3GPP TR 23.848 V0.9.0 (2010-02)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on enhancements to IMS border functions for Interconnection of IMS based Services; (Release 9)

Remove GSM logo from the cover page for pure 3rd Generation documents.

Select keywords from list provided in specs database.

Keywords
<keyword[, keyword]>

3GPP

Postal address

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

Internet
http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

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

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The objective of this document is to analyse and identify enhancements needed in the current 3GPP IMS interconnection architecture driven by the needs that new business models/service delivery scenarios impose at the interconnection points of the IMS operators.

The present document will covers network to network interconnection as main objective and addresses the issues related to both control and user plane functionalities including:

- signalling treatment,
- numbering/naming/addressing,
- IP interworking,
- policy management,
- e2e QoS,
- transcoding,
- security,
- charging.

The purpose of this document is to formulate architectural solutions for the enhanced functionalities identified to cover all IMS operator's needs in this widespread environment. These solutions should be applicable for an IMS operator in a common IMS environment (i.e. regardless the access being used) as well as for direct and indirect interconnection paradigms. Finally, the best solution/s should be agreed and impacted normative work in 3GPP identified to update current 3GPP specifications with the output of this work.

2 References

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

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

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

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

[3] 3GPP TS 29.165: "Inter-IMS Network to Network Interface (NNI)".

[4] 3GPP TS 29.238: "Interconnection Border Control Function – Transition Gateway; H.248 profile; Stage 3".

[5] 3GPP TS 23.506: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description".

[6] 3GPP TS 23.517: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[7] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[8] ETSI TS 183 017: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF);Protocol specification".

[9] ETSI ES 283 018: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification".

[10] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".

[11] 3GPP TR 22.893: "Study into Identification of Advanced Requirements for IP Interconnection of Services".

[12] GSMA PRD IR.34: "Inter-Service Provider IP Backbone Guidelines".

[13] 3GPP TS 33.106: "Lawful interception requirements".

[14] 3GPP TR 23.869: "Support for IMS Emergency Calls over GPRS and EPS".

[15] 3GPP TS 24.605: "Conference (CONF) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[16] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[17] 3GPP TS 24.229: "IP Multimedia Call Control based on SIP and SDP; Stage 3".

[18] 3GPP TR 23.812: "Feasibility Study on IMS Evolution".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

ACL Filter: The logic in the IBCF that determines whether to allow, deny and apply logging to a session.

ACL Profile: It is a handle for a set of ACL rules. These ACL rules are usually related, and can be applicable to, for example,all incoming sessions, all outgoing sessions, all incoming sessions from a particular IP address all outgoing sessions to a set of AoRs, etc.

Inbound Session: Session originated in another IMS or SIP network, routed into the considered IMS network through IMS border entities.

Inbound Traffic: Data traffic associated with an Inbound or Outbound Session, flowing into the considered IMS network through IMS border entities.

Lawful Interception (LI): Interception of telecommunications traffic and related information in modern telecommunications systems due to laws of individual nations and regional institutions, and sometimes licensing and operating conditions. It has to be noted that lawful interception shall always be done in accordance with the applicable national or regional laws and technical regulations [13].

Outbound Session: Session routed to another IMS or SIP network through IMS border entities,

Outbound Traffic: Data traffic associated with an Inbound or Outbound Session, flowing out of the considered IMS network through IMS border entities.

3.2 Symbols

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

Gq'	TISPAN Reference Point between an AF and a SPDF.
Ia	TISPAN Reference Point between a SPDF and a C-BGF/I-BGF.
Ix	Reference Point between IBCF and TrGW.
Ic	TISPAN Reference Point between an IBCF and another IBCF belonging to a different IM CN subsystem network.
Iz	TISPAN Reference Point between an I-BGF and another I-BGF or media handling node belonging to a different IM CN subsystem network.
Ici	Reference Point between an IBCF and another IBCF or I-CSCF belonging to a different IM CN subsystem network.
Izi	Reference Point between a TrGW and another TrGW or media handling node belonging to a different IM CN subsystem network.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

ACL	Access Control List
AF	Application Function
DoS	Denial of Service
IBCF	Interconnection Border Control Function
IBPCF	Interconnection Border Policy Control Function
I-BGF	Interconnection-Border Gateway Function
II-NNI	Inter-IMS Network to Network Interface
IMS ALG	IMS Application Level Gateway
IPX	IP Packet eXchange
LI	Lawful Interception
NGCN	Next Generation Corporate Networks
NGN	Next Generation Networks
NNI	Network to Network Interface
RACS	Resource and Admission Control Subsystem
SPDF	Service-based Policy Decision Function
THIG	Topology Hiding Inter-network Gateway
TrGW	Transition Gateway

4 Review of Current IMS Interconnection Architectures

Editor's note: This chapter to summarize current models of IMS interconnection, in order to show the gap between current functionalities and detected functionalities in previous chapters.

4.1 Introduction

This section makes a review of the current IMS architecture models for interconnection purposes from the perspective of different SDOs. The drivers for doing that are as follows:

- To provide the background information, establishing the starting point for further analysis.
- To avoid duplicating efforts investigating functionalities that are already identified.

- To be able to gather and show the complete harmonized portfolio of functionalities available for the IMS operators at the borders of their networks.

In the next sub-clauses, a description of IMS interconnection architectures and related functions is offered.

4.2 3GPP Release 8

This sub-clause describes the current 3GPP model for IMS interconnection purposes. This model is deeply described in 3GPP TS 23.228 [2] and 3GPP TS 29.165 [3]. The related architecture (i.e. logical entities and interfaces) is depicted in Figure 4.2-1.

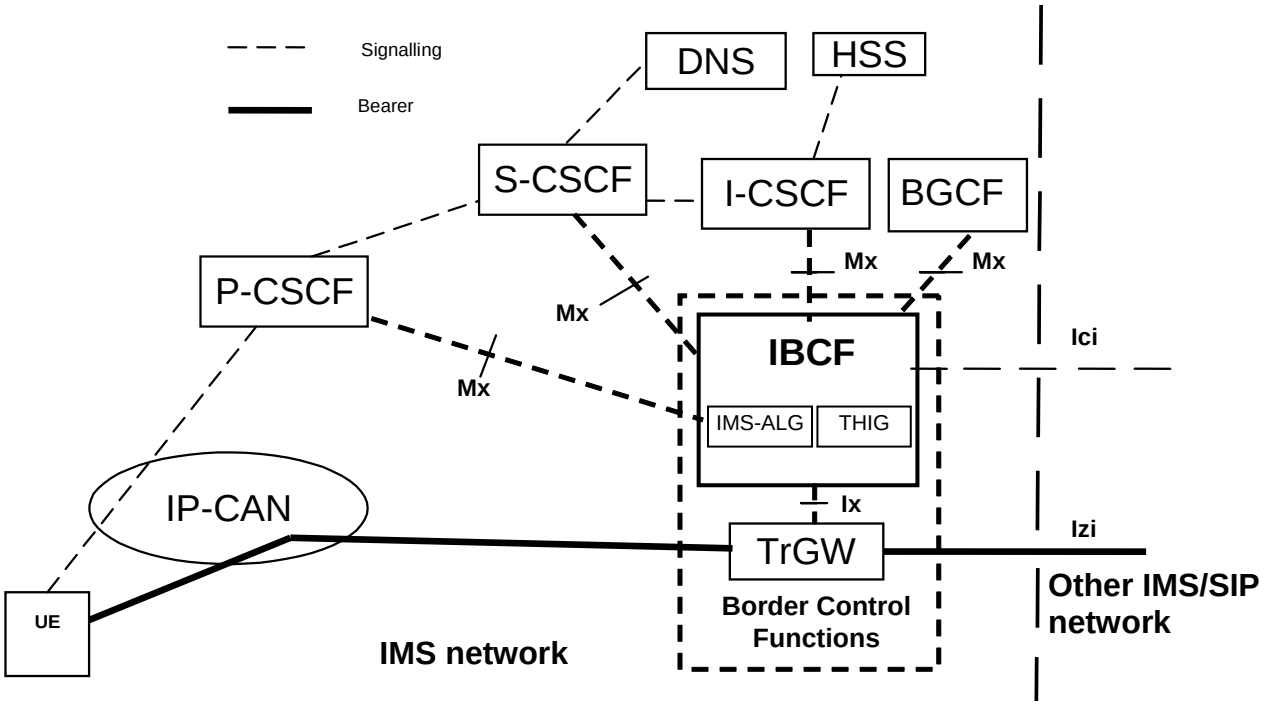

Figure 4.2-1: 3GPP IMS interconnection architecture

The interconnection model comprises IBCF and TrGW logical entities. The IBCF is located at the control plane, handling signalling; the TrGW is located at the user plane, handling IMS media flows. The control interface between them is named Ix; H.248 profile for Ix is defined in 3GPP TS 29.238 [4]. Current functionalities for both logical entities are described in 3GPP TS 23.228 [2].

4.3 ETSI-TISPAN Release 2

This sub-clause describes the current TISPAN model for IMS interconnection purposes. This model is described in 3GPP TS 23.506 [5] and 3GPP TS 23.517 [6]. The related architecture (i.e. logical entities and reference points) is depicted in Figure 4.3-1.

