ERICSSON

SmartEdge Border Gateway Function

FUNCTION SURVEY

155 13-CRA 119 1170/1 Uen J

Contents

1	**General Information**	**1**
1.1	Scope	1
1.2	Audience	1
1.3	Terminology	1
1.4	Abbreviations	5
2	**Overview**	**9**
2.1	Border Gateway Function in IMS Networks	9
3	**Border Gateway Functions**	**11**
3.1	Media Flow Gating	11
3.2	Network Address and Port Translation	11
3.3	Topology Hiding Applied to Media	11
3.4	Realm Availability Detection	12
3.5	Hosted NAT/FW Traversal	12
3.6	Media Source Filtering	13
3.7	DiffServ Enforcement and QoS	13
3.8	QoS Address Handling	13
3.9	Bandwidth Policing	14
3.10	Stream Admission Control	15
3.11	Stream Mode Enforcement	15
3.12	Media Inactivity Supervision	15
3.13	Detection of Hanging Terminations	17
3.14	Early Media	17
3.15	TCP-Based Media	17
3.16	RTP/RTCP-Based Media	17
3.17	H.248 Reported Statistics	19
3.18	Emergency Call Support	21
3.19	Network Security	21
3.20	High Availability	22
3.21	Overload Protection	23
3.22	BGF Counters	23
3.23	Alarms	23
3.24	Error Handling	24

3.25	IPV6 Support	24
3.26	Autonomous Pinhole Closing	28
3.27	KeepActive Flag	28
3.28	MSRP Support	28
3.29	Secure RTP Support	29
3.30	ICMP Error Handling	29
3.31	Optimized BGF Selection	30
3.32	Globally Unique MID	30
3.33	Media Plane Redundancy	30
3.34	BGF Statistics through Bulkstats	31
4	**Command-Line Interface**	**33**
4.1	Command Mode Hierarchy	33
5	**H.248 Signaling Support**	**39**
Reference List		**41**

1 General Information

1.1 Scope

This is a high-level description of the Border Gateway Function (BGF) in the SmartEdge 11.1.1 release. The description explains various functions provided by the SmartEdge BGF.

1.2 Audience

This description is intended for the following audience:

- Operator, system, and network administrators experienced in access and internetwork administration.
- Ericsson sales support, product management, system management, implementation engineers, and Global Services.
- Others seeking a high-level technical description of the functions provided by the BGF.

The user should have a general understanding of the concepts and requirements of telecommunication systems and Internet protocols-for example, Internet Protocol (IP), Real-time Transport Protocol (RTP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

The user should also have a general knowledge of the IP Multimedia Subsystem (IMS) standard, as well as networks that use ITU-T H.248 Media Gateway Control for establishing media sessions.

1.3 Terminology

Access Application Level Gateway
: Session Initiation Protocol (SIP) Back-to-Back User Agent (B2BUA) placed between User Equipment (UE) and an external Proxy-Call Session Control Function (P-CSCF) offloading the IMS core network by providing parts of the P-CSCF functions as well as a number of additional services.

Access Network
: Fixed broadband access network to which residential and enterprise users with SIP equipment as well as SIP and H.323 IP-PBXes are connected. Private overlapping address spaces may be used in access networks. In the present document, the term **Access Network** also includes aggregation networks.

Back-to-Back User Agent

In the Session Border Gateway (SBG) architecture, the term for the function which terminates SIP signaling from one network and, after modifying incoming messages, originates signaling to another network. The B2BUA function also performs media anchoring and controls the dynamic pinhole firewall.

Border Gateway Function

A packet-to-packet gateway providing dynamic pinhole firewall functionality for media plane traffic. Defined by TISPAN in ETSI ES 282 003: “Resource and Admission Control Sub-system (RACS); Functional Architecture”, Reference [6]

Core network

Central part of a multimedia network including, for example, databases, SIP servers, media servers, and media gateways. Compare with **IMS Core Network**

Dynamic pinhole firewall

SBG term for the function which opens and closes pinholes for media (audio, video, fax, and so on over IP) under control of a B2BUA on a per-media-stream basis. This process is known as **Media flow gating**

Early media

According to RFC 3959: “The Early Session Disposition Type for the Session Initiation Protocol (SIP)”, Reference [7]: “Early media refers to media (for example, audio and video) that is exchanged before a particular session is accepted by the called user. Within a dialog, early media occurs from the moment the initial INVITE is sent until the User Agent Server (UAS) generates a final response. It may be unidirectional or bidirectional, and can be generated by the caller, the callee, or both. Typical examples of early media generated by the callee are ringing tone and announcements (for example, queuing status). Early media generated by the caller typically consists of voice commands or Dual Tone Multi-Frequency (DTMF) tones to drive Interactive Voice Response (IVR) systems”.

Foreign network

Another network portion within a carrier's network or another carrier’s network. The foreign network can either be a trusted SIP network, an untrusted SIP network, or an H.323 network.

IMS core network

The central part of the IMS network architecture including, for example, databases (HSS), SIP call/session servers (CSCF), application servers (AS), media resource functions (MRFC and MRFP), and PSTN gateways. An IMS core network is typically separated from access networks (where users reside) and other operator's IP multimedia networks by means of an SBG.

Interconnection Border Control Function

Controls SIP traffic between the **IMS core network** and **foreign networks**. Defined by TISPAN in ETSI ES 283 003: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]", Reference [8] and 3GPP in "3GPP TS 24.229: Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 7)", Reference [9].

Latching

A method to obtain the IP address and port used by the NAT on behalf of a user behind the NAT. The source address and port of the first packet received from that user is used for sending packets to the user and for the dynamic pinhole firewall when accepting packets from that user.

Media

IP traffic containing audio, video, fax, and so on. Some packets not containing actual payload (for example, RTCP packets or TCP segments for connection establishment) are also considered media since they are prerequisites for, or closely coupled to, the payload.

Media anchoring

Forcing media to take a certain path by altering source or destination address and port in SDP or OLC in H.245. In the SBG, this is done by the B2BUA which forces the media streams to pass the media pinhole firewall.

Media flow gating

The process of the SBG opening and closing pinholes for media (audio, video, fax, and so on, over IP) on a per-media-stream basis. The media part of the function performing this task is known as **dynamic pinhole firewall**.

Media plane

In this document, the media plane refers to the traffic between users or IMS core network nodes containing media.

Pinhole
A set of criteria defining a media stream which is let through the dynamic pinhole firewall. The criteria include local IP address and port, direction of media, and transport protocol, and may include remote IP address and port for media source filtering and bandwidth for policing.

Service-based Policy Decision Function
A function that decides which media streams are allowed to be set up and the characteristics of the streams. The function requests need resources from media plane entities. Defined by TISPAN in ETSI ES 282 003: “Resource and Admission Control Sub-system (RACS); Functional Architecture”, Reference [6]. The SmartEdge Border Gateway Function (BGF) is controlled by the SPDF entity in the Session Gateway Controller (SGC).

Session Border Gateway
Ericsson IS-based product that acts as a gateway between IP Multimedia networks. The SBG ensures security, topology hiding, quality of service, service level agreements, NAT/FW traversal, address translation, and other critical functions for real-time IP streams. The SBG consists of IS application blade systems SGC and Media Proxy(MP).

Session Gateway Controller
An IS application blade system containing the B2BUA function and optionally the SIP/H.323 inter-working function of the SBG. The SGC contains the SPDF which controls the BGF.

Topology hiding
A way to prevent all information regarding IP addresses used in one network from being forwarded in signaling messages to another network.

User
Any entity (for example, a person) that uses IMS features through User Equipment (UE). The term user is sometimes also used in a little wider meaning, including both the UE and the entity using the services.

User Equipment
A device allowing a user access to network services. Defined in 3GPP TR 21.905: “Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications”, Reference [10].

