

SBG 3.1 Operation and Configuration for IMS

Disclaimer

This book is a training document and contains simplifications. Therefore, it must not be considered as a specification of the system.

The contents of this document are subject to revision without notice due to ongoing progress in methodology, design and manufacturing.

Ericsson assumes no legal responsibility for any error or damage resulting from the usage of this document.

This document is not intended to replace the technical documentation that was shipped with your system. Always refer to that technical documentation during operation and maintenance.

© Ericsson 2010

This document was produced by Ericsson.

It is used for training purposes only and may not be copied or reproduced in any manner without the express written consent of Ericsson.

This Student Book, LZT 123 9299 R3A supports course number LZU 108 7968 R1A.

Table of Contents

Chapter

- SBG 3.1 Overview
- Hardware and Software Structure
- User Interface
- Node Management
- Alarms and Events
- SBG Logs
- SBG Performance Measurement
- Signalling Through SBG
- SBG Installation
- SBG Configuration
- DIAMETER Interface
- Configure Secure and Redundant SBG

Course Main Objectives

After completing the module the student should be able to:

- Describe SBG Features and Functions
- Describe SBG System Architecture
- Perform Surveillance activities (basic operation and maintenance) of SBG
- Describe network use cases with SBG
- Describe the Installation process of SBG
- Configure and verify the SBG Interworking interfaces
- Describe and Configure SBG Features
- Describe and configure the SBG TISPAN P-CSCF functionality
- Perform root cause analysis of faults in SBG
- Set up and analyze performance measurements for SBG
- Describe how to configure a secure and redundant SBG

SBG 3.1 Operation and Configuration for IMS

SBG 3.1 Overview

The Ericsson SBG is a Session Controller.

What is a Session Controller?

- A Session-Aware Device.
- Controls call admission at the border of a network.
- May perform Call Control functions.

SBG Main Features

- High-performance carrier-class session controller
- Correlates all signalling and media streams
- Stateful B2BUA & Pinhole Firewall
- Key Functions:
 - Security
 - Privacy
 - Quality of Service
 - *LI*
 - *Charging*
 - *Geographic Location of Users*

Session Border Gateway (SBG) Introduction

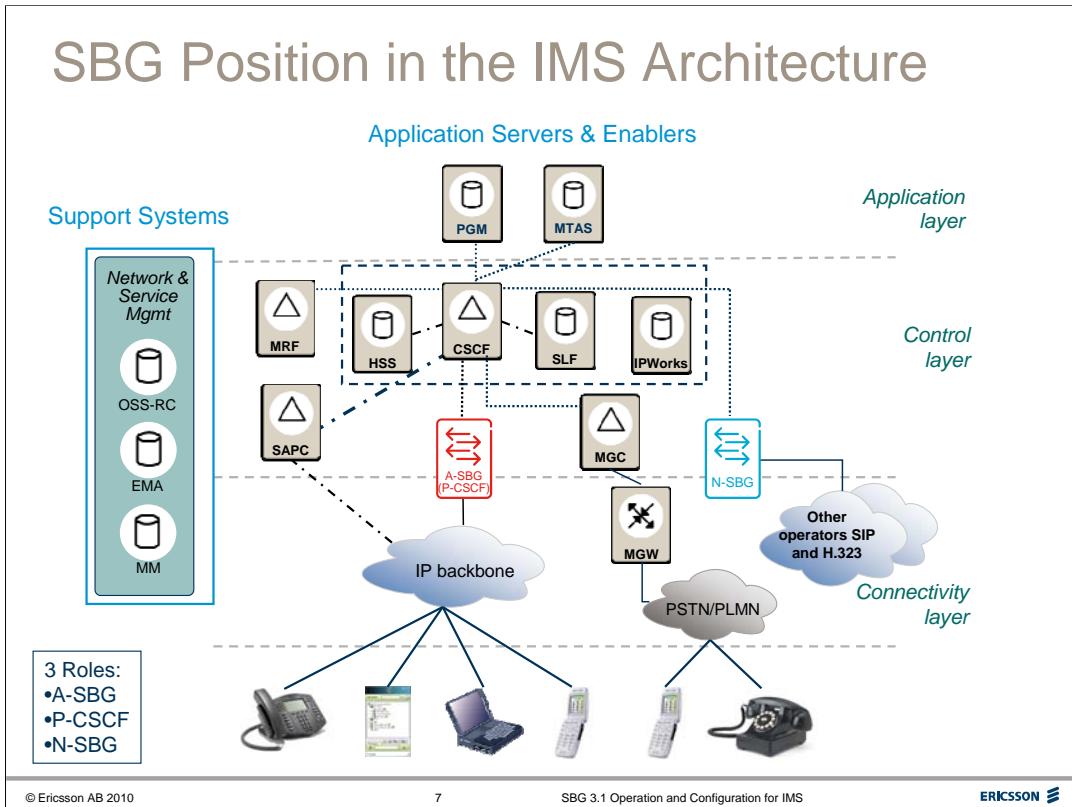
The ERICSSON Session Border Gateway is a high-performance carrier-class session controller product based on the Integrated Site (IS) Architecture.