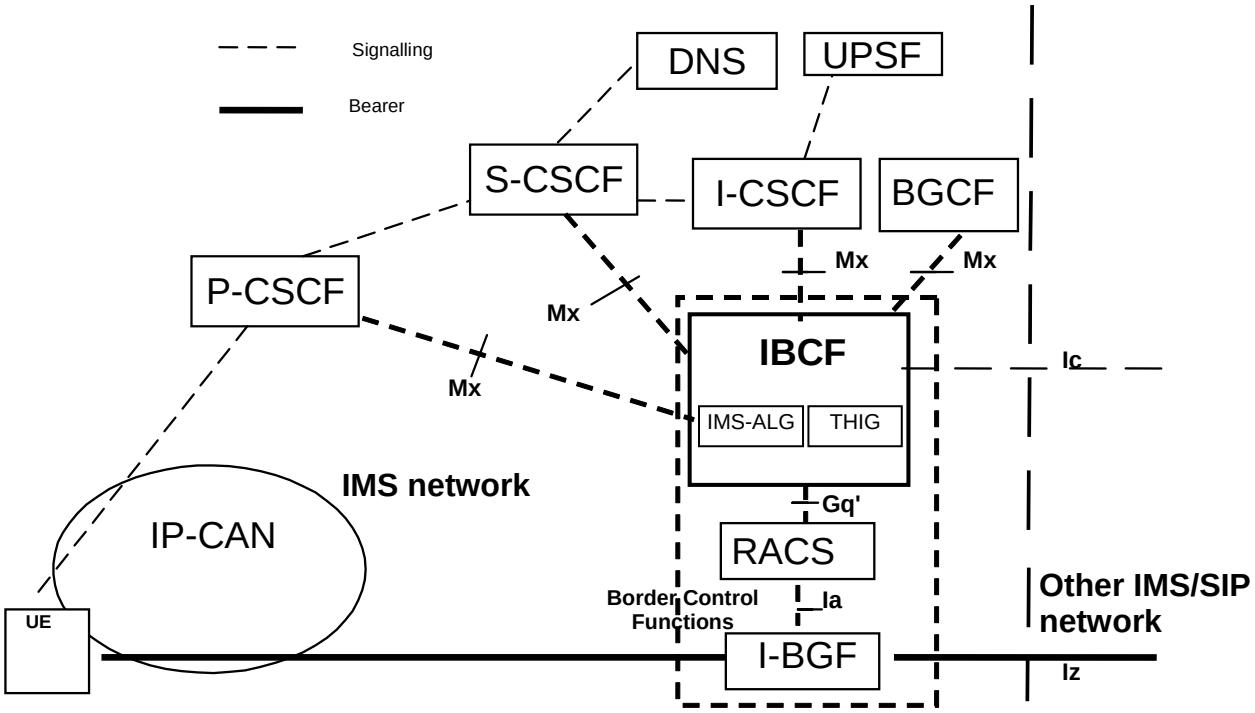

Figure 4.3-1: TISPAN IMS interconnection architecture

The interconnection model comprises IBCF, RACS (SPDF and C-RACF functions) and I-BGF logical entities. The IBCF is located at the control plane, handling signalling; the I-BGF is located at the user plane, handling IMS media flows. The RACS (SPDF) acts as a policy and resource allocation control function between the service and transport planes. The presence of a policy function at this point is one of the main different between 3GPP and TISPAN architectures. Current functionalities for IBCF and I-BGF are indicated in 3GPP TS 23.517 [6] and ETSI ES 282 001 [7], respectively.

The reference points between them are:

- Gq' between the IBCF and the SPDF. It is used for requesting transport plane resources and admission control for fixed broadband access networks. It is a Diameter based reference point [8].

- Ia between the SPDF and the I-BGF. It is used to request services. It is a H.248 based reference point for controlling Border Gateway Functions (see ETSI ES 283 018 [9]).

The table below summarizes the I-BGF tasks.

Table 4.3-1: List of I-BGF tasks

➢ opening and closing gates (i.e. packets filtering depending on "IP address / port") ➢ packet marking for outgoing traffic ➢ policing of incoming traffic ➢ resource allocation for upstream and downstream traffic ➢ usage metering ➢ allocation and translation of IP addresses and port numbers (NAPT) ➢ interworking between IPv4 and IPv6 networks (NAPT-PT) ➢ media transcoding

5 Overview. Example Service Delivery Scenarios

Editor's note: This chapter to describe whole interconnection environment that it is proposed to be addressed. Once explained, to deep case-by-case interconnection scenarios in order to result functionalities needed.

5.1 Introduction

This section provides an overview of the IMS interconnection environment intended to be addressed in this TR. This will establish a guide to drive the work and focus on concrete scenarios to be treated. A graphical representation of it is depicted in Figure 5.1-1.

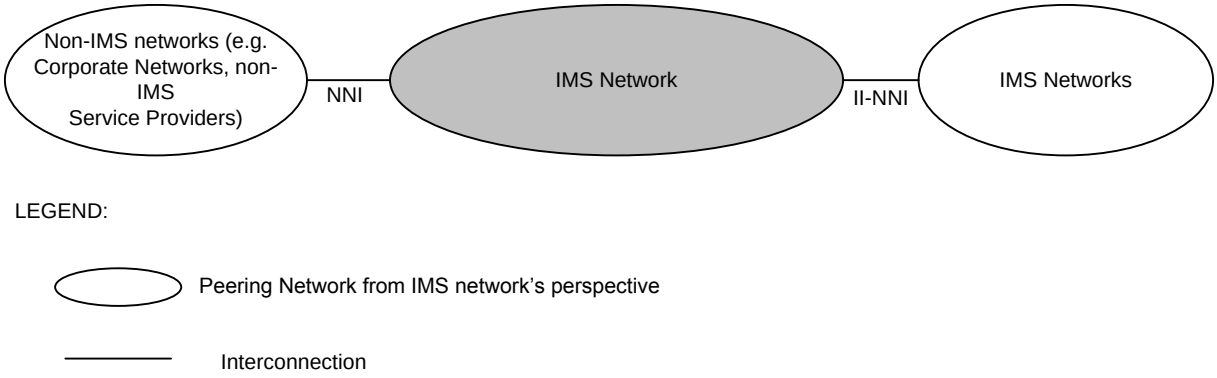

Figure 5.1-1: IMS interconnection ecosystem

Main area of interest is:

- IMS to IMS interconnection (IMS interworking and roaming)

Other area of interest should be IMS to non-IMS interconnection, including:

- IMS to corporate networks interconnection;

NOTE: This aspect could be impacted by the current work ongoing in TISPAN, about NGCN-NGN(IMS) interface implementation.

- IMS to non-IMS service providers interconnection (e.g. H.323 based, SIP-I or IETF SIP based domains).

General requirements for IMS interconnection are contained in 3GPP TS 22.228 [10] and 3GPP TR 22.893 [11]. Legacy functions (i.e. functions already existing) and new IMS border functions identified in this TR shall be applicable in a common IMS environment (i.e. being useful for both fixed and mobile IMS operators).

Thus, it should achieve a complete and harmonized set of functionalities at the border of the IMS operator network for both direct and indirect interconnection schemes:

- Direct interconnection: the interconnection between parties/networks is established without any intermediate agents/carriers (e.g. by means of a leased line or using VPNs (Virtual Private Networks)); this is likely to be the case for national traffic.

- Indirect interconnection: the interconnection link between parties/networks is established through intermediate agents/carriers (e.g. by means of an IPX Proxy , see GSMA PRD IR.34 [12]); this is likely to be the case for international traffic, in order to save CAPEX and OPEX costs.

Although new functions for IMS interconnection could result from analysis of the scenarios in the next sub-clauses mentioning a specific service, it does not mean precluding other IMS services. In fact, these new functions should be aimed to enable all type of IMS services in a worldwide ecosystem.

5.2 Inter-Operator IMS interworking/Roaming

5.2.1 Scenario 1: Conference service

Figure 5.2.1-1 depicts the provision of a conference service, following the same principles as 3GPP TS 24.605 [15] and 3GPP TS 24.147 [16]. UE#1 has created a conference and invites UE#2 to it by sending a REFER request. UE#1 and UE#2 belong to different IMS operators. Transcoding might also be provided by an MRFC/MRFP in the IMS Operator B domain; or via the MRFC/MRFP that provides the conferencing service.

The flow has been simplified to facilitate its understanding. The flow does not show the 100 Trying responses. The rest are simplified in one line, marking with a black point in the intersection with each functional entity line the functional entitys which treat them (the path of the responses).

3GPP TS 24.147 [16] subclause A.4.4.1contains a complete description of messages applicable to this scenario. The explanations below Figure 5.2.1-1 details the main steps, focussing on the behaviour at the interconnection functional entities.