1.4 Abbreviations

3GPP	3rd Generation Partnership Project
A-ALG	Access Application Level Gateway
AS	Application Server
B2BUA	Back-to-Back User Agent
BFD	Bidirectional Forwarding Detection
BGF	Border Gateway Function
BRAS	Broadband Remote Access Server
C-BGF	Core Border Gateway Function
CLI	Command Line Interface
CSCF	Call Session Control Function
D-SBC	Distributed SBC
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DTMF	Dual Tone Multi-Frequency
ETSI	European Telecommunications Standards Institute
FW	Firewall
HNT	Hosted NAT/FW Traversal
HSS	Home Subscriber Server
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-PBX	IP Private Branch Exchange
IS	Integrated Site
ITU-T	International Telecommunication Union Telecommunication Standardization Sector

IVR	Interactive Voice Response
MG	Media Gateway
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSRP	Message Session Relay Protocol
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NW	Network
OLC	Open Logical Channel
OS	Operating System
P-CSCF	Proxy CSCF
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
RTCP	RTP Control Protocol
RTP	Real Time Protocol
SBC	Session Border Controller
SBG	Session Border Gateway
SCTP	Stream Control Transport Protocol
SDP	Session Description Protocol
SE	SmartEdge
SGC	Session Gateway Controller
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SME	Small Medium Enterprise
SPDF	Service Policy Decision Function

srTCM	single rate Three Color Marker
TACACS+	Terminal Access Control Access Control System Plus
TCP	Transport Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
UAS	User Agent Server
UDP	User Datagram Protocol
UDPTL	UDP Transport Layer
UE	User Equipment
vMG	Virtual MG
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

2 Overview

2.1 Border Gateway Function in IMS Networks

Border Gateway Function (BGF) functionality enables the SmartEdge router to be a session-aware device that provides security, and service assurance, for multimedia telephony traffic such as voice, video, and Multimedia Messaging.

Unlike traditional Public Switched Telephone Network (PSTN) services, which operate using a closed network, multimedia telephony services are typically based on an open IP-based network architecture. A BGF is a packet-to-packet gateway for multimedia user plane traffic which sits at the border of an IP-to-IP network (for example, between a service provider and a subscriber, two service providers, or the access and the core network of a service provider) and manages the flow of session information across the border. The BGF provides functions which allow the operator to protect its network so that only traffic agreed on in the control plane is gated through the BGF. The BGF also provides Hosted NAT/FW Traversal (HNT), IPV6-to-IPV4 (and vice versa) protocol translations, collects statistics related to media, and supervises activity of the established media streams, and so on.

Service assurance on the SmartEdge router is provided by consolidating the BGF services with other capabilities on the SmartEdge router—such as general network security, subscriber awareness, flow-based forwarding architecture, edge routing and Virtual Private Network (VPN) functions, and advanced Quality of Service (QoS) functionality. In this way, the SmartEdge router can provide an integration of services, delivering multimedia services end-to-end with quality, security, and reliability, while enforcing Service Level Agreements (SLAs).

Within the Ericsson IP Multimedia Subsystem (IMS) network solution, the SmartEdge router can help provide a common system enabling operators and service providers to reduce costs and leverage on their legacy networks. In this capacity, the Ericsson Session Border Gateway (SBG) and the SmartEdge BGF forms the Ericsson Distributed Session Border Controller (D-SBC) in which the SBG controls the BGF.

IMS is an architectural framework that is designed to deliver IP Multimedia Services to end users, aiding in accessing multimedia and voice applications.

For call control, an IMS network utilizes standard signaling protocols, one of which is H.248. The SmartEdge BGF supports ITU-T H.248, an open-standard signaling protocol for media gateway control.

The D-SBC can also be used in multimedia or VoIP networks other than IMS. The D-SBC provides the same functions in other networks as in IMS.

Figure 1 shows the logical position of the BGF in an IMS or other multimedia network, and Figure 2 shows an example of how this may be realized when

a SmartEdge BRAS is reused as BGF. The SGC in the SBG acts as SPDF and controls the BGF.

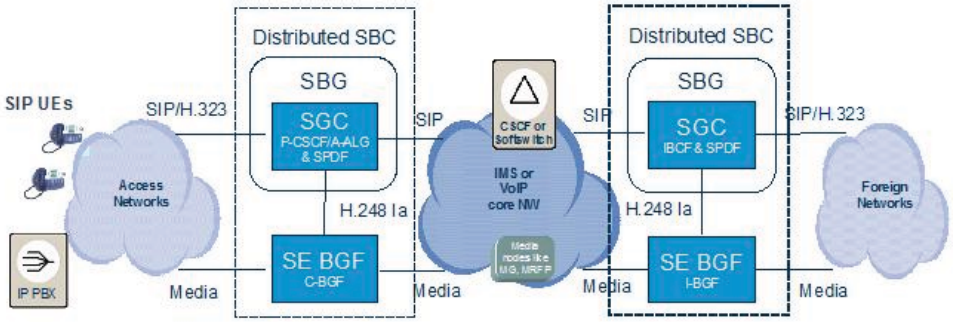

Figure 1 Logical Position of D-SBC and BGF in IMS or Other Multimedia Networks

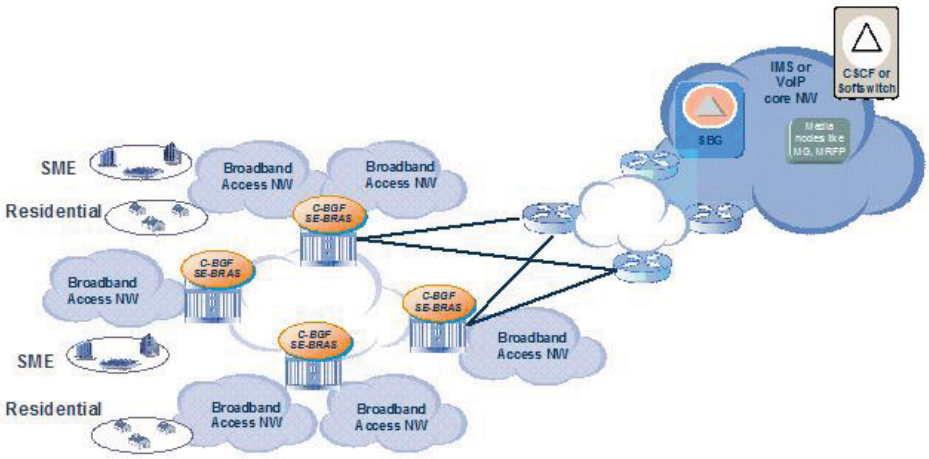

Figure 2 Example Network with SmartEdge Router Deployed as Both BRAS and C-BGF

3 Border Gateway Functions

The SmartEdge router is a full-featured multiservice network device. It has a rich set of features that can apply to BGF as well as specific features dedicated for BGF. The following sections describe the features of the BGF.

3.1 Media Flow Gating

To protect the IMS core network from media fraud, the SPDF specifies to the BGF which streams are allowed to pass through the dynamic pinhole firewall and which pinhole criteria are valid per stream.

The BGF allocates the IP address and port number to be used. The SPDF specifies the transport protocol, direction of media, and source filtering parameters to be used. To avoid possible media from an already terminated call to flow through new calls, the used ports are quarantined for a certain amount of time before they are used in new calls. To increase the capacity when there is a high volume of calls, such quarantined ports are used if all free ports are in use.

The BGF only accepts TCP and UDP as transport protocols for media.

3.2 Network Address and Port Translation

The BGF supports NAPT and media bridging by translating IP addresses and UDP or TCP ports from one network to another. The networks may use overlapping address spaces.

Both the IP source and destination addresses and ports in the TCP or UDP headers are translated. For TCP and UDP sessions, modifications include an update of the checksums in the IP and TCP or UDP headers. TCP and UDP protocol checksums are not validated.

The source IP address, UDP port, and TCP port of the received media packets are provided to the BGF by the SPDF or obtained by latching. When source filtering is enabled, the source IP address, UDP port, and TCP port of the received packet are validated against the expected ones.

Transmitted media packets will have the remote destination IP address, UDP port, and TCP port either provided by the SPDF or obtained by latching.

3.3 Topology Hiding Applied to Media

By performing NAPT as described above, the BGF prevents leakage of address information from the core network into untrusted access or foreign networks. Also the TTL or hop-limit value in all media IP packets is reset to 255 as part of

the topology-hiding function in the BGF. This feature prevents information about the core nodes and core network topology from being passed to unauthorized users and thereby reduces the risk of attacks.

3.4 Realm Availability Detection

Media flow gating, NAPT, and topology hiding are all features relying on the concept of separate logical networks. The BGF supports separate logical networks and ties those to separate realms in communication with the SPDF. For the SPDF to have awareness of which realms are configured on a specific BGF, the BGF allows the SPDF to automatically audit the set of available realms, and the BGF notifies the SPDF when the set of configured realms is changed.

