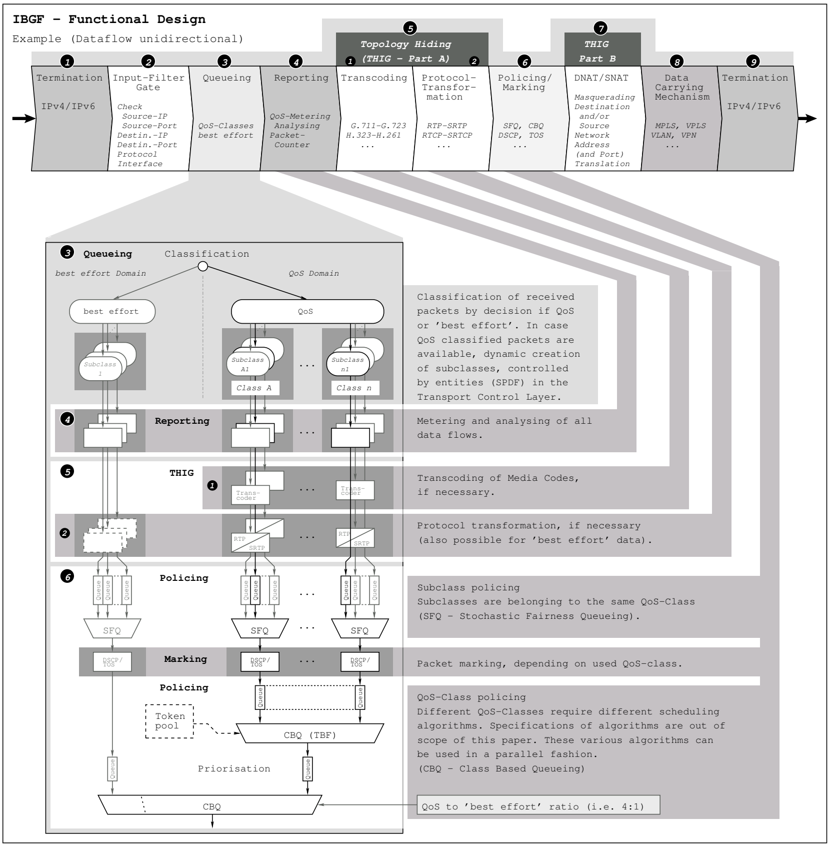
IBGF - Functional Design
Example (Dataflow unidirectional)
5
Topology Hiding
(THIG - Part A)
7
THIG
Part B
1 Termination
IPv4/IPv6
2 Input-Filter Gate
Check
Source-IP
Source-Port
Destin.-IP
Destin.-Port
Protocol
Interface
3 Queueing
QoS-Classes
best effort
4 Reporting
QoS-Metering
Analysing
Packet-Counter
1 Transcoding
G.711-G.723
H.323-H.261
...
2 Protocol-Transformation
RTP-SRTP
RTCP-SRTCP
...
6 Policing/Marking
SFQ, CBQ
DSCP, TOS
...
DNAT/SNAT
Masquerading
Destination
and/or
Source
Network
Address
(and Port)
Translation
8 Data Carrying Mechanism
MPLS, VPLS
VLAN, VPN
...
9 Termination
IPv4/IPv6
3 Queueing
Classification
best effort Domain
QoS Domain
best effort
QoS
Subclass 1
Subclass A1
Subclass n1
Class A
Class n
Classification of received packets by decision if QoS or 'best effort'. In case QoS classified packets are available, dynamic creation of subclasses, controlled by entities (SPDF) in the Transport Control Layer.
4 Reporting
Metering and analysing of all data flows.
5 THIG
1
Trans-coder
Transcoding of Media Codes, if necessary.
2
RTP
SRTP
Protocol transformation, if necessary (also possible for 'best effort' data).
6 Policing
Queue
SFQ
Subclass policing
Subclasses are belonging to the same QoS-Class (SFQ - Stochastic Fairness Queueing).
Marking
DSCP/TOS
Packet marking, depending on used QoS-class.
Policing
Token pool
CBQ (TBF)
QoS-Class policing
Different QoS-Classes require different scheduling algorithms. Specifications of algorithms are out of scope of this paper. These various algorithms can be used in a parallel fashion.
(CBQ - Class Based Queueing)
Priorisation
CBQ
QoS to 'best effort' ratio (i.e. 4:1)