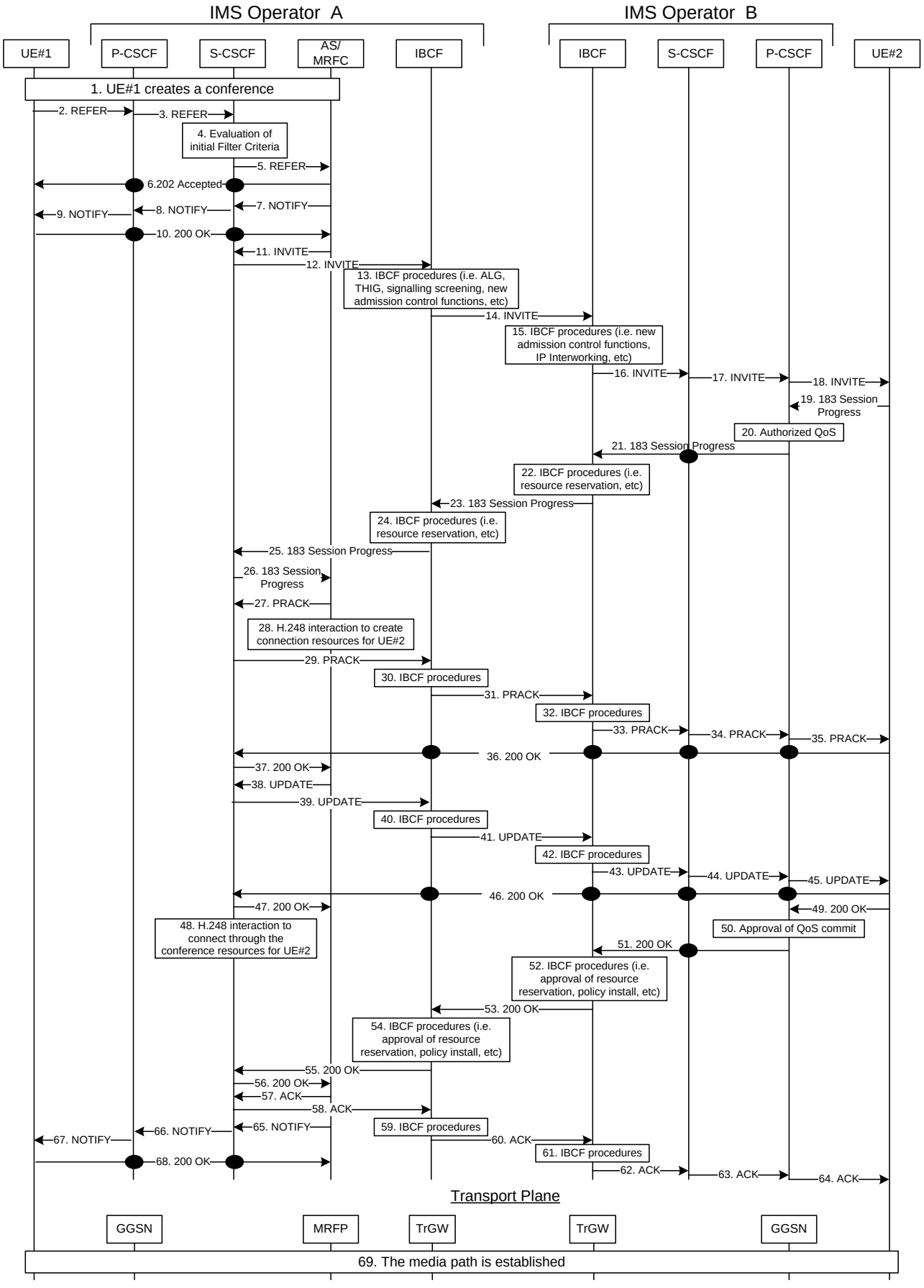

Figure 5.2.1-1: CONF call with REFER interworking at the AS. UE#1 and UE#2 belong to different operators

1. UE#1 creates a conference and learns the conference URI allocated for this conference.

2~10. UE#1wants to join UE#2 to the conference, for this purpose it sends a SIP REFER request towards the AS/MRFC. The AS/MRFC sends a SIP NOTIFY request to indicate that the AS is processing the REFER request.

11~12. The AS/MRFC sends a SIP INVITE request to the user who is indicated in the Refer-To header of the REFER method. The INVITE includes a SDP offer with all the codecs applicable for the media of this conference (e.g. H.263 for video and AMR for voice). The S-CSCF forwards the request to the operator's exit point to reach UE#2.

13~14 At the reception of the SIP INVITE, the IBCF can apply the current functionalities indicated in 3GPP TS 23.228 [2]. The related procedures are detailed in 3GPP TS 24.229 [17]. As an operator option, the IBCF could apply the following functionalities:

- Access Control List management procedures, to avoid communication with forbidden networks and DoS protection mechanisms.

- Security features: message size verification of SIP signalling, lawful interception if needed (IMS Operator A in accordance with the applicable national or regional laws).

- Admission control functions (e.g. control of established number of sessions/current bandwidth consumed) are applied, according to SLA agreed between IMS operators. Normally, these are only applied at the ingress to the IMS Operator B domain.

- If priority service is supported (i.e. containing an authorised Resource-Priority header) the IBCF applies procedures corresponding to the Resource-Priority header field value.

- If congestion is detected in the link or there are routing policies to be applied for the interconnected network, load balancing and routing mechanisms can be applied.

- Topology hiding will normally be provided at the egress of the IMS Operator A domain. Codecs may also be appended to the SDP offer at the IBCF of the IMS Operator A domain

15. The initial SIP INVITE request arrives to the IMS Operator B domain. Same procedures (both current and new) as stated in steps 13~14, can be applied by the IBCF in the terminating side. Topology hiding is not normally performed at the ingress of the IMS Operator B domain.

16~18. The INVITE arrives to the UE#2.

19~21. The UE#2 responds with a 183 Session Progress with the SDP response (with the codecs selection; if UE#2 selects an IBCF codec, transcoding will be necessary). The P-CSCF authorizes the resources for this session. The 183 Session Progress is forwarded towards the IBCF.

22~24. When it crosses the IBCFs, same procedures as identified in steps 13~15 can be applied. Additionally, the IBCFs can apply the following functionality:

- QoS authorization and resource reservation, and to generate policies to be installed in the transport plane.

- Allocation of transcoding resources, media address and codecs changes in SDP, and necessary communication with UE#2 and MRFC.

25~26. The 183 Session Progress is forwarded towards the AS/MRFC.

27~37. The AS/MRFC sends the PRACK method (without an SDP offer because there are no changes in the media characteristics). It starts the reservation procedures for the resources needed in the MRFP. The PRACK method is forwarded towards UE#2. UE#2 acknowledges the PRACK request with a 200 OK. No specific mention to IBCF procedures in steps 30~32, they can be the same as indicated in steps 13~15.

38~47. The AS/MRFC sends the UPDATE request to UE#2 when the resource reservation is completed. UE#2 acknowledges the UPDATE request with a 200 OK. No specific mention to IBCF procedures in steps 30~32, they can be the same as indicated in steps 13~15.

48. The MRFC initiates a H.248 interaction to connect through the multimedia processing for UE#2 in MRFP.

49~51. UE#2 sends a 200 OK final response to the initial INVITE. The P-CSCF approves the QoS resources. The 200 OK is forwarded towards the IBCF.

52~54. When it cross the IBCFs, same procedures as identified in steps 13~15 can be applied. Additionally, the IBCFs can apply the following functionalities:

- Approval of the resources reserved and to install the policies in the transport plane..
- At this moment, the IBCF can open a CDR to record the charging information related (per 3GPP TS 23.228 [2]).

55~64. The 200 OK is forwarded towards the AS/MRFC. The AS/MRFC responds to the 200 OK with and ACK request.

65~68. The AS/MRFC sends a NOTIFY request to inform that the referred party has joint the conference. UE#1 responds with a 200 OK.

69. The media path is now established. The TrGWs involved can apply the current functionalities indicated in 3GPP TS 23.228 [2]. Additionally the TrGWs may apply the following functionalities:

- Dynamic pin-holing: opening/closing gates on a session-by-session basis, discarding packets that don't match any data flow filter.
- Resource allocation and bandwidth reservation (per IP flow) for inbound/outbound traffic.
- Media policing of inbound/outbound traffic based on static and dynamic policies (e.g. bandwidth control).
- Packet marking of traffic to ensure an adequate treatment of traffic flows.
- Resource (e.g. QoS) monitoring: providing a real-time evaluation of network performance and giving parameters for SLA verification.
- Resource reporting and CDR generation: the TrGWs open charging records to assure a correct billing to the served user. The QoS approved in the UNI side could be different from the QoS applied in the interconnection side. The user experience depends of the QoS possible in each network side, so the charging records must take into account the real QoS provisioned.
- Capacity, based on routing policies and status of the network, to use the best path for media flows between the interconnected networks.

6 Functionalities for IMS Interconnection

Editor's note: This chapter to gather functionalities detected in previous scenarios, classified by control and user related functionalities.

6.1 Control Plane

This clause is a summary of the control plane functionalities that may be needed by an IMS operator at the border.

The list of new functions to be considered for the control plane is as follows:

- Service level interoperability related features:
  - Signalling transport protocol selection and interworking (i.e. dynamic transport protocol change for signalling; e.g. switching between UDP, TCP, SCTP,… for transport of SIP signalling between the interconnected peering networks).
  - Signalling Inspection. It should be possible to look inside SIP signalling, in particular to analyse the media types and capabilities for the purposes of applying local policies.
- Interworking between SIP and other protocols (e.g. H.323, SIP-I)

- Voice Quality Enhancements (VQE) capability exchange and selection of media processing resources (3GPP working groups specializing in this subject are invited to study the following areas):

  - Ability for border control plane node to signal to other control plane nodes the VQE capabilities that it has applied/access to and the VQE capabilities have been previously enacted on the media path.

    Editor's Note: The suitability of control plane versus user plane signalling is FFS.

  Note: Specific codecs may have built in VQE capabilities (e.g. the Silence Suppression capability of G.729)

  - Communicate with other control plane nodes in order to determine whether to apply the appropriate VQE resources to the user plane in order to achieve the best voice quality and most effective use of network resources.

    Editor's Note: The suitability of control plane versus user plane signalling is FFS.

  Note: there may be no requirement to apply VQE resources at the network border, depending on whether they have been applied elsewhere.

- Service Level Agreement enforcement related features:

  - Resource admission control, according to Service Level Agreement (SLA) agreed between involved parties. This may be based on policies per interconnected domain or per Public Service destination (e.g. application of specific resource control policy to sessions targeted to PSIs related to gaming services), using quantitative criteria (e.g. total number of established Inbound/Outbound Sessions, total amount of related bandwidth consumed, application of an agreed traffic model), and/or qualitative criteria (e.g. number of sessions with a given priority, QoS, media type). Prior establishment of a new session, it is verified that the available resources are compatible with the requested resources taking into account existing reservations (i.e. number of current sessions/bandwidth already allocated) in order to assess the limit is not surpassed, and consequently accept or reject this new session. Inside this functionality two specific procedures could be applied:

    - Session rate based admission control. This means controlling total number of Inbound Session attempts in a given window of time coming from the interconnected domain. In case the number of session attempts exceeds an agreed threshold, incoming sessions should be rejected during a grace period.

    - Overbooking admission control: additional admission control procedure used when there is a lack of resource availability for a specific request. In this case, it should be considered (sum) the available resources plus the already committed resources for other requests and verified whether the requested resources do not exceed this amount. If it is the case, the admission is granted provided that only one request commits the same resources at a time; otherwise the request shall be denied.