3.5 Hosted NAT/FW Traversal

Sending media from the BGF to the address and port agreed between the user and the SPDF using SDP is not possible when a NAT/FW is placed between the BGF and the user. In these cases, the BGF will instead set the destination address and port to the source address and port of the first packet received on the BGF local destination address and port reserved for the stream. Setting the destination address and port criteria in the BGF by using the first received packet is known as latching. When the first packet is received, the BGF will also set its pinhole filter according to the source address and port of this first packet.

When setting up media streams through the BGF to a user behind a remote NAT/FW, the BGF expects the SPDF to explicitly order the BGF to perform latching.

In some cases, for example, depending on session scenario the following occurs:

- The SPDF instructs the BGF to perform a new latch, which means that the BGF pinhole is locked to the source address and port of the next incoming packet.
- The SPDF may also instruct the BGF to perform a relatch, however, the SmartEdge BGF does not distinguish between latch and relatch commands and applies latching functionality at a relatch request.

The BGF supports HNT for UDP-based traffic (such as RTP/RTCP). The BGF also supports HNT for TCP, but if both users are behind a NAT/FW, the NAT/FW has to comply with RCF 5382: NAT Behavioral Requirements for TCPReference [12]. In the case of HNT for TCP, the BGF expects the SPDF to explicitly order latching.

Note that NAT/FW traversal and latching is generally not required for non-TCP IPv6 traffic, but BGF supports latching for all IPv6 media traffic if instructed to do so by SGC.

3.6 Media Source Filtering

The BGF allows media source filtering for a pinhole based on the originating IP address and port information.

Media source filtering is controlled through H.248, and has the following options:

- No media source filtering
- Only media source address filtering
- Media source address and port filtering

Packets that do not match the filter are discarded.

3.7 DiffServ Enforcement and QoS

The SPDF specifies to the BGF which DSCP (DiffServ Code Point) to be set per outgoing media stream. This allows the operator to be in control of media plane traffic prioritization.

As a full-featured networking device, the SmartEdge router also supports standard Quality of Service (QoS) functions such as the following:

- Scheduling
- Packet classification
- Ratelimiting

The SmartEdge router can classify and rate-limit incoming packets according to priority groups, policy access control groups, and QoS policing and metering policies, independent of the BGF functionality. Rate limiting is not performed on a per-media stream basis. The SmartEdge router can also be configured with specific mapping of egress P-bit setting dependent on the egress DSCP value.

3.8 QoS Address Handling

The BGF allows configuration of media address groups based on a specified DSCP range value. Each media local interface configured under the realm can be attached to these newly configured groups. Two media address groups are supported.

The following rules apply when an IP address is selected for a new call:

- If the DSCP value specified in the signaling is within the range of a user-configured media address group, a port will be allocated from IPs that match the realm, media address group, and the address family (IPv4 or IPv6). If none of the ports are free, the call is rejected with error code 510.

- If the DSCP value specified in the signaling is not in any of the user-configured media address groups, a port will be allocated from IP addresses that match the realm default media address group and the address family. If none of the ports are free, the call is rejected with error code 510.
- If the DSCP value is not specified in the signaling, the configured default DSCP value is used to select the media address group. The port is selected based on the criteria mentioned above.
- If the DSCP value is not specified in signaling and no default DSCP value is configured, the BGF will try to allocate a port from any IP address configured that matches the realm and the address family. If none of the ports are free, the call is rejected with error code 510.
- The overriding option of the DSCP CLI will not affect the address selection.
- If no IP addresses are configured for the BE group, the IP addresses from the QoS group shall serve both BE streams and QoS streams; the opposite is also true.
- Modification of the DSCP after address selection has no impact on address selection.

3.9 Bandwidth Policing

The BGF can perform bandwidth policing on ingress traffic per established media stream. For each stream the SPDF sends all bandwidth policing parameters to the BGF. This feature allows the SPDF to control the bandwidth usage per stream.

Only SDR (Sustained Data Rate) and MBS (Maximum Burst Size) parameters are used. The PDR (Peak Data Rate) parameter is ignored. Packets exceeding the policing level will be dropped and counted. No DSCP marking will be done.

The bandwidth policing also includes any associated RTCP streams. The percentage of RTCP ingress traffic is controlled by the SPDF. If no such parameter is given by the SPDF, a configured value is used. The default value for the percentage of RTCP traffic is set to 5% of the RTP traffic.

The bandwidth policing algorithm is based on RFC 2697, srTCM (single rate Three Color Marker); refer to RFC 2697: A Single Rate Three Color Marker , Reference [11]. The packets are classified according to the RFC and packets classified as red are dropped. Any other color is forwarded but no color marking is done.

The existing circuit level rate control on the SmartEdge router can be utilized in combination with the dynamically enabled bandwidth policing for media streams. In such a case, the circuit level rate limits are applied first.

3.10 Stream Admission Control

Stream admission control or the bandwidth Connection Admission Control (CAC) gives the operator control over the bandwidth usage on a per-realm basis. Different bandwidth values for the ingress and egress direction can be configured. Calls are admitted until the total bandwidth usage exceeds the configured maximum value for the realm in either direction. The calls are rejected until enough bandwidth is available again. All bandwidth increase requests for a stream will be rejected if the bandwidth limit for the realm is achieved. When the bandwidth limits are changed, existing calls are not affected, but new calls will be subject to the new limits.

The bandwidth usage per stream is given by the SPDF in the add/modify request. If no such parameter is given, the SDR value is used. If neither value is available, the call will be accepted without affecting the total bandwidth in use.

A percentage of the bandwidth per realm can be reserved for emergency calls, for information see Section 3.18 on page 21.

3.11 Stream Mode Enforcement

The stream mode is a method the SPDF uses to control the traffic flow per stream end-point. It is set by the stream mode property. The total flow depends on the stream mode for both terminations. The function has four possible modes which can be set on each stream on each terminaton: *Inactive*, *ReceiveOnly*, *SendOnly*, and *SendReceive*. The stream mode enforcement in the BGF is in accordance with the H.248.1 definition.

Some media streams cannot utilize all stream mode property values, or they do not apply to all layers of the protocol stack. The SPDF always sets the stream mode property to *Inactive* or *SendReceive* for media streams using TCP or UDPTL as transport type.

Forwarding of RTCP packets for associated RTP streams is handled separately and is described in Section 3.16.2 on page 18.

For TCP/MSRP messages such as TCP control messages, bodiless SEND, REPORT and 200 OK are allowed regardless of the stream mode. This allows clients to keep the NAT pinhole open and maintain compliance with MSRP RFC 4975.

3.12 Media Inactivity Supervision

An unexpected break in connectivity anywhere in the network or another unusual situation could result in multimedia calls being disconnected but not released through control signaling. The BGF detects such a situation and reports it to the SPDF for appropriate action. The media flow can be supervised on termination level in the BGF. A media inactivity notification is sent to the SPDF through H.248 if no media (including RTCP) has been received from

any side for any stream in the session within the specified time period. This time period can be defined per realm.

The notification is sent repeatedly after each time period as long as the criteria above are fulfilled.

If media is inactive on a stream or if there is a termination, the BGF reports the inactivity to the SGC along with the time of the occurrence, thereby allowing more accurate billing for the user. The media inactivity timestamp is passed from the BGF to the SGC using the new optional statistics parameter “eri_seco/mstime” defined in the eri_seco package, version 5. The BGF includes the media inactivity timestamp in the H.248 Subtract reply message, unless the SGC has included an empty statistics descriptor in the Subtract request. The BGF also includes a media inactivity timestamp in the H.248 Modify reply message if the SGC included an audit statistics descriptor in the Modify request message. If a stream or termination is deleted, the timestamp for each termination is reported independently.

The BGF reports the media inactivity timestamp at the granularity of 1 second using the Coordinated Universal Time (UTC) format (yyyymmddThhmmssssZ). For example, eri_seco/mstime = 20100706T17231200Z. The last two *s*’s in the string represent milliseconds, which the BGF populates with 00 because it does not report at this level of granularity. A null value in the UTC format is “00000000T00000000Z”. The BGF sets the timestamp to the null value if the following conditions are met based on the eri_seco package description:

- No media stop event occurred during the given reporting time.
- The SGC did not order a media stop event, or the SGC turned off the media stop event during the call.
- Media is temporarily stopped and then restarted during the session.