Fig. 5. IBGF - Functional Design Example

a TBF is implemented for quantity management of outgoing QoS data traffic. A final utilization of CBQ considers the division of 20% of all resources for 'best effort', and 80% for QoS data. The marking of data streams of a traffic class is accomplished after combining subclasses by manipulating the Differentiated Service (DS) and TOS fields respectively. Therefore, data packets can be treated according to their QoS in the subsequent differentiated service classes domain. Also, the implementation is carried out with functionalities of the netfilter framework.

❼ At this point, masquerading of both data streams is realized, using the netfilter framework. For this purpose, source and destination descriptions are translated.

❽ In a separate implementation, traffic grouping is carried out for the mutual transport over a MPLS network. To accomplish this, data streams with similar QoS and a common destination are combined.

❾ Finally, the outgoing IPv4/IPv6 termination is executed for the unidirectional data stream.

4 QoS-Measurements

4.1 Standardization

Several parameters have been defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) describing boundaries acceptable by real time media transport in IP networks. Definitions mainly focussed on are:

- **IPPR** IP Packet Rate (proportional to Bandwidth): IPPR (Packet · s-1), specifies the total number of IP packets during a specified time interval divided by the time interval duration[9].
- **IPTD** IP packet Transfer Delay: IPTD (s), specifies the time between two events at time t_1 (ingress event) and t_2 (egress event), where both events corresponds to one IP packet. Two conditions have to be fulfilled, where T_{max} defines the maximum Transfer Delay Time[9]: $(t_2 > t_1)$ and $(t_2 - t_1) \leq T_{max}$.
- **IPDV** IP packet Delay Variation (Jitter): IPDV (s), specifies the variation of the IPTD. Different methods of calculating IPDV are known and described in[9][10][11]. It is irrelevant which method will be choosen, because the range given by absolute values between min. and max. IPTD is independent.
- **IPER** IP packet Error Ratio: IPER (1), specifies the number of total errored IP packets divided by the sum of total successful transfered IP packets and the errored IP packets. Both numbers must refer to the same time interval[9].
- **IPLR** IP packet Loss Ratio: IPLR (1), specifies the number of total lost IP packets divided by the total transmitted IP packets. Both ratios must refer to the same time interval[9] [12].

4.2 Measurement

The measurement of achievable QoS parameter demands on an arrangement in several parts providing a set of functions needed by described measuerement methods (see Figure 6). In the following, all measured QoS parameters of the described prototypical IBGF are named and exemplified:

- IPPR: Throughput using an increasing bitrate and Type of Service (TOS) marked IP packets
- IPTD: Delay between each incoming and outgoing IP packet, using an identifier contained in the payload
- IPDV: Delay variation between each measured delay of incoming and outgoing IP packets
- IPER: Comparision of header and payload of sent and received IP packets including the same content
- IPLR: Counting dropped IP packets by checking if sent unified identicable IP packet was received during the measure time or not

As described in IPPR measurement, an increasing bitrate IP flow was used to test several conditions: underload, limit load and overload. Achieved values have been selected to these operating states and evaluated as limited to underload and limit load condition. These different operating states can be defined as follows:

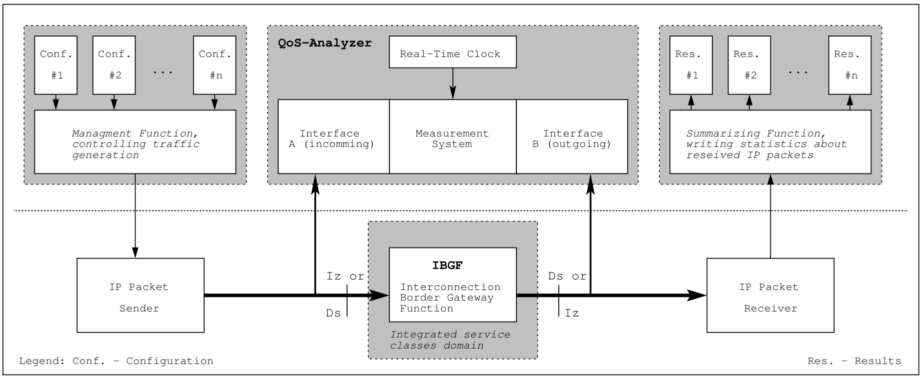
Conf. #1
Conf. #2
...
Conf. #n
Managment Function, controlling traffic generation
QoS-Analyzer
Real-Time Clock
Interface A (incomming)
Measurement System
Interface B (outgoing)
Res. #1
Res. #2
...
Res. #n
Summarizing Function, writing statistics about reseived IP packets
IP Packet Sender
Iz or Ds
IBGF
Interconnection Border Gateway Function
Integrated service classes domain
Ds or Iz
IP Packet Receiver
Legend: Conf. - Configuration
Res. - Results

Fig. 6. IBGF - Test Setup for QoS Measurements

- Underload: Incoming IP traffic (λ) is lower than max. outgoing IP traffic (μ); $\lambda < \mu$
- Limit Load: Incoming IP traffic (λ) is equal to max. outgoing IP traffic (μ); $\lambda = \mu$
- Overload: Incoming IP traffic (λ) is higher than max. outgoing IP traffic (μ); $\lambda > \mu$

Each particular measurement point has been calculated using five measurement points preventing random errors. The results for these five related test series were obtained from similar test executions. Furthermore all tests have been done under the condition that impacts based on processing power, memory, operating system etc. have no bearing on IP packet processing. Based on five specified traffic classes in ITU-T standard a combination into three traffic classes has been done on condition that lower QoS classes are included in next upper QoS class, that means:

- class 0 contains class 0 and class 1 (Upper bound on the mean IPTD delay of class 0 is $100ms$; class 1: $400ms$),
- class 2 contains class 2 and class 3 (Upper bound on the mean IPTD delay of class 2 is $100ms$; class 3: $400ms$),
- class 4 contains class 4 and class 5 (Upper bound on the mean IPTD delay of class 4 is $1s$ and upper bound on the packet loss probability of class 4 is $1 * 10 \exp -3$; class 5 has not specification for IPTD, IPDV, IPLR adn IPER).

4.3 Measurement Results

All named parameters like IPPR, IPTD, IPDV, IPLR and IPER have been measured. Due to the fact that all tests resulted in an IPER of zero, no further diagrams containing the error ratio are figured out. In terms of comparision different tests related to various physical links, i.e. 10/100/1000MBit/s bandwidth