The SBG provides the ability to correlate all signalling and media streams (such as audio and video) that pass the network borders, hence providing a comprehensive suite of functions required to access and interconnect IP core domains (e.g. IMS) and other IP networks with preserved security, privacy, and quality of service.

The SBG ensures network security, bandwidth fraud protection, topology hiding, quality of service, service level agreements, hosted NAT/FW traversal, address and port translation (NAPT), and other critical functions for real-time IP streams.

The SBG also enables lawful intercept, charging, IP-PBX business trunking, handling of geographical location of users, access network connection admission control, and functionality for handling geographical redundancy of other nodes, as well as admission control and bearer authentication (3GPP).

The SBG in general acts as 1) a **Stateful B2BUA**, terminating SIP/H323 signalling from one network and sending SIP/H323 Signalling to another network; and 2) a dynamic pinhole **Firewall**.



SBG in the Ericsson IMS architecture

In the Ericsson IMS network solution, the SBG can be used in three main roles in the IMS Network:

Access Session Border Gateway

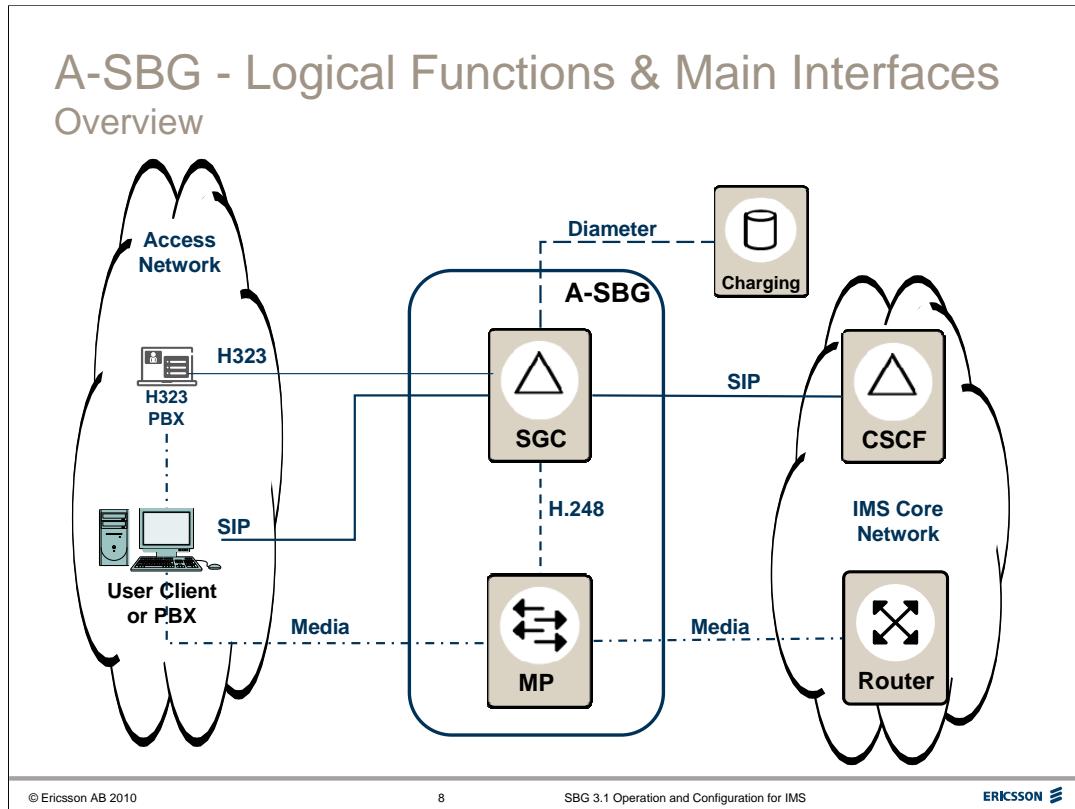
- As an access gateway at the border between the IMS core network and the access networks – the Access SBG or **A-SBG**