For each stream with a media stop event, the BGF stores the associated inactivity timestamp and also sends it to the SGC. The SGC selects the relevant timestamp among the reported inactivity timestamps. The “show media-gateway media-flow detail” command now includes a Media Stop Time field that provides a timestamp at which the most recent media stop event occurred on the stream.

You can configure the media inactivity supervision time period in the BGF per virtual media gateway (vMG), from 10 seconds up to 24 hours. If the SPDF specifies the supervision time and orders supervision on both terminations in a context, it sets the time on both terminations. If the supervision time period differs for the terminations, the smaller time period is chosen and applied to both terminations.

The SPDF specifies whether media inactivity is detected in only one or both directions on a termination. The BGF translates this internally to perform the detection on ingress on each termination without considering the stream mode settings.

The SPDF releases the related BGF resources when the SPDF is notified of the media stop event.

3.13 Detection of Hanging Terminations

The hangterm package is implemented according to the standard H248.36. When the hangterm/thb is enabled on a termination, a timer is started when the SPDF sends a hangterm/thb event in the event descriptor of that termination. When the timer expires, an event notification is sent to the SPDF. If the termination is considered to be unused or unknown to the SPDF, it will be deleted.

The timer value can be given by the SPDF in the hangterm/thb event or if it is missing, a configured value will be used. The range for the configured default timer value is 0-86400 seconds with an initial default value of 3600. The value 0 will disable the hangterm detection for that specific termination.

The timer will be restarted for every Modify command on the termination and also after every expiration event notification sent to the SPDF. The granularity of the timer is 300 seconds.

3.14 Early Media

Early media is the term for media exchanged between users before 200 OK has been sent on the SIP level. On the media plane, this corresponds to requests from the SPDF for opening pinholes in the BGF before all information of the stream is known to the BGF. For example, media may be sent one-way through the BGF when the source of the media is not yet known to the BGF. Early media can also be set up by the SPDF on the media plane with no differences compared to normal media.

3.15 TCP-Based Media

The BGF supports TCP-based media with the same features as UDP-based media except for HNT. TCP-based media cannot re-use local ports used by UDP traffic.

3.16 RTP/RTCP-Based Media

The BGF handles RTP media traffic. The RTP protocol fields padding, extension field, Contributing Source Count, marker field, payload type, and timestamp are ignored for received packets and forwarded unchanged.

3.16.1 UDP Port Usage for RTP and RTCP

RTP is layered over UDP. An even UDP port number is assigned to each RTP stream. For each RTP stream, there may be an associated RTCP stream on the subsequent odd port number.

This even and odd UDP port numbering for RTP and RTCP is encouraged by the RTP protocol standard. However, it cannot be assumed that incoming RTP and RTCP streams follow this convention for the UDP source ports.

The BGF will always allocate consecutive UDP port numbers for RTP and RTCP.

The UDP port range used for RTP and RTCP is between 16384 and 32768, but can be extended to 49152.

3.16.2 RTCP Handling

Forwarding of RTCP packets in the BGF is dependent on instructions from SPDF.

The SPDF orders the BGF to either assign or not assign an RTCP port for each RTP stream:

- Off: An RTCP port will not be allocated in the BGF for the RTP media streams for the indicated network. All received RTCP packets will be dropped.

- On: An RTCP port will be allocated in the BGF, for each RTP media stream on the indicated network. The RTCP port allocated in the BGF is the RTP port +1. If the remote end point uses non-standard RTCP ports, the SPDF can give the remote RTCP port information through SDP to the BGF.

Forwarding of received RTCP traffic can have five different behaviors on each termination for an RTP stream, as per the order from SPDF, see Table 1. The resulting action is a combination of the RTCP port allocation and mode on both terminations.

Table 1 Actions per stream and termination as a result of RTCP port allocation and RTCP mode

RTCP Port Allocation	RTCP Mode	Action
Off	Any	Ingress RTCP packets are discarded. Egress RTCP packets from the other termination are discarded.

RTCP Port Allocation	RTCP Mode	Action
On	Inactive	Ingress RTCP packets are discarded. Egress RTCP packets from the other termination are discarded.
On	Send-only	Ingress RTCP packets are discarded. Egress RTCP packets from the other termination are sent.
On	Receive-only	Ingress RTCP packets are sent to other termination. Egress RTCP packets from the other termination are discarded.
On	Send-receive	Ingress RTCP packets are sent to other termination. Egress RTCP packets from the other termination are sent.

Note: Forwarding of RTCP is not affected by the stream mode.

3.17 H.248 Reported Statistics

The BGF collects a set of statistics in each termination for each stream. If the SPDF requests the statistics, they are reported when the stream is removed. BGF collects the following statistics:

- Duration (nt/dur)
- Octets Sent (nt/os)
- Octets Received (nt/or)
- Discarded Packet (gm/dp)
- Packets Sent (rtp/ps)
- Packets Received (rtp/pr)
- Discarded Octets (eri_seco/do)
- Discarded Packets–Policing (eri_seco/dpp)
- Discarded Octets–Policing (eri_seco/dop)

- RTCP Reported Average Jitter (eri_seco/rraj)
- RTCP Reported Packets Lost (eri_seco/rrpl)
- Media Inactivity Timestamp (eri_seco/mstime)
- Accepted MSRP Chunks (eri_seco/amc)
- Discarded MSRP Chunks (eri_seco/dmc)
- Number of Replayed Packets (srtp/replay)
- Number of Authentication Failures (srtp/authfail)
- Sent SRTP Packets Protected by Master Key (srtp/srpk)
- Sent SRTCP Packets Protected by Master Key (srtp/scpk)
- Received SRTP Packets Protected by Master Key (srtp/rrpk)
- Received SRTCP Packets Protected by Master Key (srtp/rcpk)

The statistics indicated as nt, gm, or rtp are according to the corresponding H.248 packages described in ITU-T Recommendation H.248.1 (2005): "Gateway control protocol: Version 3", Reference [3] and ITU-T Recommendation H.248.43 (2008): "Gateway control protocol: Gate Management and Gate Control packages", Reference [4] except that the discarded packets (gm) are counting all discarded packets except those discarded due to policing. All octet counts are on the complete IP packet, excluding the IP header

The eri_seco statistics are proprietary statistics going beyond the H.248 standard and are defined as follows.

- Discarded Octets: The number of discarded octets on a Stream, except discards due to policing
- Discarded Packets – Policing: The number of discarded packets (IP packets) on a Stream, due to policing
- RTCP Reported Average Jitter: The average jitter as experienced and reported by a client, according to RFC 3550. Expressed in timestamp units.
- RTCP Reported Packets Lost: The accumulated number of lost packets as experienced and reported by a client, according to RFC 3550.
- Media Inactivity Timestamp: The time when the latest media stop was detected, minus the detection time, dt. If media is started again after the detection time and then followed by another detected media stop, the timestamp is replaced by the latest timestamp.
- Accepted MSRP chunks: Number of MSRP chunks accepted for this stream.

- Discarded MSRP chunks: MSRP chunks discarded due to noncompliance according to security and syntax rules.

For the RTCP reported average and lost packets, only the first report block in the SR/RR packet will be interrogated to get these statistics.

BGF snoops the RTCP stream for the values of jitter and packets lost. A termination facing user A collects the eri_seco/rraj and eri_seco/rrpl statistics as reported by user A as shown in Figure 3. In effect, this means the statistics for the A termination describe the quality of the media path in the direction from user B to user A.