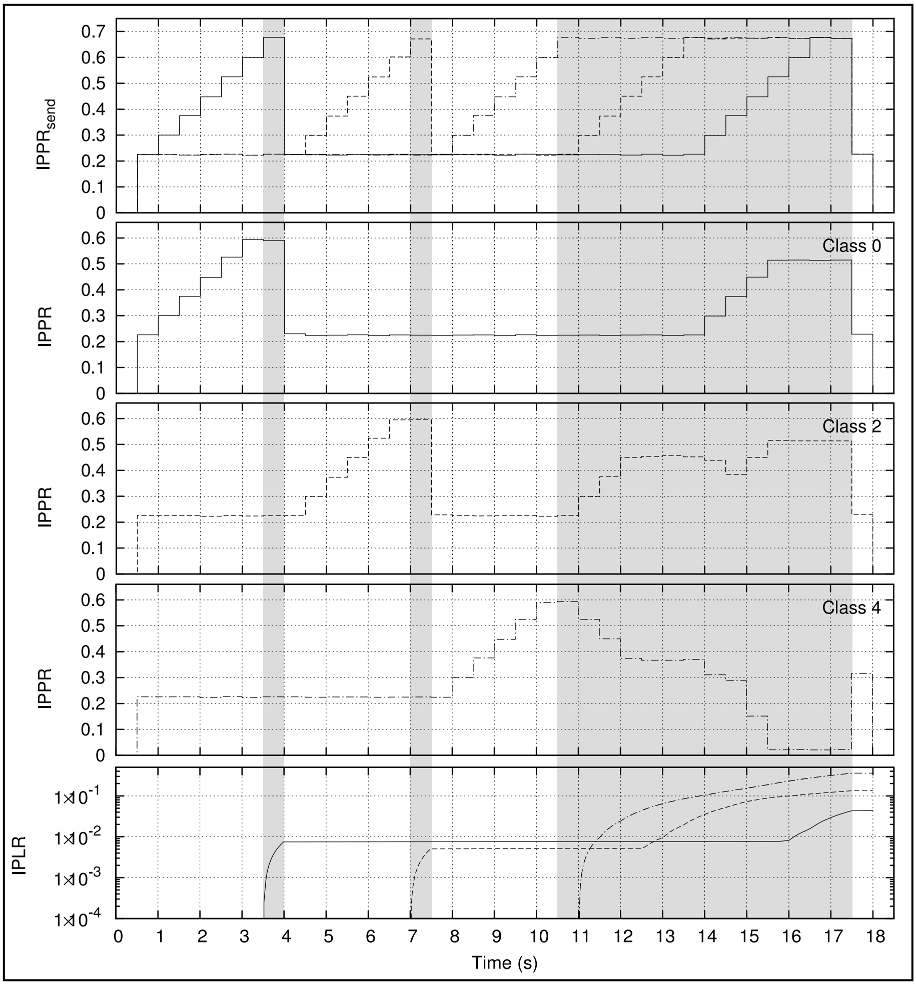

Fig. 7. IPPR and IPLR Measurements (overload condition in gray highlighted parts) Note: IPLR results are cumulated

and diverse logical links from 1MBit/s to 250MBit/s bandwidth no dependencies have been identified. Seeing that a detailed diagram for each test does not offer more information, all IPPRs have been normalized. All QoS classes named class 0, 2 or 4 are exactly the same as described in ITU-T standard[13]. Based on used IP traffic flows, test results are drawn seperatly and combined, distinguishable in line types. In addition all sent IP traffic flows ($IPPR_{send}$) are shown above in Figure 7. For all diagrams, time intervals are the same and overload conditions are marked by gray highlighted areas.

Using the normalized view of incoming and outgoing IP traffic limit load and subsequently overload conditions are readily identifiable using IPLR by evaluating too (see Figure 7). While operating condition is below overload status,