TISPAN P-CSCF and A-SBG

- The A-SBG can also be configured to perform the role of the TISPAN **P-CSCF**.

Network Session Border Gateway

- As a generic IP-IP NNI gateway at the border to another core network – the Network SBG or **N-SBG**



SBG Logical Functions and Main Interfaces

The SBG consists of two main functions, each implemented on separate IS Blades.

Session Gateway Controller (SGC)

The SGC is the signalling B2BUA, handling all SIP & H323 signalling with the Access network and SIP to the IMS Network plus most of the control functions such as Charging, Lawful Intercept, Admission Control and so on.

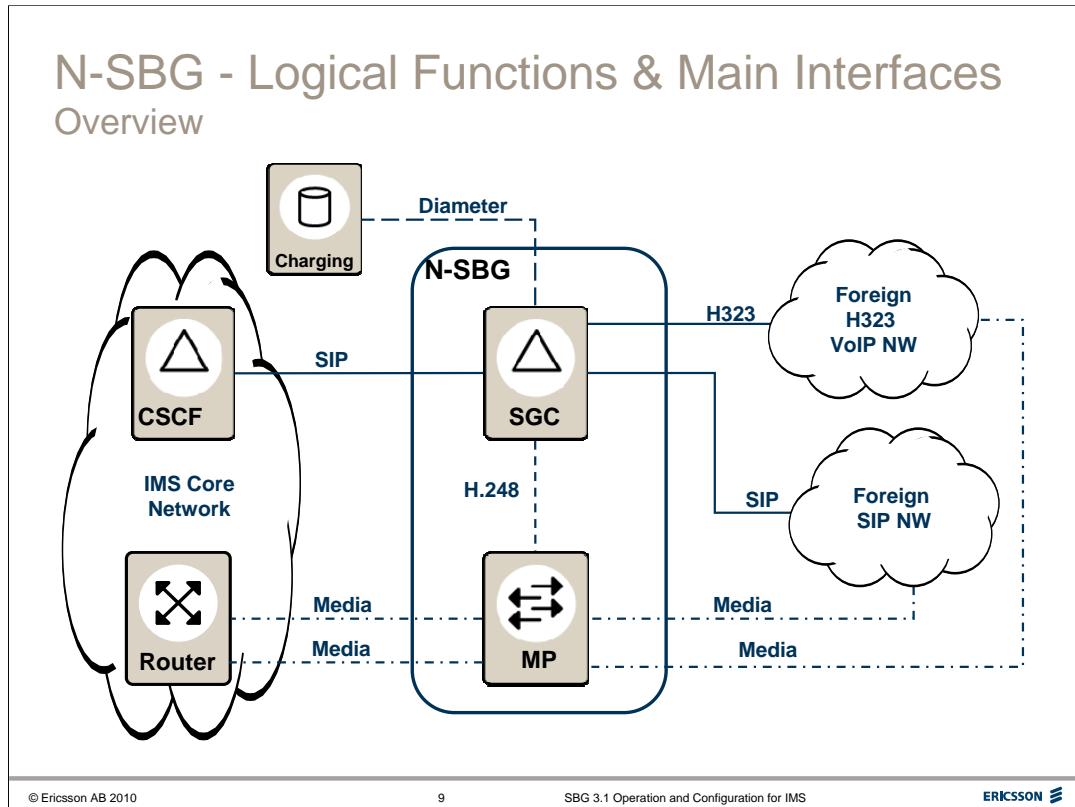
The SGC controls the Media Proxies (“Firewalls”) using H248/MeGaCo over the **Ia** interface

Media Proxy (MP)

The Media Proxy contains the dynamic pinhole firewall function for Media streams to/from the IP Access Network and the IMS core IP network.