  - Authorization of network resources after a successful admission control procedure.

- End-to-End QoS management related features:

  - Policy control: application of static and dynamic policies , related to SLAs agreed between operators for individual services or combination of services, in the transport plane, in order to control the resource allocation and bandwidth reservation (maximum/guaranteed bandwidth) procedures as well as dynamic pin-holing (i.e. gating control).

  - Support for the packet marking of Inbound/Outbound Traffic (e.g. setting the DiffServ Code Point, based on the associated QoS Class Identifier (QCI)).

- Policy-based Media Routing related feature: making the decision of inserting or otherwise a TrGW in the path of the user plane to influence the routing of media path (e.g. via the Home network) and therefore the use of other features, e.g. influencing the efficiency of OMR, local breakout.

Editor's Note: The Criteria of how and where the decision is made to involve the TrGW, based on IMS service and policies (e.g. OMR, LBO), is FFS.

- Load Balancing and Routing management related features:

  - Load Balancing across multiple remote IBCF nodes at interconnected peering network(s) with equal level of priority.

- Routing to multiple remote IBCF nodes at interconnected peering network(s), allowing several levels of priority between these nodes (e.g. using one node as primary and another node for overflow). This may be based on various criteria, such as threshold on the number of simultaneous sessions or on the total traffic sent to a peering network.

- Dynamic adaptation of routes in order to handle with different situations: node failures, overloads, precedence as destination. For this purpose, routing policies could be applied.

- Route hunting (serial forking) of sessions to remote IBCF nodes (multiple IBCF entry nodes at remote network forking to multiple interconnect peering networks). This may be accomplished by means of local route tables or external ENUM resources.

- Routing based on qualitative criteria:

  - originating peering networks (e.g. to provide the service agreed between peering operators),

  - specific SIP header value (e.g. to apply priority service).

- Selection of the TrGW to be used, based on the load of each TrGW.

- Security and protection related features:

  - Denial of Service (DoS) protection and prevention mechanisms (e.g. attacks from unknown/untrusted sources, volume-based attacks).

  - Message size verification, ensuring signalling messages formats do not exceed the sizes according to the corresponding standards (e.g. SIP message size control), avoiding to waste unnecessary resources (i.e bandwidth).

  - Overload control features:

    - Session spacing: this means to protect the next hop (for the SIP signaling session) in the near overload condition. This may be based on information received about the load in the node over the next hop. The next hop could be in the domain of the current network (inbound) or on the interconnection to the neighbouring network (outbound).

      Editor's Note: How the load information is received is FFS.

    - Session blocking: this means limiting the rate of accepted session to a given percentage (e.g. accept only 50% of incoming sessions).

  - Filtering of SIP methods and headers.

  - Ensuring authentication of the peering network, and signalling integrity, confidentiality and non-repudiation.

Editor's Note 1: Determination of what security related features are required is subject to investigation by SA3 (for example in the SA3 feasibility study on unsolicited communication).

- Access control features:

  - Management of Access Control Lists (ACLs); static and dynamic provision of allowed/forbidden domains/networks for enforcement of access control.

- System redundancy features:

  - System redundancy: back-up functionality in order to maintain service to the end user when an attack or disaster drops down the active system at the interconnection border (e.g. when a natural disaster or an attack drops down an IBCF, another IBCF should handle the current sessions of the first one).
    3GPP TR 23.812 [18] will document the results of the Study on IMS Evolution, including the results of investigation into IMS system redundancy in general.

- Regulatory related features:

  - Priority service support.

NOTE: The exact meaning of priority is left to national regulation and network configuration.

  - IMS Emergency calls support, handling and prioritization. Specific details for IP-CAN networks (i.e. GPRS and EPS) are being studied in 3GPP TR 23.869 [14].

  - Lawful Interception of signalling (control plane).

Editor's Note 2: Security and other features possibly should be considered inside SA3.

- Other features:

  - Simultaneous support of non-IMS traffic (e.g. legacy circuit-switch services) on the same IP interconnection than IMS traffic.

6.2 User Plane

This clause is a summary of the user plane functionalities that may be needed by an IMS operator at the border.

The list of new functions to be considered for the user plane is as follows:

- NA(P)T

- Transrating (i.e. change of codec packetization time)

- Detection of inactive bearer connections: in case no Inbound Traffic is received for a significant period of time, the IMS border may decide to release the session.

NOTE: This is to avoid maintaining "ghost" sessions, for which the UE connected to another network has been disconnected without releasing the session; in such case the serving network should detect the disconnection and release the session, but the IMS network needs to protect itself in case the peering network does not behave properly.

- End-to-End QoS management related features:

  - Dynamic pin-holing: opening/closing gates on a session-by-session basis (i.e. packets filtering depending on IP address/port, domain, number of connections, etc).

  - Resource allocation and bandwidth reservation (per IP flow) for Inbound/Outbound Traffic.

  - Packet Marking (per IP flow) for Inbound/Outbound Traffic: appliance of QoS differentiation mechanisms to allow an efficient and adequate management of the IP flows in the transport plane (i.e Diffserv, ToS class, MPLS support).

  - Media policing of Inbound/Outbound Traffic based on static and dynamic policies (e.g. bandwidth control).

  - Resource monitoring and reporting: QoS parameters like jitter, delay, data throughput, bandwidth, number of connections, session duration, octets send/received,…should be monitored for several purposes (e.g. from charging purposes up to real-time evaluation of the network, route performance and SLA verification). QoS metrics should be collected and reported on a per-session basis and with different levels of granularity [9]:

    - IP granularity: session duration, octets sent/received, discarded packets,…

    - Service granularity (e.g. RTP): packets sent/received, packet loss (%), delay, jitter, throughput,…

- Multilevel end-to-end billing related features:

  - IP flow-based charging in the user plane: generation of Charging Data Records (CDRs) and forward them to the Billing Domain for further processing, e.g. making subscriber bills. The user plane CDRs should contain information about the QoS applied for the interconnected domain to adequate the charging to the real E2E QoS enjoyed by the subscriber (e.g. the QoS applied in the UNI side could not be achieved in the NNI side).

- Routing related features:

  - Based on local routing policies and real-time traffic conditions monitored, it should be possible to use the best path to provide the service (i.e. manage the volume and rate of traffic).

  NOTE: specific implications of supporting Local Breakout and Optimal Media Routing are FFS.

- Security related features:
  - Handling of media flows according to DoS protection and prevention mechanisms.
  - Message size verification, ensuring media messages formats do not exceed the sizes according to the corresponding standards (e.g. RTP message size control), avoiding to waste unnecessary resources (i.e. bandwidth).

Editor's Note 1: Determination of what security related features are required is subject to investigation by SA3 (for example in the SA3 feasibility study on unsolicited communication).

- System redundancy features:
  - System redundancy: back-up functionality in order to maintain service to the end user when an attack or disaster drops down the active system at the interconnection border (e.g. when a natural disaster or an attack drops down a TrGW, another TrGW should handle the media flows, related to the current sessions, of the first one). 3GPP TR 23.812 [18] will document the results of the Study on IMS Evolution, including the results of investigation into IMS system redundancy in general.
- Regulatory features:
  - Lawful Interception of media (user plane).

Editor's Note 2: Security and Other features possibly should be considered inside SA3.

7 Architectural Proposals for IMS interconnection

Editor's note: This chapter to describe architectural solutions to cover the above scenarios indicating, architecture description, functional entities and their features, QoS and policy management impacts, Rx/Gq' harmonization, security considerations…

7.0 General considerations for the architectural proposals

Although this study is for the IMS border functions, the applicability for new proposed functionality to other 3GPP NNIs, e.g. the CS-NNI shall be considered.

If such applicability to other NNIs exist, it is highly desirable that the proposed architecture for the IMS NNI as far as possible can be applied for these other NNI in a similar fashion. In particular for the CS-NNI for which the existing architecture in TS.29.235 provide almost a one-to-one mapping of the current IMS border architecture, the different architectural proposals need be evaluated against how the can be applied for the CS-NNI.

7.1 Access Control List Management

7.1.1 General

Access Control Lists are managed using ACL profiles.

7.1.2 Alternative 1: ACL profile statically configured in IBCF

The ACL profiles are statically configured in the IBCF itself. This is a trivial case and does not need additional explanation.

7.1.3 Alternative 2: ACL profile stored in APR

The ACL profiles are stored in ACL Profile Repository (APR) managed by the Operator and are pushed to the IBCF. ACL profiles may also be pulled by the IBCF.

ACL profiles are transported over the Xp reference point as shown in Figure 7.1.3-1.

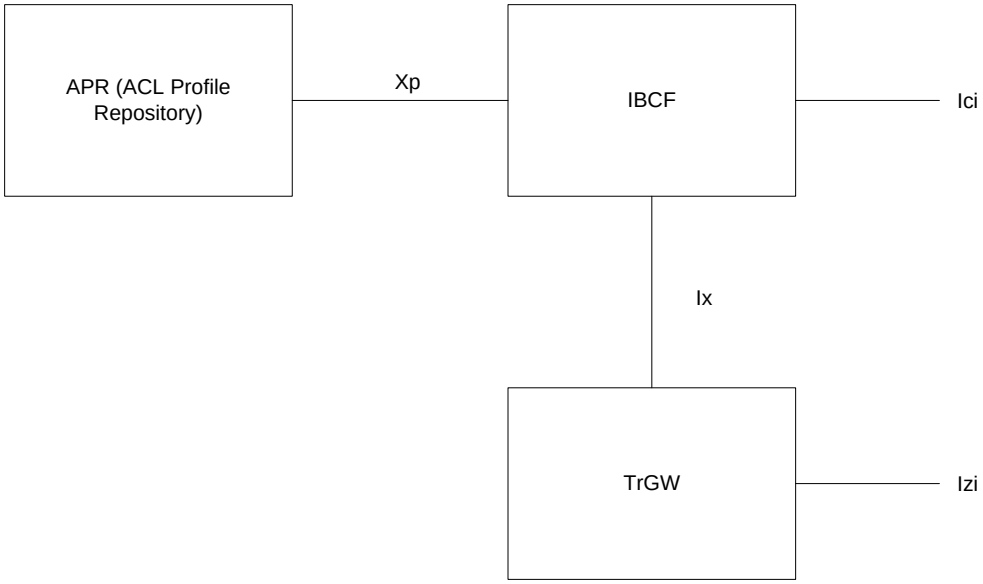

Figure 7.1.3-1: 3GPP IMS interconnection architecture with IMS ACL profile management

7.1.4 Access Control Lists

7.1.4.1 General

Access Control Lists are assigned to an IMS public identity (e.g. SIP URI) or a group of IMS public identities.