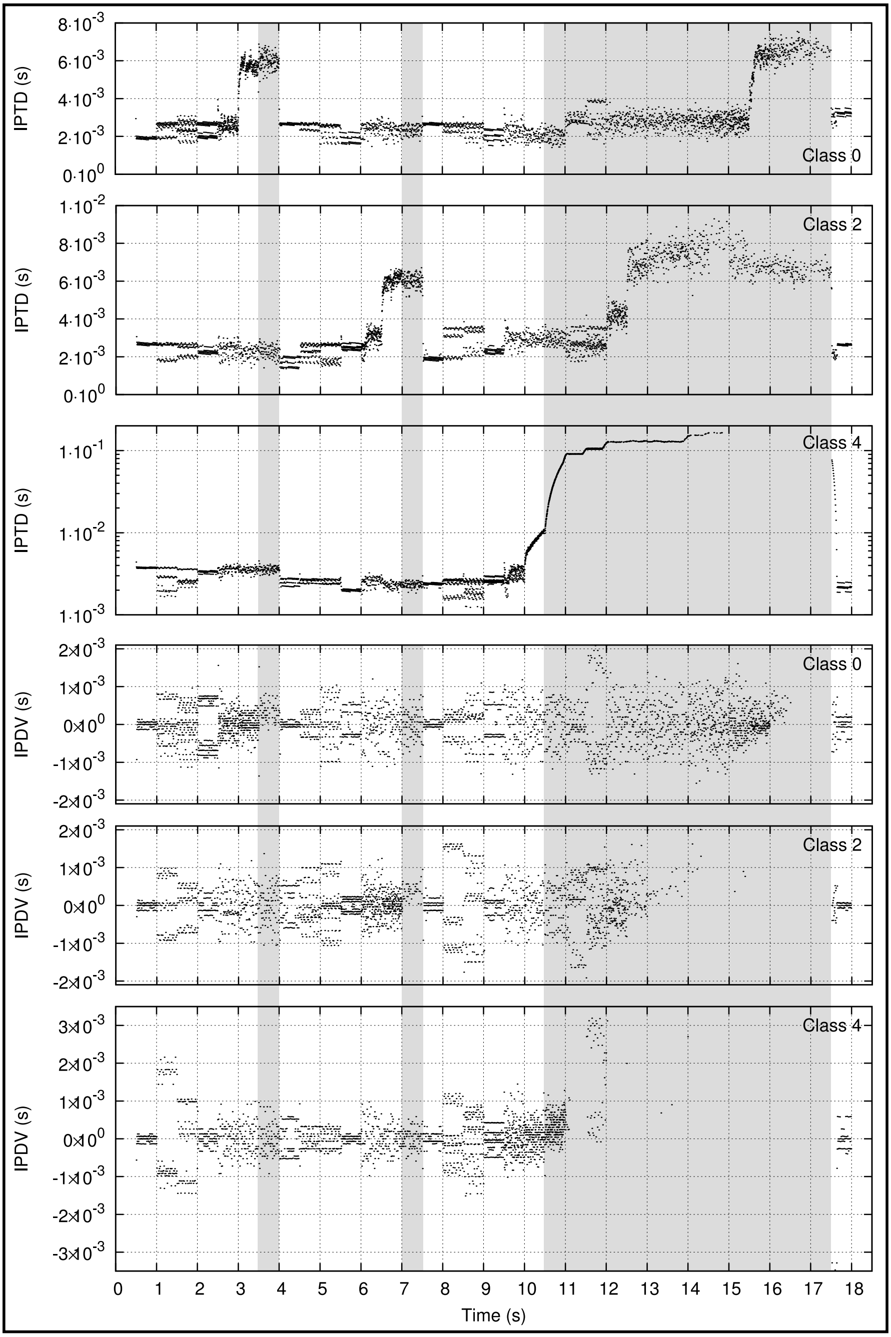

Fig. 8. IPTD and IPDV Measurements (overload condition in gray highlighted parts)

Table 1. QoS Class 0 - Measurement results (underload and limit load)

Parameter	Maximum Value from Standard	Measured Value	Evaluation
IPTD	3ms	$< 3.5ms$ (underload) $< 6.9ms$ (limit load)	(pass)
IPDV	3ms	$< 2.1ms$	pass
IPER	$1 * 10 \exp -4$	0	pass
IPLR	$1 * 10 \exp -3$	$0 * 10 \exp -3$	pass

Table 2. QoS Class 2 - Measurement results (underload and limit load)

Parameter	Maximum Value from Standard	Measured Value	Evaluation
IPTD	3ms	$< 4.0ms$ (underload) $< 6.8ms$ (limit load)	(pass)
IPDV	unspecified	$< 2.1ms$	pass
IPER	$1 * 10 \exp -4$	0	pass
IPLR	$1 * 10 \exp -3$	$7.3 * 10 \exp -4$	pass

Table 3. QoS Class 4 - Measurement results (underload and limit load)

Parameter	Maximum Value from Standard	Measured Value	Evaluation
IPTD	64ms	$< 12ms$	pass
IPDV	unspecified	$< 3.2ms$	pass
IPER	$1 * 10 \exp -4$	0	pass
IPLR	$1 * 10 \exp -3$	$9.2 * 10 \exp -4$	pass

all IP traffic flows will be scheduled as given by traffic policing rules related to each IP traffic class. In doing so, no packet loss has been detected exceeding maximum values from ITU-T standardisation[13]. In case an overload condition occurs, packets have been lost. On the basis of recorded IPLR, it is evident that class based queueing and sceduling algorithms have been implemented as well as configured policing rules in terms of traffic class hierarchy.