A-SBG Interfaces

A-SBG Interfaces the SIP and H323 Access Network(s) on one side, and the IMS Core Network on the other side.



N-SBG Functions

Session Gateway Controller (SGC)

The SGC is the signalling B2BUA between the IMS Core and “Foreign” SIP and H323 Networks

It also implements most of the control functions such as Charging, Lawful Intercept, Admission Control and so on.

Media Proxy (MP)

The Media proxy contains the dynamic pinhole firewall function for Media streams to/from the IMS Core IP Network and the Foreign IP Networks.

N-SBG Interfaces

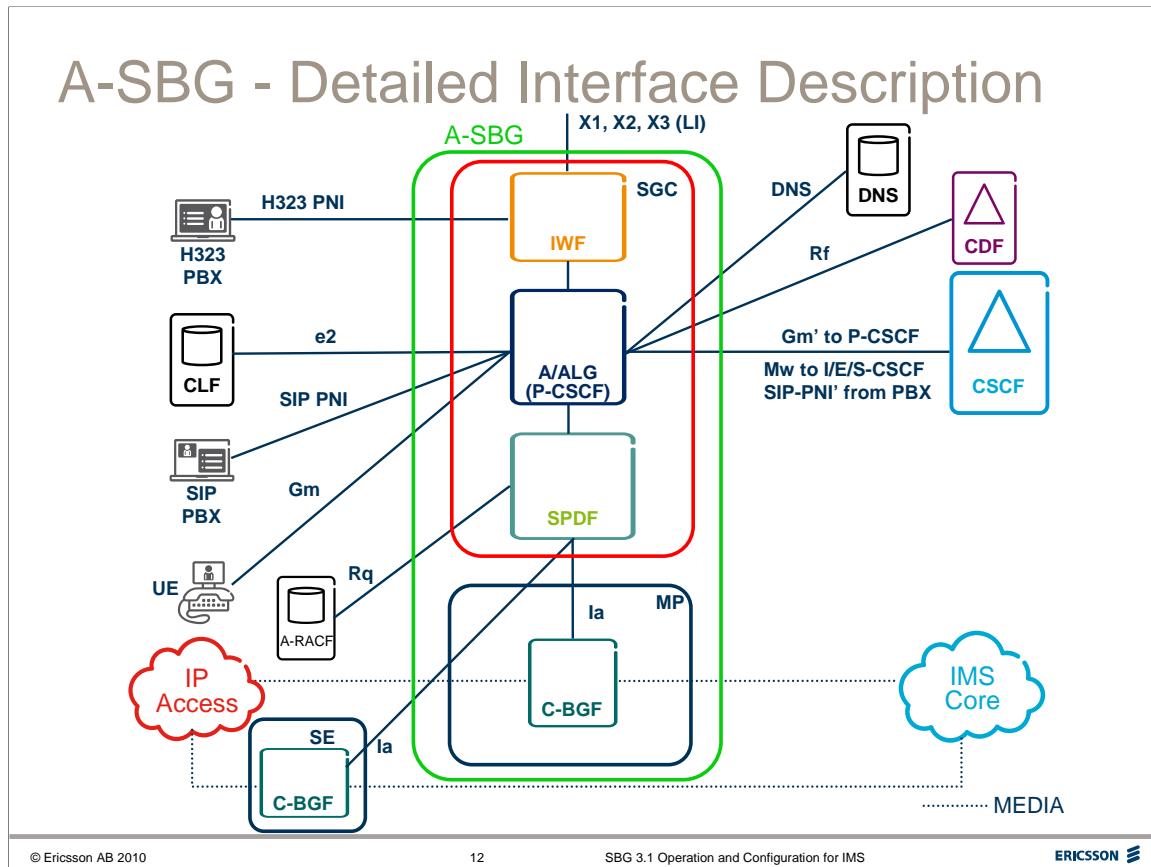
N-SBG Interfaces the IMS Core Network on one side, and the Foreign SIP and H323 Network on the other side.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

SBG 3.1 Internal Architecture and Interfaces



The A-SBG **Session Gateway Controller** comprises three main functions:

Access Application Level Gateway (A/ALG)

The A/ALG acts as the B2BUA between the Access Networks and the CSCFs in the IMS core. The A/ALG has SIP Registrar functionality to support registration of users and to support routing of SIP to the Access Networks.