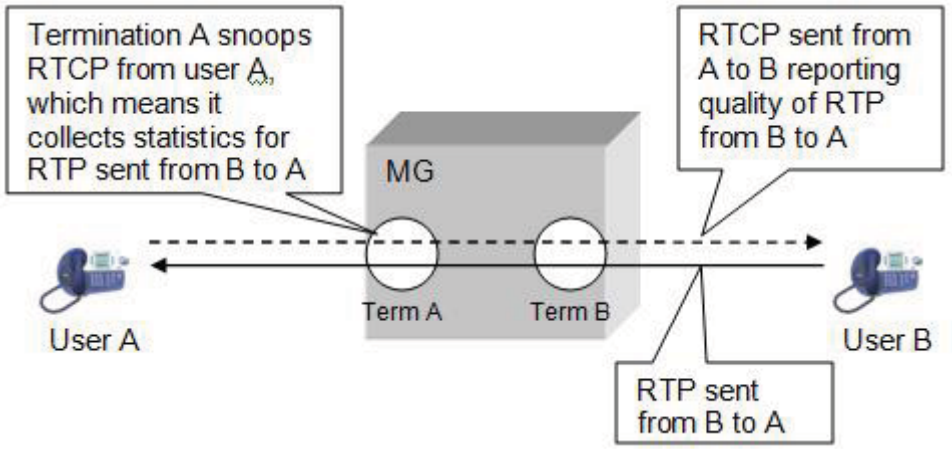

Figure 3 Collection of RTCP Reported Statistics in the BGF

The jitter value in RTCP reports indicates a moving average of the jitter over the existence of a stream. The BGF stores the most recent value received and reports it at deletion of a stream.

As the RTCP packets lost counter is cumulative, only the most recent value needs to be stored and reported at deletion of a stream.

3.18 Emergency Call Support

The BGF allows the operator to reserve a percentage of the total number of licenses and a percentage of the total bandwidth usage per realm. Once the total number of calls or realm bandwidth usage (including emergency calls) reaches the threshold value, only emergency calls are allowed. The threshold value is the same for the licenses and the bandwidth usage. There is no port reservation for emergency calls. If the maximum number of ports configured on one realm is reached, the emergency calls from/to that realm will be rejected.

3.19 Network Security

In addition to the above-mentioned Media flow gating, NAPT, media source filtering, stream mode enforcement, and RTCP handling, which all provide

security for the core network, the SmartEdge router supports a set of native security features which extend the perimeter protection of the IMS core network. As a general networking platform, the SmartEdge router supports the following:

- Access Control Lists (ACLs), IP service forwarding policies, authentication, authorization, and accounting, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+), and key chains provide general platform security
- Filtering, overload protection, and rate limiting are used to block IP traffic floods and provide protection against Denial of Service (DoS) attacks.
- IPv4/IPv6 ACL rules can either permit or deny a packet based on the following match criteria:
  - IP header fields - Source address, Destination Address, Protocol, DSCP, ToS, Total Length
  - TCP – Port, Flags
  - UDP – Port
  - ICMP – Type, Code
  - IGMP - Type
- IP spoofing attack can be prevented by configuring RPF checks for IPv4 and IPv6 packets. RPF check for IPv6 traffic is limited to subscriber circuits.
- Implicit checks are done on incoming packets. Packets with an IP version other than IPV4 or IPv6, header length < 20 bytes, incorrect header checksum, and invalid packet length and so on, will be dropped.
- Packets dropped due to implicit checks, ACL violations, reassembly failures, and so on, are considered as malicious traffic and can be optionally counted and logged. These counters are grouped into a number of categories for display purposes. The malicious counters are aggregated to trigger a context-wide malicious traffic alarm when the counter reaches a high watermark. The alarm is cleared when the aggregated malicious traffic counter drops below a low watermark.
- Both IPv4 and IPv6 malicious traffic can be logged to syslog servers or local files. For more information on how to configure malicious traffic protection for the SmartEdge router, refer to Configuring Malicious Traffic Detection and Monitoring, Reference [2].

3.20 High Availability

The SmartEdge BGF includes the following high availability features:

- Stateful process restart. Data is persistent for established calls. It is not persistent for in-progress calls; all in-progress calls are lost if the process is restarted.

- Stateful XCRP Controller card switchover. Data is synchronized for established calls. Data is not synchronized for in-progress calls; all in-progress calls are lost if the XCRP Controller card is restarted. The standby XCRP card is running hot allowing for a fast switch-over.

- Stateful PPA line card switchover. Latching information is synchronized between PPA line cards. Media plane statistics are not replicated and start from zero after switchover. To keep the switch-over times as short as possible, it is recommended to utilize VRRP with BFD detecting.

3.21 Overload Protection

The SmartEdge BGF is protected against overload. The system monitors the H.248 transaction response times for ADD and MODIFY commands. If the average rate of transactions, that do not complete within a latency threshold, exceed the crossing rate, an overload condition is declared. Two latency threshold values exist, Normal latency threshold, and Emergency latency threshold. If only Normal threshold is exceeded, all new emergency calls are accepted, but new non-emergency calls are selectively rejected with error code 510 "Insufficient resources", depending on the amount of overload. However, if Emergency threshold is also crossed, then all new calls requests are rejected. Any messaging for already accepted calls is never rejected due to overload.

The overload situation is cleared when the latency threshold crossing rate falls below the configured rate.

3.22 BGF Counters

The SmartEdge router possesses finely-grained performance management capabilities through its general platform statistics interface and MIB support.

On the SmartEdge BGF, the control interface is supervised as follows:

- SCTP association. A rich set of SCTP statistics is maintained. SCTP association statistics are counted per link.

- Control link. H.248 transaction-related and session-related statistics are maintained per BGF application.

3.23 Alarms

A MIB is defined for SmartEdge BGF notifications. For these notifications, specific traps are designed to raise and clear alarms using the alarm model MIB

framework in SNMP. The active and clear tables of alarms are accessible for viewing with CLI show commands as well as through SNMP query.

All alarms raised by an MGD instance will be deleted during process restart of that instance. If the alarm condition continues to exist, those alarms will be raised again.

The following alarms and events are supported in this release:

- **rbnH248LinkStatusAlarm**

  This alarm will be raised (trap sent) when the H248 link for a vMG is detected to be down for more than the configured alarm interval because the MGC is not reachable, the MGC is administratively down, or there is no MGC configuration. The alarm will have the vmg name, which is “mgc-group-name/mgd-instance-id”, as the identifier for the vMG. This alarm and associated notification is always enabled for an active vMG.

  The alarm is cleared (trap sent) for the following conditions:

  – vMG is able to connect to any of configured MGC successfully

  – The corresponding MGC group is deleted or shut down

  – The Media Gateway configuration is deleted or shut down

- **rbnMaliciousPktThresholdHiExceeded**

  This alarm will be raised when the context-wide aggregate drop counter reaches or exceeds the configured high watermark within the configured interval. A raised alarm will be cleared when the counter reaches or falls below the configured low watermark.

3.24 Error Handling

The BGF will test for routing failures at call setup. If the endpoints are not routable at the call setup, the call will be rejected with an error response (error code 531). A route lookup will also be done during latching. A routing failure during latching will generate a g/cause with general cause as FP (Fault Permanent) and failure cause as “No Route Found” to MGC. During an active session, only media inactivity will be detected.

3.25 IPV6 Support

The SmartEdge BGF supports IPv6 payload traffic including IPv4-to-IPv6 (and vice versa) protocol translation. The BGF can be used as a C-BGF that sits on the border of access and core networks, as well as an I-BGF that sits on the border of core and foreign networks. The following diagrams depict the configurations supported by the BGF.

3.25.1 SmartEdge BGF as C-BGF

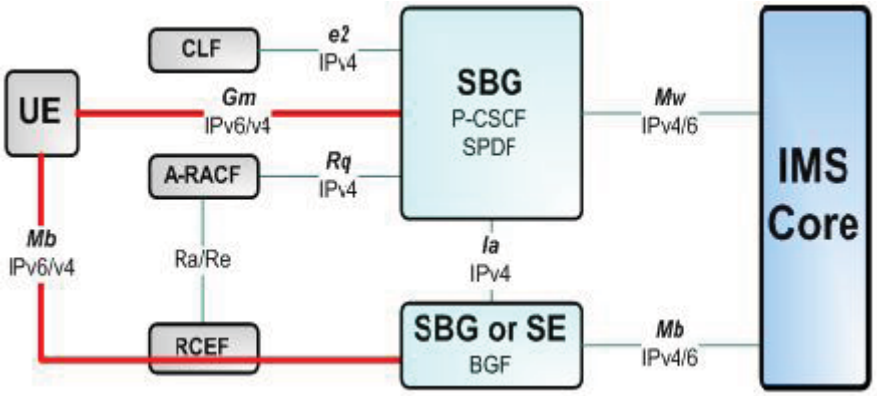

Figure 4

The BGF supports IPV4 , IPV6, and a mix of IPV4 and IPV6 endpoints in the core and access networks. The H.248 interface supports only IPV4 address.