IBCF implements an ACL filter where the assigned ACL policy profile is used an input for the execution of the ACL filter when an IMS session is being setup.

ACL profiles mapped to wild carded public identities may be used provide access control to interconnected NGCNs (IMS corporate networks).

ACL profiles are managed between IBCF and an Operator's data repository as shown in Figure 7.1.2-1.

The ACL profiles are stored either in a new data/management repository or in IBCF.

An example usage shows how Access Control Lists may use wild carded public identities and provide access control e.g. *@telemarketing-company.com matches all IMPUs from realm "telemarketing-company".

7.1.4.2 ACL content and structure

ACLs are lists of rules , with each rule comprising of rule action, rule type and filter criteria.

7.1.4.2.1 Rule action

Rule action takes on one of the following values :

- **Permit:** The session is accepted and processed.
- **Deny:** The session is rejected.
- **Log:** Logs the sessions meeting the criteria specified in the ACL and can be done in conjunction to the actions above.

7.1.4.2.2 Rule filter criteria

Each ACL consists of one or more rules specifying the criteria that session initiation requests shall be compared against. The following criteria may be supported:

- **Any:** Applies to all the session requests
- **Source IP**: Applies to session requests based on source IP address of a peer IMS border node.
- **Source AoR :** Applies to session requests based on the source AoR.
- **Destination AoR :** Applies to session requests based on the destination AoR.

Rule filter criteria containing wildcarded public identities may be used provide access control to interconnected NGCNs (IMS corporate networks).

7.1.4.2.3 Rule types

Rule type is one of the following :

- **Inbound ACLs**: These ACLs will be applied to inbound sessions that are entering the IMS CN.
- **Outbound ACLs**: These ACLs will be applied to outbound sessions that are exiting the IMS CN.

7.2 Policy Control related features

7.2.1 Alternative 1

7.2.1.1 Functional split

The IBCF and TrGW are enhanced in order to split these features between these two functional entities.

New functions hosted by the IBCF:

- Resource admission control
- Policy control.
- Support for the packet marking / media policing of Inbound/Outbound Traffic based on static and dynamic policies: *provide directives to the TrGW*
- Selection of the TrGW to be used, based on the load of each TrGW.
- IMS Emergency calls support, handling and prioritization.

New functions hosted by the TrGW:

- Media policing of Inbound/Outbound Traffic: apply directives from IBCF

7.2.1.2 Description

The current architecture is kept. The functionality for policy and resource control is showed explicitly in Figure 7.2.1.2-1 to show the functional division.

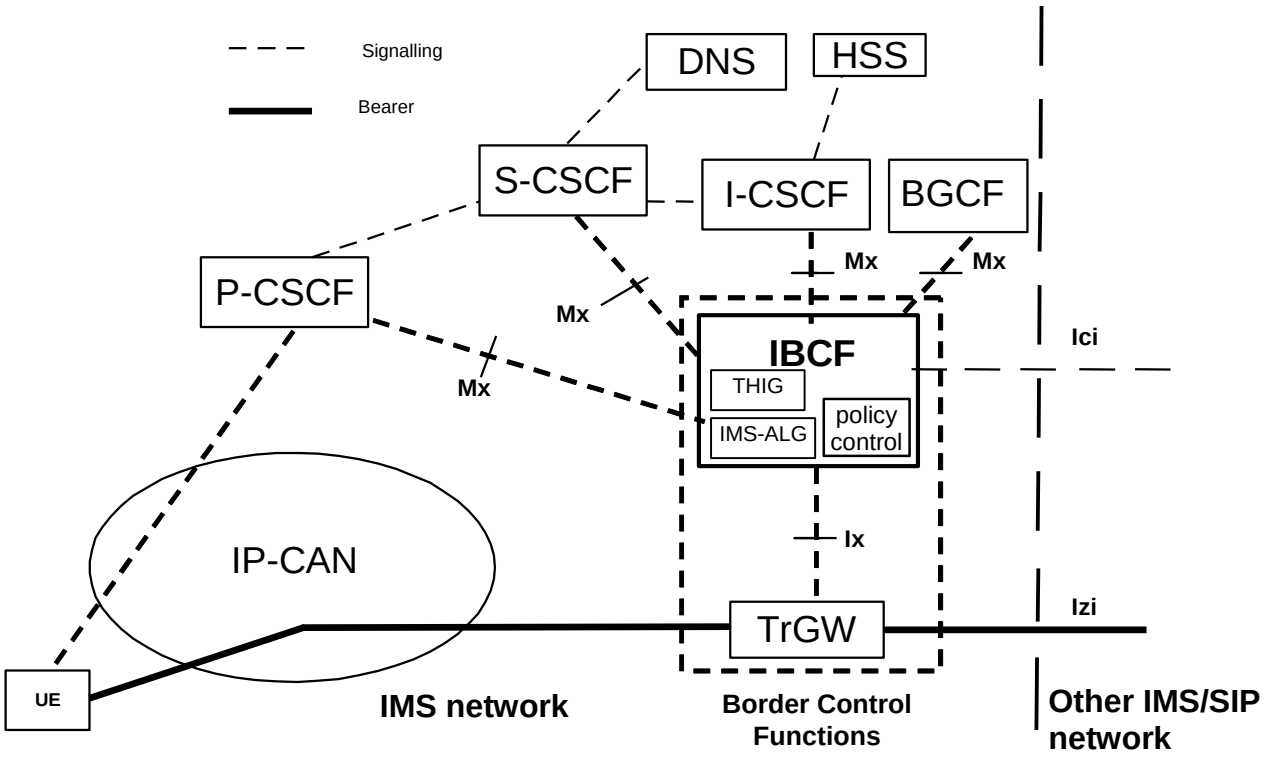

Figure 7.2.1.2-1: 3GPP IMS interconnection architecture with policy control clarified

7.2.1.3 Applicability to the simultaneous support of non-IMS traffic

Because policy control functions are in the IBCF, this alternative does not currently address the issue of having a policy control platform serving both IMS and non-IMS applications.

7.2.1.4 Information flow for media flow establishment

The following diagram provides a typical information flow for media flow establishment under this alternative.

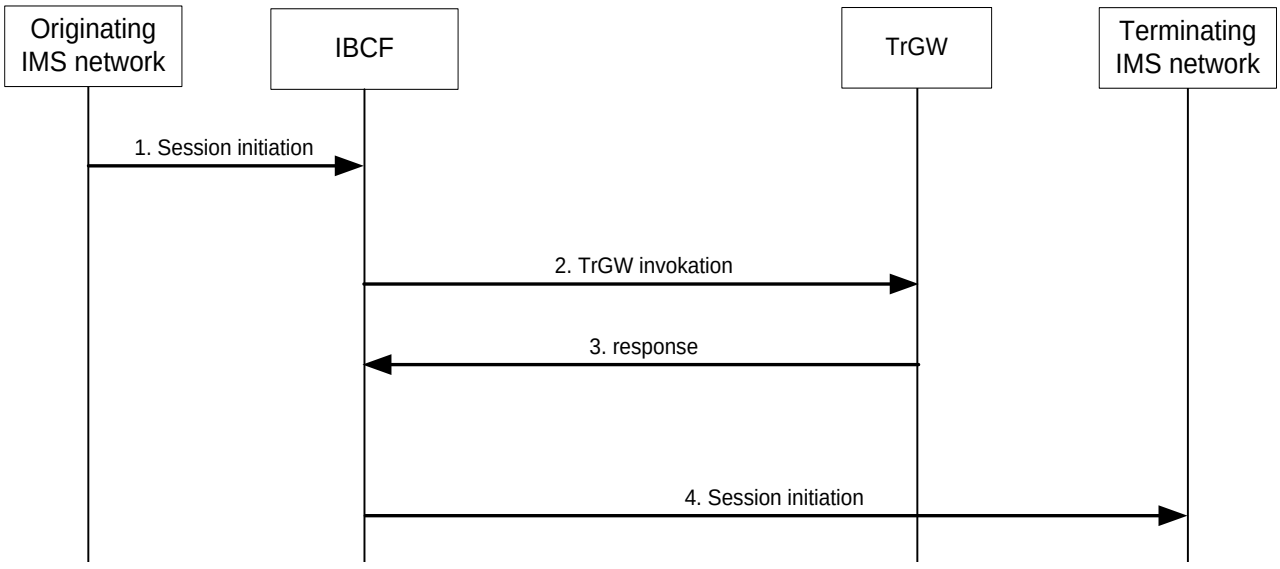

Figure 7.2.1.4-1: Information flow for media flow establishment under Alternative 1

7.2.2 Alternative 2: addition of a functional entity for policy control

7.2.2.1 Functional split

A new functional entity called Interconnection Border Policy Control Function (IBPCF) is added.

7.2.2.2 New functions hosted by the IBCF:

- IMS Emergency calls / Priority service support and handling.