Service-based Policy Decision Function (SPDF)

The SPDF decides which Media streams are allowed to be set-up and the characteristics of the streams. The SPDF requests required resources from BGFs & A-RACF.

Inter-Working Function (IWF)

The IWF is defined by TISPAN as the entity which performs the inter-working in the SBG between H.323 and SIP.

The **Media Proxy (MP)** includes the:

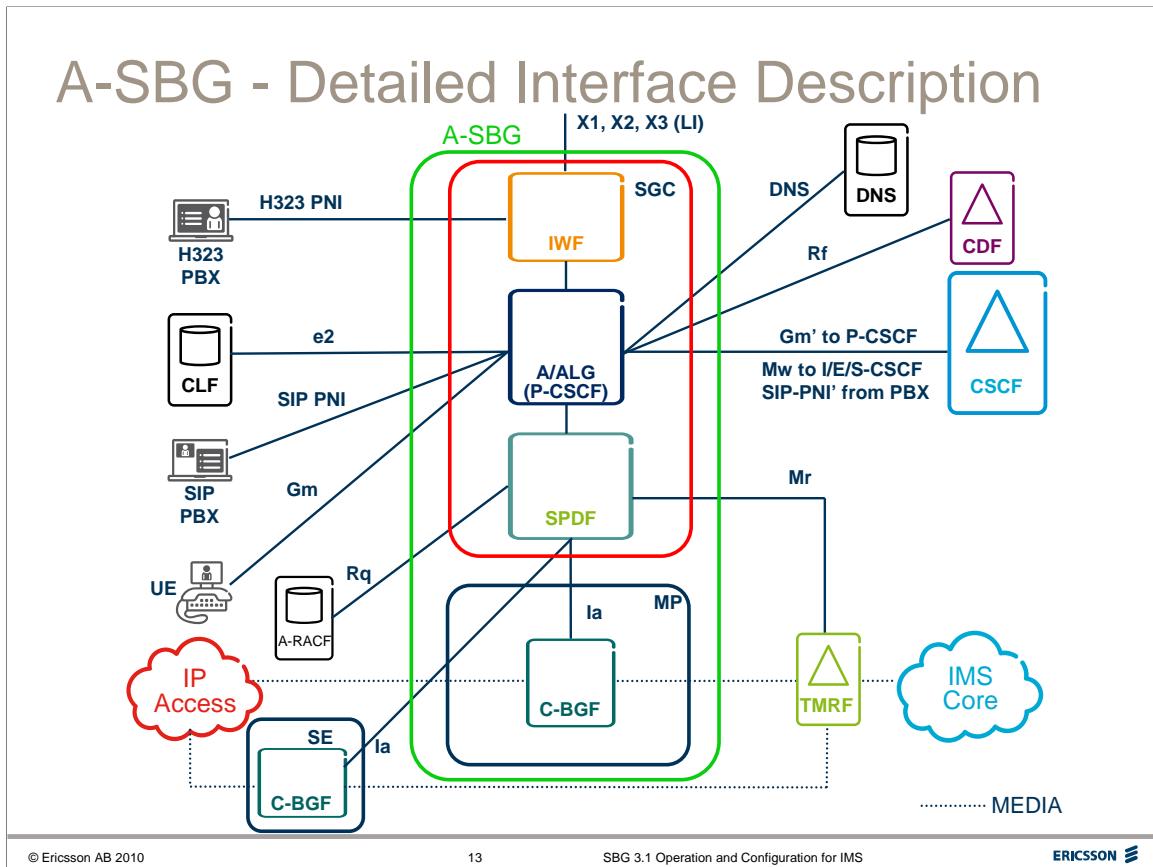
Core Border Gateway Function (C-BGF)

The BGF is a packet-to-packet gateway for media plane traffic.

BGF performs the following functions under SPDF control:

- *Opening/closing pinholes*
- *Packet marking. DSCP*
- *Resource allocation per flow. bandwidth CAC*
- *NAPT*
- *Policing of downlink and uplink traffic & Usage metering; reports to the SGC*
- *Hosted NAT/FW traversal.*

The BGF can be either integrated or distributed on ERICSSON RedBack SmartEdge.