Commonly obtained results about IPTDs shows the IP packet processing time does not exceed considerable given maximum values in underload condition. Other operating states cause in significant exceedings of IPTD maximum values compared with underload condition (see Figure 8)[13]. Minor deviations about $0.5ms$ to $1.0ms$ have to be evaluated with reference to IPDV results. Based on the worst case both values, maximum IPTD ($3ms$) and maximum IPDV ($3ms$) results in an interval of $3ms + 3ms = 6ms$, a differentiated evaluation should be done. So an under-usage of IPDV enables an exceeding of IPTD in theory provided that in doing so the sum of IPTD and IPDV does not exceed $6ms$. Regarding measured results this theoretical fact can be applied here. All results marked by brackets in table 1, 2 and 3 are evaluated involving the limitation described above. Further collected data about IPDV results have been analysed. Thereby an under-usage for all traffic classes has been found evidently (see

Figure 8). Summarized for all measured traffic classes as defined in ITU-T table 1, 2 and 3 contains maximum values and measured values added by an evaluation. Contained maximum values related to given QoS class are assigned to a Border Gateway Function equates to the presented IBGF prototyp. Partially, table elements are splitted to seperate different operating states like underload and limit load condition. Only underload operation state has been evaluated expecting work load states were been lower than limit load state.

5 Summary

By evaluating different processed data streams, the prototypical correctness was proven by using a range of Open Source Software tools (NetFilter, TrafficControl). Therefore, basic functions required by the standard are realized. Moreover, by implementing points 5.1 and 5.2, special functions of the IBGF for converting transported data were successfully demonstrated. Further studies and research are still necessary for the data carrying mechanism illustrated in point 8. The communication over the Ia-Interface was realized by means of an Extensible Markup Language Remote Procedure Call (XML-RPC) on a functional level, and terminated by a custom replication (protocol generator and receiver) instead of the SPDF. Achieved measurement results shows detailed that the presented IBGF prototyp meet the requirements given by ITU-T standardisation related to the Border Gateway Function. Minor changes in results of IPTD are acceptable due to under-usage of IPDV because the interval sum does not exceed theoretical maximum value.

6 Future Prospects

The implementation for the illustrated structure of the IBGF was carried out using Open Source Software components. However, implementing the Ia-interface according to standards[3] for the communication with the SPDF is still outstanding. A focus for further studies is benchmarking the IBGF with respect to the expected data throughput of each corresponding operation and subsequent optimization of function blocks, which were illustrated here. Moreover studies related to optimizing control parameters of traffic control should be aimed from the viewpoint of existing media codecs capsulated in IP packets. With the prototypical implementation of the IBGF it is possible, in principle, to realize a carrier grade conform interconnection of IMS networks and IP Multimedia networks on the transport layer.

Acknowledgement

Supports from students have contributed to prepare this presented IBGF prototype. The authors would like to thank Stephan Händel for implementing the IBGF using OSS, Peter Hermann for testing performance and desired policing rules related to QoS parameters and Michael Erler for supporting test tools. We would like to thank the Institute of Telecommunication and Information Technology at the HfTL for making test and measurement equipment available to us.

References

1. ETSI-TISPAN ES 282 001: NGN Functional Architecture v3.3.0 (February 2009)
2. ETSI-TISPAN ES 282 003: Resource andAdmission Control Sub-System (RACS): Functional Architecture v3.3.0 (February 2009)
3. ETSI-TISPAN ES 283 018: Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification v2.7.1 (September 2009)
4. ETSI-TISPAN TS 183 048: Resource and Admission Control System (RACS); Protocol Signalling flows specification; RACS Stage 3 v1.4.0 (June 2008)
5. ETSI-TISPAN TR 182 022: Architectures for QoS handling v2.0.0 (December 2007)
6. IETF RFC 2474 (Kathleen Nichols and Steven Blake and Fred Baker and David L. Black): Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 Headers (December 1998)
7. IETF RFC 1349 (Philip Almquist): Type of Service in the Internet Protocol Suite (July 1992)
8. netfilter Framework (October 2008), `http://www.netfilter.org/`
9. ITU-T Y.1540: Internet protocol data communication service IP packet transfer and availability performance parameters (November 2007)
10. IETF RFC3393: IP Packet Delay Variation Metric for IP Performance Metrics, IPPM (2002)
11. IETF RFC3550: RTP: A Transport Protocol for Real-Time Applications (2003)
12. IETF RFC3357: One-way Loss Pattern Sample Metrics (2002)
13. ITU-T Y.1541: Network performance objectives for IP-based services (February 2006)