7.2.2.3 Functions hosted by the IBPCF:

- Resource admission control
- Policy control.
- Support for the packet marking / media policing of Inbound/Outbound Traffic based on static and dynamic policies: *provide directives to the TrGW*
- Selection of the TrGW to be used, based on the load of each TrGW.
- Prioritization, *based on directives from IBCF*.

7.2.2.4 New functions hosted by the TrGW:

- Media policing of Inbound/Outbound Traffic: *apply directives from the IBPCF*

7.2.2.5 Description

A new functional entity called Interconnection Border Policy Control Function (IBPCF) is added between the IBCF and the TrGW, terminating the the Ix reference point with the TrGW, as shown in Figure 7.2.2.5-1.

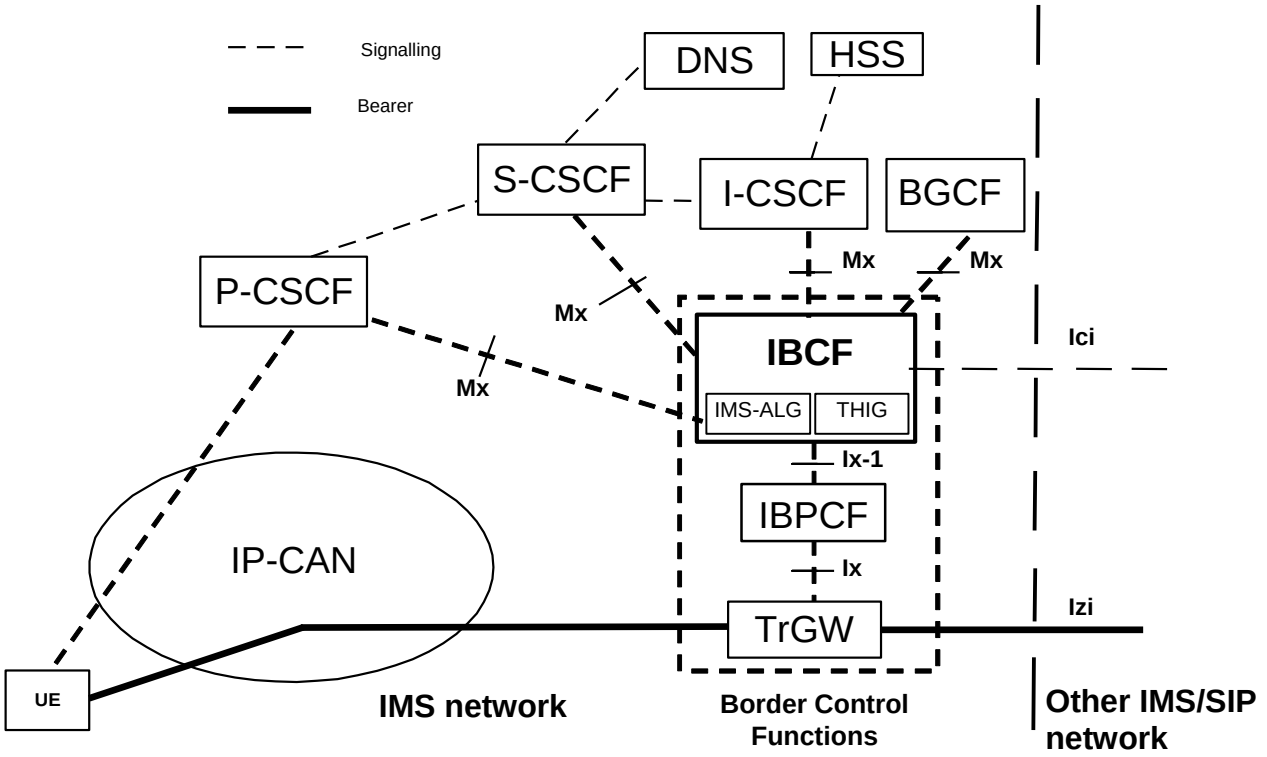

Figure 7.2.2.5-1: 3GPP IMS interconnection architecture with IBPCF for policy control

Editor's Note: The name Ix-1 is subject to re-consideration.

The IBPCF is responsible for mapping requests received from the IBCF on to configuration requests to be sent to the TrGW, taking into account operator-specific policy rules and inter-operator service level agreement (SLA) data.

It encompassed the following functions:

- Resource admission control;
- Policy control, providing directives to the TrGW for packet marking or media policing of Inbound/Outbound Traffic, based on static and dynamic policies;
- Selection of the TrGW to be used, based on the load of each TrGW;

7.2.2.6 Applicability to the simultaneous support of non-IMS traffic

The following figure depicts an example where the same interconnection is used for IMS traffic and non-IMS IP traffic (e.g. non-IMS voice over IP, Softswitch-based PSTN Emulation Subsystem), with policy control applied thanks to the IBPCF.

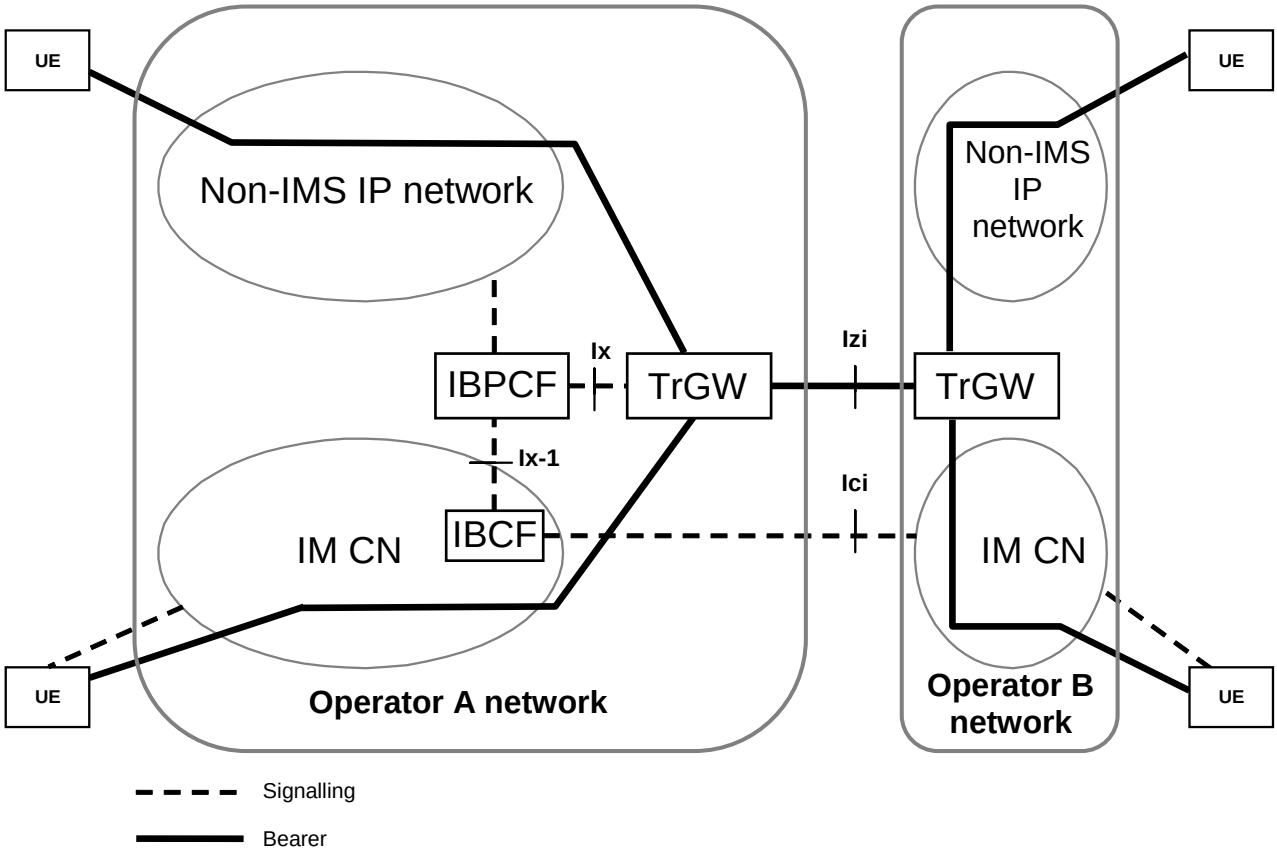

Figure 7.2.2.6-1: Common IP interconnection for IMS and non-IMS traffic under Alternative 2Editor's Note: Compatibility with CS CN and impact on CS CN needs to be further elaborated.

7.2.2.7 Information flow for media flow establishment

The following diagram provides a typical information flow for media flow establishment under this alternative.

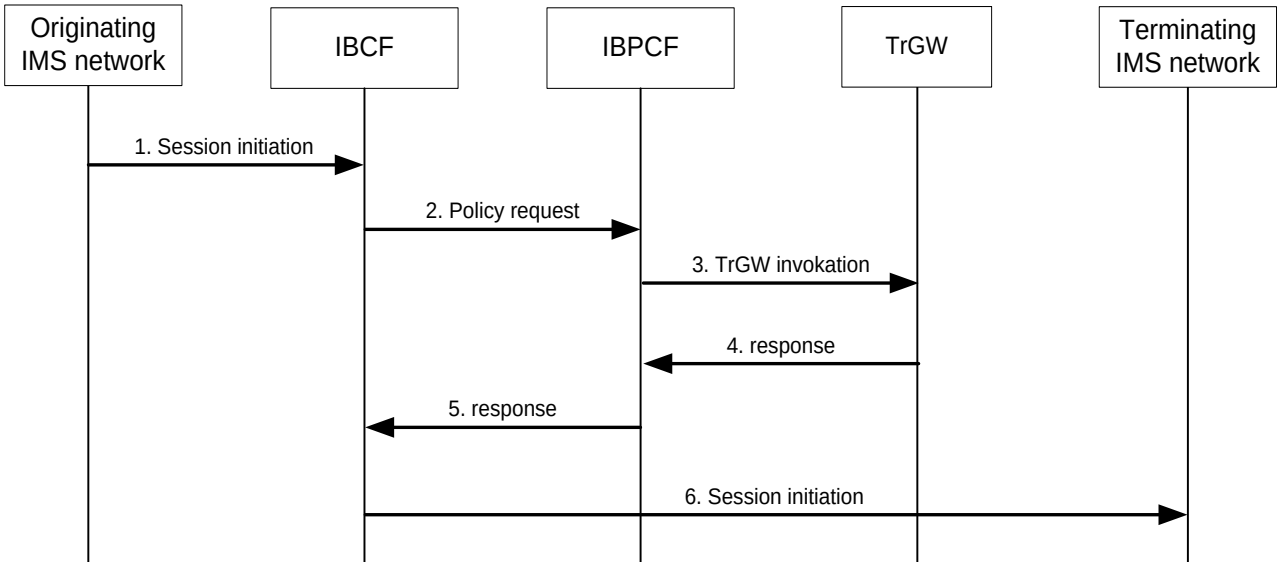

Figure 7.2.2.7-1: Information flow for media flow establishment under Alternative 2

7.2.3 Alternative 3: Addition of a functional entity for policy control without affecting existing reference points

7.2.3.1 Functional split

A new functional entity called Interconnection Border Policy Control Function (IBPCF) is added.