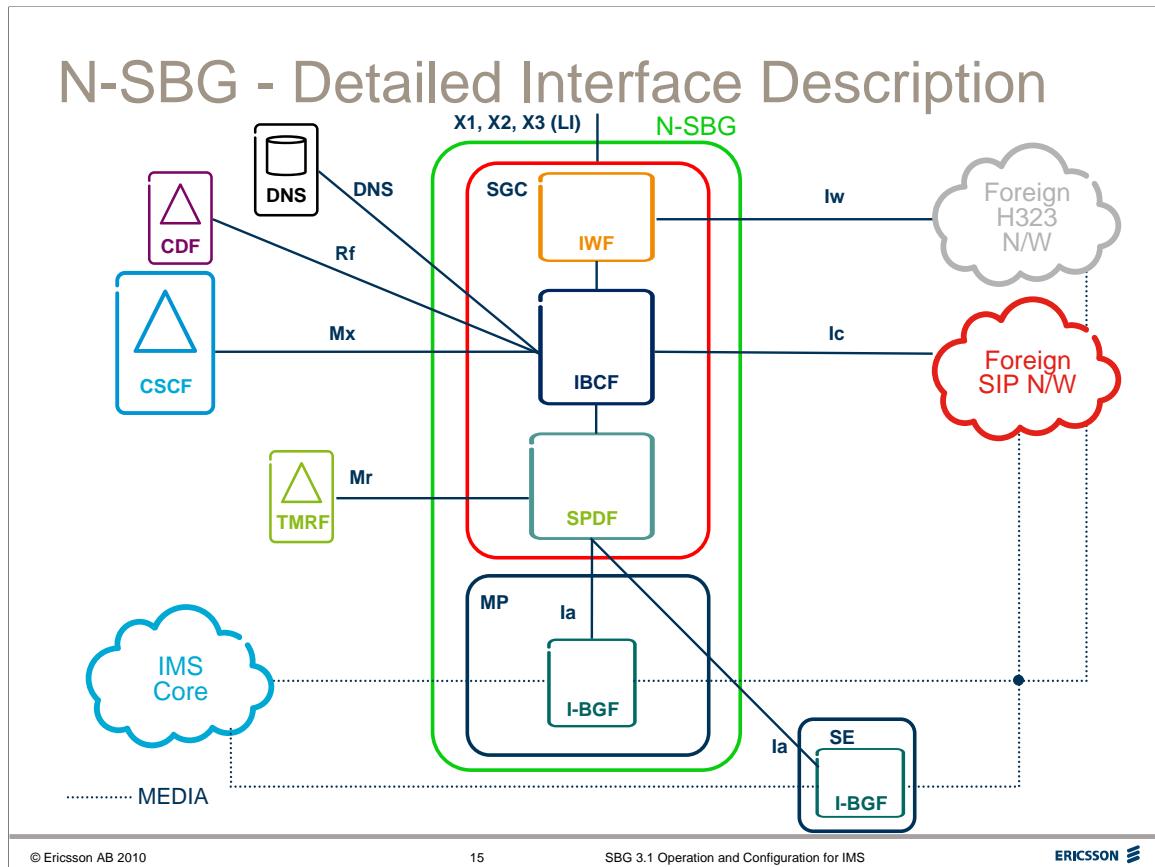
The TRMF is a Trial function for codec translation.

Legend

A-RACF	Access Resource Admission Control Function
CDF	Charging Data Function (ERICSSON MultiMediation)
CLF	Connectivity Session Location & Repository Function
IWF	H323 Interworking Function
MP	Media Proxy
SGC	Session Gateway Controller
TRMF	Transcoding Media Resource Function
SE	Ericsson RedBack SmartEdge Router