3.25.2 SmartEdge BGF as I-BGF

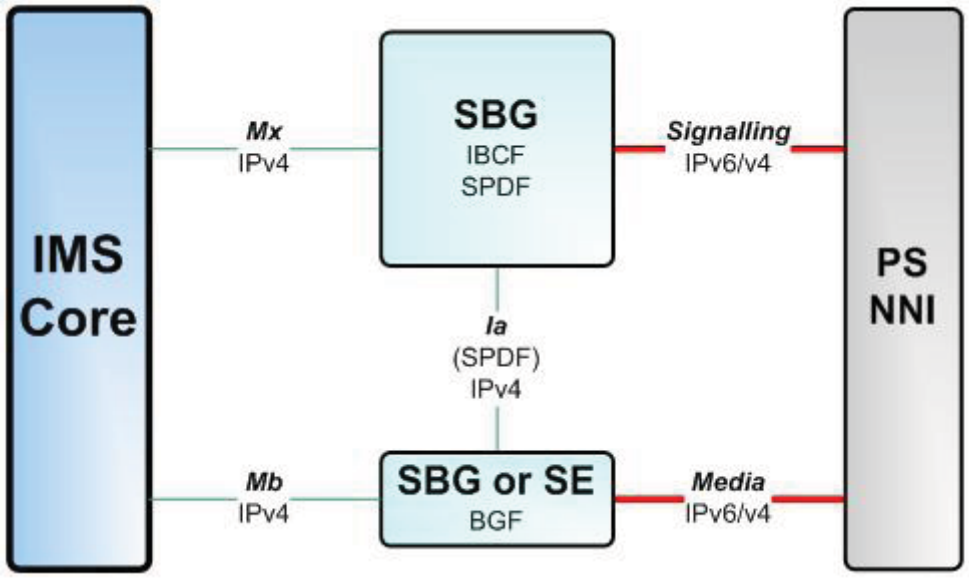

Figure 5

When acting as an I-BGF, it supports an IMS core that is either IPV4 or a combination of IPV4 and IPV6.

3.25.3 Media Address Handling

The BGF allows operators to configure both IPv4 and IPv6 addresses within a realm. The BGF gets information about the address family (IPv4 or IPv6) to be

used for the media stream from SDP in H.248 ADD/MODIFY commands, and it then allocates a corresponding media address and port for the media stream.

The BGF processes any type of media addresses in all relevant SDP lines; for example, c-line and a=rtcp attributes. It also processes both IPv4 and IPv6 addresses in different Gate Management (GM) Package properties, for example SAM (Remote Source Address Mask) and LSA (Local Source Address),

Different media streams on the same termination can have different address families. Similarly, related media streams (streams with same stream ID) on different terminations in the context can have different address families, which requires protocol translation for the stream. If related media streams on different terminations in a context use same address family, protocol translation is not required.

When an address family (IPv4 or IPv6) is selected for the media stream during creation, BGF rejects (with error code 501, “Not implemented”) any command that tries to change the address family mid-call.

The BGF supports symmetric address families for receiving and sending media, so it rejects (with error code 421 “Unknown action or illegal combination of actions”) any command that tries to use a different address family for:

- Remote address (address in c-line in RD)
- Remote RTCP address (address in a=rtcp attribute in RD)
- GM/SAM
- GM/LSA compared to the address family of Local address (address in c-line in LD)

3.25.4 Fragmentation and Reassembly

The BGF supports fragmentation and reassembly for both IPv4 and IPv6 traffic. For media traffic that is converted from IPv4 to IPv6, fragmentation and reassembly is supported for both IPv4 and IPv6 traffic. You can configure an ACL to drop fragmented IPv4 and IPv6 packets.

3.25.5 Checksum Adjustment

The BGF supports incremental checksum adjustment for all outgoing media packets for the following media traffic:

- IPv4 to IPv4
- IPv6 to IPv6
- IPv4 to IPv6
- IPv6 to IPv4

When an IPv4 UDP packet with a zero checksum is received and requires translation to IPv6, the UDP checksum is computed for each translated packet. It is assumed that UDP packets with a zero checksum are sent by legacy clients only and are expected to be less than 5% of the overall traffic. The UDP checksum computation for each packet requires higher processing on the media plane and might affect the overall performance of the solution if a large number of media packets is received with a zero checksum.

3.25.6 Option and Extension Headers

During conversion from IPv4 to IPv6, IPv4 options are ignored and not mapped.

- IPv4-to-IPv4 flow: IPv4 options (if present) are forwarded transparently.
- IPv4-to-IPv6 flow: IPv4 options (if present) are ignored. When an IPv4 header is translated to an IPv6 header, no extension header is added.
- IPv6-to-IPv4 flow: The following IPv6 extension headers are ignored and forwarded if received. Packets with extension headers not listed below are dropped.
  - Hop-by-hop options extension header: The outgoing IPv4 packet does not have an options header.
  - Destinations options extension header: The outgoing IPv4 packet does not have an options header.
  - Routing extension header with Segments Left equal to zero: The outgoing IPv4 packet does not have an options header.
  - Routing extension header with non-zero Segments Left: Generates an ICMPv6 “Parameter problem/erroneous header” toward the sender, and the packet is dropped.
- IPv6-to-IPv6 flow: The following IPv6 extension headers are ignored and forwarded if received. Packets with extension headers not listed below are dropped.
  - Hop-by-hop options extension header: The outgoing IPv6 packet does not have this extension header.
  - Destinations options extension header: The outgoing IPv6 packet does not have this extension header.
  - Routing extension header with Segments Left equal to zero: The outgoing IPv6 packet does not have this extension header.
  - Routing extension header with non-zero Segments Left: Generates an ICMPv6 “Parameter problem/erroneous header” toward the sender, and the packet is dropped.
  - IPv6 packets that exceed the MTU are dropped.

3.26 Autonomous Pinhole Closing

BGF provides autonomous pinhole closing to optionally terminate all calls in the system when it cannot reestablish the H.248 association within the configured time limit. Once the BGF Association link with the MGC is operationally down, the BGF starts a timer (configurable in the CLI). If the timer expires and BGF has not reestablished connection, it terminates all calls on the virtual MG and uses the initial start procedure to connect to MGC again. All call data is lost. The next ServiceChange that is sent has Restart as the method and Cold Boot as the reason.

This timer is started independently of the link-down alarm timer.

By default, autonomous pinhole closing is disabled.

3.27 KeepActive Flag

The BGF assumes that all events have the KeepActive flag and it will not cause any signal to stop. An events audit does not report a KeepActive flag.

The KeepActive flag functionality is supported for latch signal. The SGC starts the relatching process by including the signal latch. If later the SGC modifies the termination signals descriptor, the SGC keeps the signal latch (to avoid the signal being stopped if it had not completed) and adds the KeepActive flag to prevent the signal latch from reactivating.

If the SGC adds a second stream and the latch state on the 1st stream is not known, then the SGC would send the signal descriptor with latch (without KeepActive) on 2nd stream and latch (with KeepActive) on 1st stream

The KeepActive flag, if applied, is reported in the Audit descriptor for the latch signal.

3.28 MSRP Support

Message Session Relay Protocol (MSRP) is supported on SmartEdge BGF through multiple mechanisms. An MSRP B2BUA is implemented with the capability to change the MSRP “From-path” and “To-path” headers negotiated through SIP/SDP. MSRP B2BUA requires additional ASE2 hardware that supports fast media plane processing with hardware assist for a large number of TCP connections. ASE2-based implementation also supports TCP B2BUA implementation that allows clients behind a NAT/Firewall to successfully initiate a TCP connection to each other through SmartEdge BGF assisted TCP NAT traversal. This feature works with legacy NATs that are not compliant with the TCP simultaneous open procedure as per RCF 5382: NAT Behavioral Requirements for TCP, Reference [12].