7.2.3.2 New functions hosted by the IBCF:

- IMS Emergency calls / Priority service support and handling.

7.2.3.3 Functions hosted by the IBPCF:

- Resource admission control
- Policy control.
- TrGW selection

7.2.3.4 New functions hosted by the TrGW:

- Media policing of Inbound/Outbound Traffic:

7.2.3.5 Description

A new functional entity called Interconnection Border Policy Control Function (IBPCF) as well as a new reference point R? between the IBCF and the IBPCF, as shown in Figure 7.2.3.5-1.

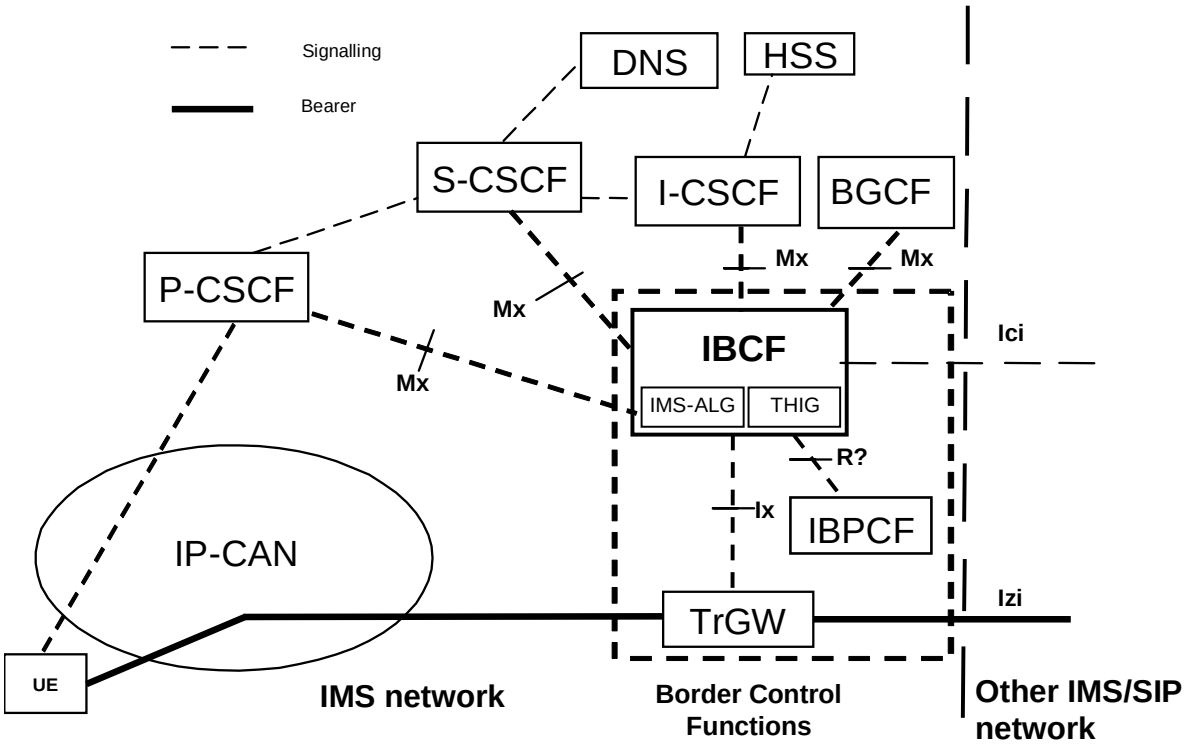

Figure 7.2.3.5-1: 3GPP IMS interconnection architecture with IBPCF for policy control

Editor's Note: The name R? is subject to re-consideration.

The IBPCF is responsible for policy decision for signalling and media sessions to other IMS/SIP networks. It acts on policy requests received over the R? reference point and returns policy decisions over the same reference point to the requestor, taking into account operator-specific policy rules and inter-operator service level agreement (SLA) data.

It encompassed the following functions:

- Resource admission control;
- Policy control, providing directives for packet marking or media policing of Inbound/Outbound Traffic, based on static and dynamic policies;

NOTE: The status and utilization of resources is out of scope for the IBPCF

7.2.3.6 Applicability to the simultaneous support of non-IMS traffic

Figure 7.2.3.6-1 depicts an example where the same interconnection is used for IMS traffic and non-IMS IP traffic (e.g. CS-CN), and how the Policy control functionality of the IBPCF could be applied also to the non-IMS IP traffic by extending the new reference point R? to the appropriate non-IMS control node.

This allows a consistent use of media QoS and other policies and a common resource allocation view for the IP-interconnects, while still not requiring any other changes to the control and user plane architectures for non-IMS.

NOTE: The R? for the non-IMS may require additional functions / policies not used by IMS.

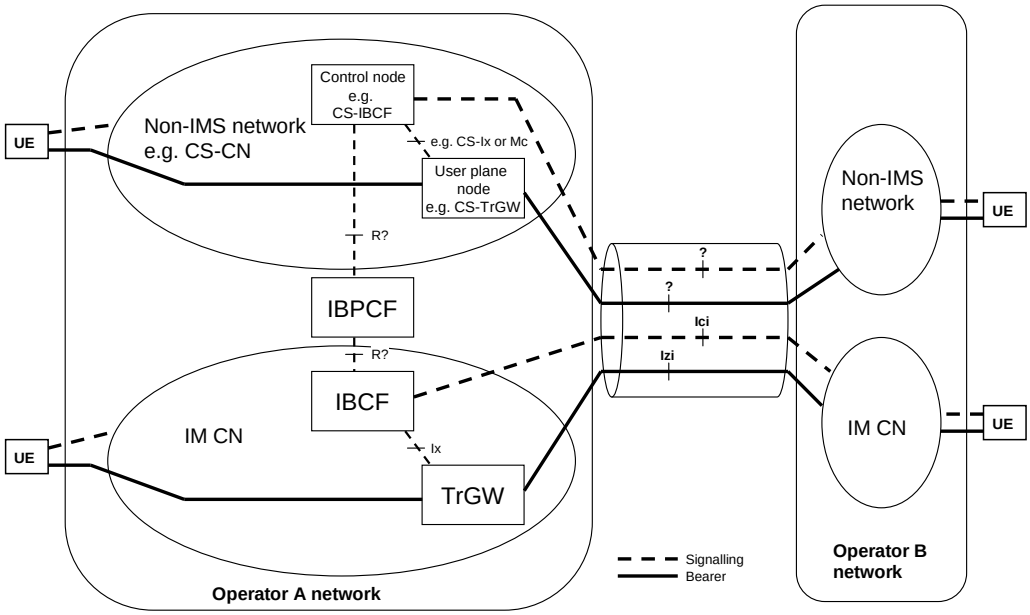

Figure 7.2.3.6-1: Common IP interconnection for IMS and non-IMS traffic under Alternative 3

7.2.3.7 Information flow for media flow establishment

The following diagram provides a typical information flow for media flow establishment under this alternative.

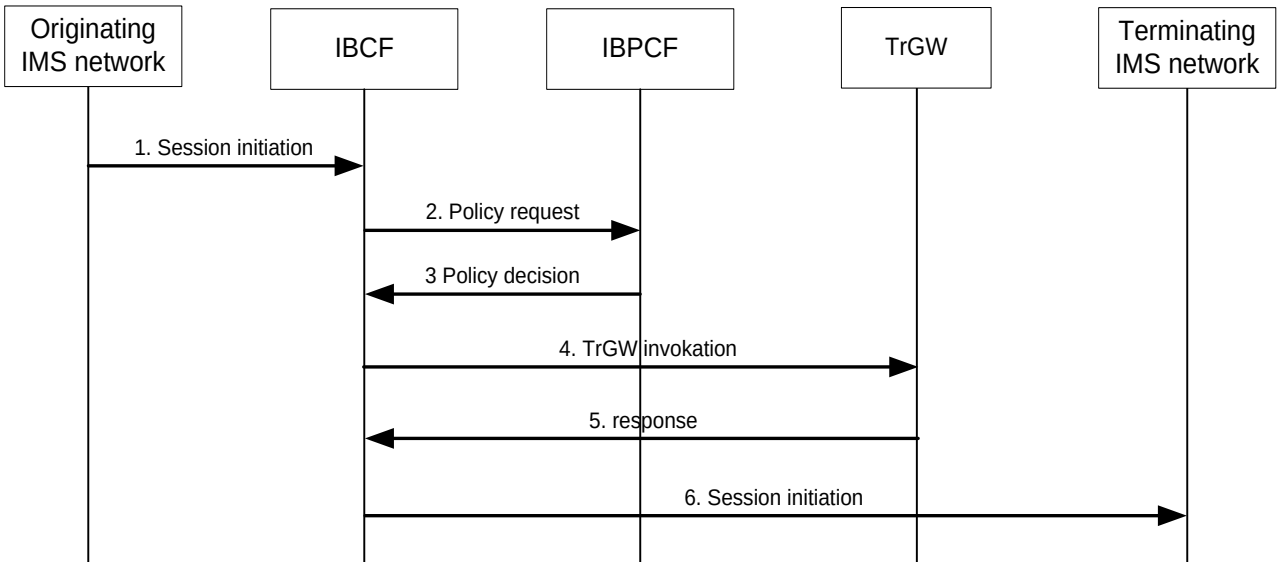

Figure 7.2.3.7-1: Information flow for media flow establishment under Alternative 3

8 Conclusions

Editor's note: This chapter to indicate consolidated functionalities needed and state the current impacted areas in order to identify future work –affected specs, normative work-.