Interface**Description**

DNS	DNS to DNS server.
e2	Diameter to CLF for geographical location query.
Gm	SIP to UE (not to IP-PBX).
Gm'	SIP to external P-CSCF.
H.323 PNI	H.323 to H.323 IP-PBX.
Ia	An open Ia interface to the External BGF, the ERICSSON Redback Smart Edge. The external BGF is not a replacement for the Internal BGF. H.248 is used between SGC and BGF (Integrated or External). The H.248 profile used is an enhanced version of the ETSI TISPAN defined Ia profile (ETSI ES 283 018).
Ic	SIP to foreign SIP network.
Iw	H.323 NNI. H.323 to foreign H.323 network.
Mw	SIP interface between P-CSCF role in SBG and I/S/E-CSCF.
Rx	Diameter for PCRF, Bearer Authentication.
Mb	Media plane traffic to any node terminating media.
Mx	SIP interface to I/S-CSCF.
Rf	Diameter to CDF for off-line charging.
Rq	Diameter to A-RACF for network admission control.
SIP PNI	SIP to SIP IP-PBX.
SIP PNI'	SIP to IMS core node for handling traffic from SIP and H.323 IPPBX.
X1	X1 from LI-IMS for ordering LI of specific users. The term X1 is used in SBG documents as a short term for the standard X1_1 interface.
X2	X2 to LI-IMS for delivery of intercepted control plane traffic.
X3	X3 to LI-IMS for delivery of intercepted media plane traffic.



The **N-SBG Session Gateway Controller** comprises three main functions:

Interconnection Border Control Function (IBCF)

The IBCF acts as a B2BUA between the IMS core network and 'foreign' SIP and H323 networks

Service-based Policy Decision Function (SPDF)

SPDF in the N-SBG performs the same function as described for the A-SBC.

The SPDF decides which Media streams are allowed to be set-up and the characteristics of the streams. The SPDF requests required resources from media plane entities.

Inter-Working Function (IWF)

The IWF in the N-SBG performs the same function as described for the A-SBC, it performs inter-working between H.323 foreign networks and IMS.

The **Media Proxy (MP)** includes the:

Core Border Gateway Function (C-BGF)

The BGF in the N-SBG performs the same function as described for the A-SBC:

- *Opening/closing pinholes.*
- *Packet marking. DSCP*
- *Resource allocation per flow. bandwidthCAC*
- *NAPT.*
- *Policing of downlink and uplink traffic.*
- *Usage metering. gathers statistics and reports to the SGC.*
- *Hosted NAT/FW traversal.*

The BGF can be either integrated or distributed on ERICSSON RedBack SmartEdge



ERICSSON

SBG 3.1 Operation and Configuration for IMS

SBG 3.1 Features

This section lists the main features of the SBG3.1.

The features are *briefly* described here.

More detailed descriptions will be found later in the book, together with configuration and management details.

SBG Features 1 - Network Security

- Perimeter protection of the core network
 - Protection against DoS, voice hammer attacks and hijacking of media streams
- Logging and alarming for network attacks
- SIP and H.323 message validation
- SIP header blacklists
- Maximum SIP message size.
- Topology hiding
- Configure how RTCP packets are forwarded
- Media anchoring
- Media flow gating
- Bandwidth policing per media stream.
- Validation of IP addresses received in SDP
- TLS (Transport Layer Security) of SIP
- IPsec
- SIP abuse protection from unregistered users
- SIP Message Throttling
- User Agent Whitelists

NETWORK SECURITY

The main function of an SBG is to provide Network Security. There are many features in SBG which contribute to Network Security, many are briefly described below. These features will be further explained and their configurations described later in the book.

Perimeter protection of the core network: filtering, overload protection, and rate limiting is used to block IP traffic floods.

Provide protection against ***Denial of Service*** (DoS) attacks and protection against ***voice hammer*** attacks (by validation of IP addresses in the SDP against source IP address) and ***hijacking*** of media streams by ***latching*** (The source IP address and port of the first packet received from a user behind a NAT is used in the BGF for sending packets to the user and for the dynamic pinhole firewall when accepting packets from that user).

Logging and alarming for network attacks and security-related events. So that historical records of Network security breaches are available for examination.

SIP and H.323 message validation: Check of message syntax.

Multipart/MIME (Multipurpose Internet Mail Extensions) bodies are supported in SIP, which allows Session Description Protocol (SDP) handling as well as forwarding for example SIP for Telephones (SIP-T) and SIP with encapsulated ISUP (SIP-I).

In addition, A-ALG/P-CSCF (ASBG) only accepts messages from registered user agents or configured IP-PBXs or messages related to emergency calls (emergency calls can also be accepted from unregistered users).

SIP header blacklists

The SBG maintains an incoming blacklist profile and an outgoing blacklist profile per signaling network. The blacklist function *filters SIP headers* in requests, responses or both according to the configured blacklist profile in each network. The filtering can be different for different networks and directions so a header could be removed when entering from a certain network or removed when the messages is sent out to a certain network.