In addition to the MSRP B2BUA mode of operation, the SmartEdge BGF also supports non-B2BUA mode, where MSRP is supported for clients and MSRP

servers that are compliant with MSRP ACM (Alternate Connection Mode) described in An Alternative Connection Model for the Message Session Relay Protocol, Reference [13] and MSRP session match described in Session Matching Update for the Message Session Relay Protocol (MSRP) , Reference [14]. This mode of operation does not require an ASE2 card and work with existing PPA2- and PPA3-based hardware. The BGF adds the MSRP URI in the a=path SDP attribute in the Local Descriptor and returns this information to the SGC. The path header contains the IP address from the c line and the port number from the m line of the SDP. For the TCP and TCP/MSRP media types, the BGF latches to the first TCP packet received. Once a TCP connection is established, the MSRP traffic flows through the BGF. The To/From-Path headers in MSRP packets are not modified for non-B2BUA mode. In MSRP B2BUA mode, packets are validated at the MSRP level. MSRP B2BUA mode requires an additional license.

3.29 Secure RTP Support

SmartEdge BGF supports both End to End(E2E) and E2AE(End to Access Edge) secure RTP. For E2E secure RTP, the BGF does not decrypt or encrypt RTP media but it supports all other media plane services supported for regular RTP streams. If SRTCP is enabled for E2E RTP streams, snooping and reporting of SRTCP statistics is not supported. Additional hardware is not required for E2E SRTP.

The BGF supports E2AE SRTP through ASE2 cards which supports hardware-assisted encryption and decryption of secure RTP media. In E2AE SRTP, the media from the end-user device to the SmartEdge BGF is encrypted and the media traveling towards the core is RTP. The SDES protocol, described in Session Description Protocol (SDP) Security Descriptions for Media Streams , Reference [15], is used as the SRTP key management protocol by the end devices. Because the keys are exchanged over clear text, IPsec is strongly recommended to secure the H.248 Ia interface. The H.248 SRTP package is supported for E2AE security. The following cryptograpy suites are supported by the SmartEdge BGF in this release:

- AES_CM_128_HMAC_SHA1_
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

This feature requires an additional license and requires support on SGC.

3.30 ICMP Error Handling

SmartEdge BGF supports ICMP error generation and propagation for IPv4 and IPv6 BGF traffic.

ICMP error generation: The BGF generates ICMP ‘Packet Too Big’ messages for IPv6 and ‘Fragment Needed but DF bit set’ messages for IPv4 if the effective MTU size exceeds or if the size of the packet is larger than the maximum l4-payload-size configured per realm.

ICMP error propagation: The BGF propagates the received ICMP ‘Packet Too Big’ messages for IPv6 and ‘Fragment Needed but DF bit set’ messages for IPv4 from a node along the media path.

3.31 Optimized BGF Selection

Multiple BGFs can be connected to one SGC in most operator deployment scenarios. The SGC selects a BGF for a call based on supported realms; if more than one BGF supports the realms required for a call, the SGC uses a round-robin algorithm to select the BGF. The selection can be further optimized by selecting the closest BGF or selecting the BGF that was previously used for anchoring the same call. The new selection criteria require BGF to have a location-based identifier, which can be configured by the operator. BGF “siteID”, a new property in the “eri_seco” package introduced to support this feature, is a root-level property that can be audited by the SGC. The “siteID” can be configured through the CLI and follows the domain name syntax. For more details on how to configure the “siteID”, refer to BGF Command Reference, Reference [1]. This feature requires that the SGC support the optimized BGF selection feature.

3.32 Globally Unique MID

The H.248 message ID, also known as the MID, is used to uniquely identify a virtual media gateway. Multiple virtual media gateways can be supported by a single SmartEdge BGF. SmartEdge BGF supports the device-name format for the MID, as follows:

<MGC-group name>/<MGD instance id>@<system MAC>

where:

- MGC-group name is the MGC group name configured using the CLI command
- MGD instance id is the media gateway daemon’s process instance ID
- System MAC is the unique MAC for the Backplane which does not change even when XCRP cards are changed

3.33 Media Plane Redundancy

The SmartEdge BGF uses BFD, ND, VRRP, and LAG to support media redundancy. Redundancy is achieved by providing media forwarding path

redundancy even when one of the media forwarding cards on SmartEdge fails or when the next-hop router to which the media packets are being forwarded fails. The status of ongoing calls is not affected by failover between media interfaces, and there is no notification on the H.248 interface with SGC.

BFD is used to achieve sub-second failover time, which is vital for real-time applications like VoIP. BFD failover time can range from 150 ms to 640 ms, depending on the configuration. BFD over IPv4 is fully supported and works for both static and dynamic routes. Single-session and multisession BFD over IPv6 are not supported for static routes.

ND (Neighbor Discovery) supports Neighbor Unreachability Detection, which is used to detect next-hop failure for IPv6. The detection time is 1 to 2 minutes.

VRRP (Virtual Router Redundancy Protocol) provides IP redundancy on the physical interfaces that are connected to the next-hop router. When the physical link fails because of a local media/data card failure, the slave takes the role of the master (active), and the media packets are received and forwarded without interruption. To protect against media card failures, it is highly recommended that the master and slave ports for VRRP be configured on two physically separate media cards. VRRP is only supported for IPv4.

Two or more physical ports can be configured for LAG on a SmartEdge router. When one or more ports that are part of a LAG go down, other ports act as the backup and share the load, and packets are forwarded without interruption. To protect against data plane card failures, it is highly recommended that LAG members belong to different physical cards. You can configure all the LAG members as active to maximizing physical port usage. In failure conditions, if the traffic does not exceed the port physical maximum, media packets are forwarded without interruption. Trunk LAG is supported for both IPv4 and IPv6.

Core networks are typically IPv4, so VRRP should be used to protect against local media card failure, and BFD should be used to detect next-hop failure on the core side.

Access networks often use both IPv4 and IPv6, so trunk LAG should be used to protect against local media card failure, and BFD over IPv4 or ND over IPv6 should be used to detect next-hop failure on the access side.

3.34 BGF Statistics through Bulkstats

The bulkstats feature can gather BGF-related performance statistics and periodically send this data as part of its updates to a management station. The “bulkstats schema profile” command is enhanced for this feature.

In global configuration mode, this command includes a new schema media gateway profile type to collect media gateway (MG) statistics at the global or MG controller (MGC) group level.

In media-gateway configuration mode, the “bulkstats schema” applies a predefined MG global schema profile, along with the policy and context in which the policy is defined, to collect global MG statistics.

In mgc-group configuration mode, this command applies a predefined MGC group schema profile, along with the policy and context in which the policy is defined, to collect MGC group statistics.

4 Command-Line Interface

In general, one instance of a SmartEdge BGF can be defined on a SmartEdge router using the SmartEdge OS command-line interface (CLI). This configuration is called *global BGF configuration*, and it applies to the SmartEdge router as a whole. (This kind of configuration may not be performed, for example, from within a VPN context.)

Once the BGF instance has been defined, it may be referred to from within a configuration context and its operation can be customized for that context. This configuration is called *context-specific BGF* configuration, and it applies only to the specific context in which it is applied. (In this section, “Context” refers to a SmartEdge context rather than a H.248 context.)

The context-specific configuration would typically correspond to settings done per realm. As discussed in Section 3.4 on page 12, realms are used in the communication between SPDF and BGF to identify the logical networks which the BGF provides media bridging between. The context names configured on the BGF are used as the IP Realm Identifiers in communication with the SPDF.

When the term BGF is used in the SmartEdge CLI, it only refers to configurations of the BGF and does not include any P-CSCF, A-ALG, IBCF, or SPDF configuration.

The following section provides an overview of the command hierarchy. For details on CLI, refer to BGF Command Reference, Reference [1].

4.1 Command Mode Hierarchy

Command modes exist in a hierarchy. You must access the higher-level command mode before you can access a lower-level command mode in the same chain.

Figure 6 shows the hierarchy of the command modes used to configure global BGF features.