Annex A:
NNI Policy Control Alternative comparison

Table X provides information for the identified candidate NNI Policy Control Alternatives with respect to functionality that can be provided and other key characteristics and aspects that may be important to consider when recommending an alternative.

Table X: Comparison between the different NNI Policy control alternatives

Function/characteristics	Alternative 1 Policy control in IBCF	Alternative 2 Policy control in new IBPCF between IBCF and TrGW	Alternative 3 Policy control in New IBPCF interfacing IBCF only
Functionality:			
NNI Resource allocation	Can have view of allocated resources that are available for a certain IBCF. May require partitioning of NNI resources between IBCF.	Yes, can have full view of allocated and available resource.	Yes can have full view of allocated and available resources.
Policy control	Can manage both media and call control policies.	Can manage both media and call control policies.	Can manage both media and call control policies.
QoS directives	Yes.	Yes from IBPCF.	Yes from IBPCF.
TrGW selection	Selected by IBCF.	Selected by IBPCF based on NNI selected by IBCF.	IBCF can select TrGW, where IBPCF may provide information affecting selection process. There is currently no defined interface or procedure for the admission control function to the transport/user plane and consequently it cannot be made aware of e.g. link failures.
Decisions making	Local decisions in IBCF/IBPCF	Possible to centralize decisions with IBPCF	Possible to centralize decisions with IBPCF
TrGW status	Monitored by IBCF.	Monitored by IBPCF.	Monitored by IBCF.
Signalling & Protocol aspects			
Protocol work needed	• No New Interface or protocols. Further enhancements may be needed. • All interactions between policy control and signalling over Ici/Mx and Ix are internal to IBCF.	• New Protocol between IBCF and IBPCF needed. • New stage 2 signalling procedures corresponding to 29.162 is needed to cover for new interactions in IBCF between SIP and the new Ix-1 Protocol, and for interactions in IBPCF between the New IX-1 and the Ix interfaces. • Introduction of new Functionality between IBCF and TrGW affect also the IBPCF.	• New protocol between IBCF and IBPCF is needed. • Stage 2 signalling procedures in 29.162 need be complemented to define interaction between SIP IX and the new R? protocol.
Signalling efficiency (number of additional signalling hops compared to today)	• No additional signalling "hops" compared to today.	• Two signalling hops added for policy control decisions. • No additional signalling hops for TrGW interactions when coordinated with Policy decision request. • Two more signalling hops needed for SIP related TrGW interaction when there	• Two additional signalling hops need for policy control decisions. • No additional signalling hops for TrGW interactions.

		is no need for new Policy decision. • No additional signalling hops for non-SIP related TrGW interaction form IBPCF (e.g., TrGW reselection after TrGW selection failure).	
Robustness			
IBCF Failure	All sessions establish via the failed IBCF are lost. Other IBCFs may be used to establish new session for same NNI. However NNI resources partitions dedicated to failed IBCF cannot be reused.	All sessions establish via the failed IBCF may be lost. If no session updates are done, the session may continue during a period of time. Other IBCF, may be used to establish new sessions for same NNI.	All sessions establish via the failed IBCF are lost. Other IBCF, may be used to establish new sessions for same NNI.
IBPCF Failure	Same as IBCF Failure.	All sessions established via the failed IBPCF may be lost. If no session updates are done, the session may continue during a period of time. New connections can be established using redundant IBPCF. May take some time before NNI resource status fully up to date.	Sessions established using failed IBPCF may still remain. However, IBCF may need to synchronize the events on Ix and R? reference points in case such failure occur (and provide roll back mechanism) New sessions can be established using redundant IBPCF. May take some time before NNI resource status fully up to date.
TrGW user plane link failure	The IBCF is aware of link failure and can update the available bandwidth.	The IBPCF is aware of link failure and can update the available bandwidth.	The IBPCF has no interface to the TrGW. It cannot be made aware of link failures except if the IBCF acts as a relay or if the IBPCF has other monitoring functionality. The IBCF is aware of link failure and may have to update the IBPCF.
IBCF control plane link failures	Reusing existing Ix procedures.	Reusing existing Ix procedures and requires similar procedures for Ix-1.	In case of failure of the R? interface, same procedure will apply as for IBPCF failure. In case of failure of the Ix interface, the IBCF may have to update the IBPCF.

Backward compatibility and service introduction			
Introduction of Policy control	• Upgrade of IBCF only to host Policy control functionality and execute policy decisions. • Existing Ix interface not affected, except for control of new functionality in TrGW. • TrGW not affected, except for new functionality in TrGW.	• Upgrade of IBCF access IBPCF over new interface instead of TrGW directly for Policy decisions and any TrGW interaction. • As exiting Ix interface is split to introduce IBPCF upgrade is more complicated. IBPCF need be act TrGW controller in parallel with IBCF before IBCF upgrade. • TrGW not affected, except for new functionality in TrGW, but IBPCF need to be configured in TrGW as controller prior to IBCF upgrade, and IBCF need to be removed as controller in TrGW after IBCF upgrade.	• Upgrade of IBCF to access IBPCF over new interface for policy decisions. • Existing Ix interface not affected, except for control of new functionality in TrGW. • TrGW not affected, except for new functionality in TrGW.
Architecture Aspects			
Basic	Existing FEs are used	New FE IBPCF required	New FE IBPCF required
Applicability for non-IMS	Not applicable	IBPCF may be used as a policy control platform serving both IMS and non-IMS	IBPCF may be used as a policy control platform serving both IMS and non-IMS
Architecture agility	Policy control functions need to be embedded in the IBCF, in addition to the normal SIP call control logic.	The IBPCF can be implemented as a stand alone node or co-located with the IBCF or the TrGW.	The IBPCF can be implemented as a stand alone node or co-located with the IBCF.
Compatibility with current IBCF specifications	Same as Rel-9.	Aligned with the architecture specified in TS 23.517.	Aligned with TS 23.238.
Applicability for non-IMS	Not applicable	Allows introduction of Policy control to non-IMS. May require further changes to the non-IMS architecture as the introduction of the IBPCF requires a split of the Interfaces between user plane and control plane nodes.	Allows introduction of Policy control to non-IMS without requiring any other architectural changes than Introduction the IBPCF and the R? reference point.

Annex <X>: Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
16/10/2008					TR Skeleton and Scope (S2-086965)	-	0.0.0
27/10/2008					Added agreed text of S2-086966, S2-087207 and S2-087216	0.0.0	0.1.0
03/12/2008					Added agreed text of S2-087899, S2-087901, S2-087902, S2-087903, S2-087904 and S2-088309	0.1.0	0.2.0
01/16/2009					Merged agreed tdocs S2-090260, 090439, 090259	0.2.0	0.3.0
2/20/2009			S2-091400		Revision of: Revised Text for TR 23.848	0.3.0	0.4.0
2/20/2009			S2-091401		Revision of: Outbound Session spacing	0.3.0	0.4.0
2/20/2009			S2-091437		Revision of: Revision of: Architectures for IMS Border Functions	0.3.0	0.4.0
2/20/2009			S2-091216		Discussion paper on the storage of ACL	0.3.0	0.4.0
2/20/2009			S2-091403		Revision of: Policy control and resource admission at the IMS border segment	0.3.0	0.4.0
2/20/2009			S2-090927		IMS border access control	0.3.0	0.4.0
4/4/09			S2-092028		Editorial Corrections	0.4.0	0.5.0
4/4/09			S2-092558		Revision of: Clarification of overload control function	0.4.0	0.5.0
4/4/09			S2-092559		Revision of: Definition of ACL filter and ACL profile	0.4.0	0.5.0
4/4/09			S2-092560		Revision of: Restructuring of ACL Management clause	0.4.0	0.5.0
4/4/09			S2-092561		Revision of: Policy and resource control at NNI	0.4.0	0.5.0
4/4/09			S2-092286		Resolving Editor's Notes in clause 7.2 (Policy Control related features)	0.4.0	0.5.0
9/4/09			S2-095643		Role of IBCF for enabling LBO	0.5.0	0.6.0
11/21/2009			S2-097143		Policy Control at the interconnection	0.6.0	0.7.0
11/21/2009			S2-097144		Policy and resource control at NNI	0.6.0	0.7.0
11/21/2009			S2-097145		Enhancement of border architecture to improve end to end voice quality	0.6.0	0.7.0
01/22/2010			S2-100613		Comparison of different NNI policy control Alternatives	0.7.0	0.8.0
01/22/2010			S2-100614		Policy control at the interconnection	0.7.0	0.8.0
01/22/2010			S2-100614		Policy control at the interconnection – errata (missing 4th change)	0.8.0	0.8.1
02/22/2010			S2-101524		Merge of Evaluation Comparison information for NNI policy control	0.8.1	0.9.0
02/22/2010			S2-101525		Assessment of alternatives for Policy control at the interconnection	0.8.1	0.9.0
02/22/2010			S2-101526		Applicability to non-IMS for Policy Control alternative 3	0.8.1	0.9.0