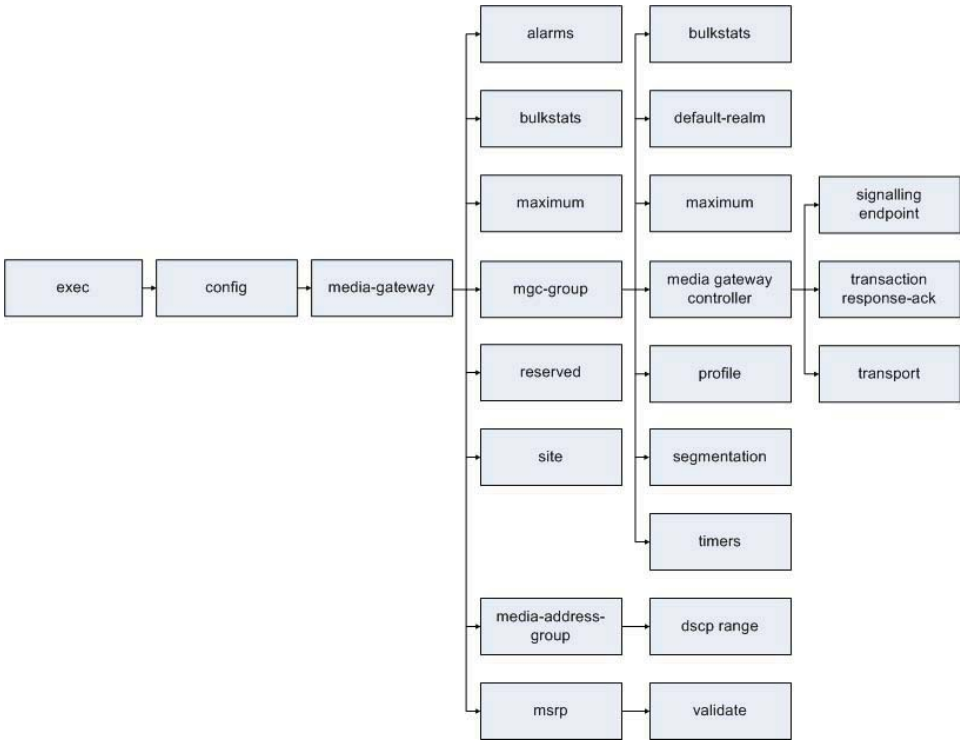

Figure 6 Command Mode Hierarchy for Global BGF Commands

Table 2 lists the global BGF command modes (in alphabetical order) relevant to global BGF features and services provided on the SmartEdge routers. It includes the commands that enable access to each mode and the command-line prompt for each mode.

Table 2 Command Modes and System Prompts for BGF

Mode Name	Command Used to Access	Command line Prompt
exec	**(user logon)**	# or >
global	**`configure`** command from exec mode	(config)#
bulkstats schema profile	**`configure bulkstats schema profile`**	(config)#
asp pool <pool-name> service media-gateway	**`configure asp pool`** for media-gateway services	(config)#
media-gateway	**`media-gateway`** command from global configuration mode	(config)#

Mode Name	Command Used to Access	Command line Prompt
alarms	**alarms** command from media-gateway configuration mode	(config-mg)#
bulkstats	**bulkstats** command from media-gateway configuration mode to enable MG-level statistics	(config-mg)#
media-address-group	**media-address-group** command from media-gateway configuration mode	(config-mg)#
mgc-group	**mgc-group** command from media-gateway configuration mode	(config-mg)#
msrp-validate	**msrp-validate** command from media-gateway configuration mode	(config-mg)#
reserved	**reserved** command from media-gateway configuration mode (config-mg)#	(config-mg)#
site	**site** command from media-gateway configuration mode	(config-mg)#
dscp	**dscp** command from media-address-group configuration mode (config-mg-media-addr-grp)#	(config-mg-media-addr-grp)#
bulkstats	**bulkstats** command from media-gateway configuration mode to enable MG-level statistics	(config-grp)#
default-realm	**default-realm** command from mgc-group configuration mode	(config-grp)#
maximum	**maximum** command from mgc-group configuration mode	(config-grp)#

Mode Name	Command Used to Access	Command line Prompt
media-gateway-controller	**media-gateway-controller** command from mgc-group configuration mode	(config-grp)#
profile	**profile** command from mgc-group configuration mode	(config-grp)#
segmentation	**segmentation** command from mgc-group configuration mode	(config-grp)#
timers	**timers** command from mgc-group configuration mode	(config-grp)#
signaling endpoint	**signaling endpoint** command from media-gateway-controller configuration mode	(config-mgc)#
transaction-response-ack	**transaction-response-ack** command from media-gateway-controller configuration mode	(config-mgc)#
transport	**transport** command from media-gateway-controller configuration mode	(config-mgc)#

Figure 7 shows the hierarchy of the command modes used to configure context-specific BGF features.

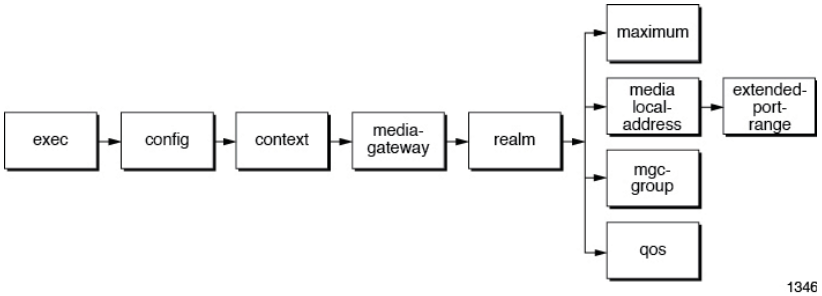

Figure 7 Command Mode Hierarchy for Context-Specific BGF Commands

Table 3 lists the context-specific BGF command modes (in alphabetical order) relevant to context-specific distributed BGF features and services provided on the SmartEdge routers. It includes the commands that enable access to each mode and the command-line prompt for each mode.

Table 3 Command Modes and System Prompts for Context-Specific BGF

Mode Name	Command Used to Access	Command line Prompt
exec	(user logon)	# or >
global	**configure** command from exec mode	(config)#
context-specific	**context** command from global configuration mode where context is the name of the context	(config-ctx)#
bulkstats policy	**bulkstats** command from context configuration mode defining the bulkstats policy	(config-ctx)#
media-gateway	**media-gateway** command from context configuration mode	(config-ctx)#
realm	**realm** command from media-gateway configuration mode	(config-ctx-mg)#
maximum	**maximum** command from realm configuration mode	(config-realm)#
media-local-address	**media-local-address** command from realm configuration mode	(config-realm)#
mgc-group	**mgc-group** command from realm configuration mode	(config-realm)#
qos	**qos** command from realm configuration mode	(config-realm)#
extended-port-range	**extended-port-range** command from realm mg configuration mode	(config-realm-media)#

5 H.248 Signaling Support

The BGF supports an extended version of the TISPAN H.248 Ia profile version 2.5.0. For more information, refer to ETSI TISPAN ES 283 018 v2.5.0 (2008-11): “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”, Reference [5]. This profile defines the set of commands, descriptors, packages, and procedures used by the SPDF to control the BGF.

Reference List

Ericsson Documents

[1] *BGF Command Reference*, 127/1090 82-CRA 119 1170/1 Uen

[2] *Configuring Malicious Traffic Detection and Monitoring*, 87/1543-CRA 119 1170/1 Uen

Non-Ericsson Documents

[3] *ITU-T Recommendation H.248.1 (2005): "Gateway control protocol: Version 3"*

[4] *ITU-T Recommendation H.248.43 (2008): "Gateway control protocol: Gate Management and Gate Control packages"*

[5] *ETSI TISPAN ES 283 018 v2.5.0 (2008-11): "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"*

[6] *ETSI ES 282 003: "Resource and Admission Control Sub-system (RACS); Functional Architecture"*

[7] *RFC 3959: "The Early Session Disposition Type for the Session Initiation Protocol (SIP)"*

[8] *ETSI ES 283 003: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified]"*

[9] *"3GPP TS 24.229: Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 7)"*

[10] *3GPP TR 21.905: "Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications"*

[11] *RFC 2697: A Single Rate Three Color Marker*

[12] *RCF 5382: NAT Behavioral Requirements for TCP*, http://www.ietf.org/rfc/rfc5382.txt

[13] *An Alternative Connection Model for the Message Session Relay Protocol*, http://tools.ietf.org/html/rfc6135

[14] *Session Matching Update for the Message Session Relay Protocol (MSRP)* , http://tools.ietf.org/html/draft-ietf-simple-msrp-sessmatch-10

[15] *Session Description Protocol (SDP) Security Descriptions for Media Streams* , http://tools.ietf.org/html/rfc4568