Configurable maximum SIP message size.

Topology hiding: No information regarding IP addresses used in the core network or by users is forwarded in signaling messages to the access network or foreign network.

RTCP forwarding

Configure how RTP Control Protocol (RTCP) packets are forwarded in order to restrict, for example, topology information to users. RTCP packets may contain IP address information or user-specific information. The SBG offers functions to control how RTCP packets are forwarded to prevent that address information, or other content, being passed between networks. RTCP packets can be forwarded in both directions, in one direction only, or dropped.

Media anchoring: Update of addresses and ports in the SDP or OLC (Open Logical Channel) to direct media streams to pass through SBG.

Media flow gating to protect against bandwidth fraud: Only media streams corresponding to the observed signaling state and allowed SDP or OLC parameters are passed, that is, the SBG acts as a dynamic pinhole firewall for media streams.

Bandwidth policing per media stream, based on the SDP or OLC in H.245 information in the signaling; logging and alarming of excessive media.

Validation of IP addresses received in SDP. Addresses not allowed (for example, broadcast) are filtered out.

TLS (Transport Layer Security) Encryption (replaces Secure Sockets) for protection of SIP between users and A-ALG/P-CSCF.

IPsec for protection of for example control plane and OAM traffic. Each IP packet is encrypted.

SIP abuse protection: The SBG (P-CSCF, A-ALG) can be configured to enable/disable SIP abuse protection from unregistered users per access network.

SIP Message Throttling

The throttling mechanism in SGC limits the rate of SIP messages to protect core networks from overload, for example, if many users try to register simultaneously.

Uses the *Retry-After* header.

User Agent Whitelists

Lists of user agents (software) that are allowed to register from an access network.

SBG Features 2

- Lawful Intercept
- QoS Assurance
 - Access admission control
 - DiffServ
 - Rq to RACF
 - QoS Logs
 - Codec usage enforcement
- Proxy Registrar
- Optimized authentication
- Geographic location
- Wildcard IMPU
- TISPAN IBCF & P-CSCF

Lawful intercept

Provides for monitoring of both control and media plane traffic.

QoS assurance

Access network admission control is realized via the Diameter-based TISPAN Rq resource reservation interface to A-RACF, ensures that each network is guaranteed the configured share of the SGC session handling capacity and media plane capacity.

The SBG admission control also ensures that links to the SBG are not over-utilized.

DiffServe: Enforcement of operator policies for QoS packet marking: DiffServ (Differentiated Services) code points. DiffServ Enforcement is a function which enforces the priority level for outgoing traffic.

The DSCP value is configured per media type, for example audio or video. DSCP is set individually per stream. The SPDF forwards the DSCP values to the MP. The DSCP values may be remapped by the MP, for external interfaces, or ISER, for internal interfaces.

Enforcement of operator policies for **codec usage**.

User & Network QoS Logs.

Proxy registrar function in A-ALG/P-CSCF

The A-ALG/P-CSCF only permits signaling traffic to and from users who are registered with the core network and to and from IP-PBXs configured in the A-ALG/P-CSCF.

Implicit registration is supported.

Message throttling, which, for example, prevents a registration avalanche overload of IMS core network, by rate limiting in the SBG.

Control plane connectivity supervision, user may be de-registered.

Optimized authentication

Used to decrease the load on the core network by optimizing the amount of authentication. When dialogs are initiated, there is a check to see that the message comes from the same address and port as the UE registered. The message is forwarded to the core network which can be configured to trust that the SBG has verified the source of the message.

Geographic Location:

A-ALG/P-CSCF obtains the geographic location/user information from the CLF and inserts in signaling towards core network; can insert a configured default location.

Wildcarded IMPU:

Support for **wildcarded IMPU** according to 3GPP (TS23.003 & TS23.228).

TISPAN/3GPP IBCF

IBCF controls borders between different multimedia network domains by screening and modifying control plane signaling.

TISPAN P-CSCF

In addition to the limited P-CSCF functionality provided by the A-ALG role, the P-CSCF role also:

- Makes sure it is the first SIP node interfacing the UE, adding and marking its own Via header towards the S-CSCF

- Performs handling P-Preferred-Identity and P-Asserted- Identity

- Performs mandatory usage of preloaded route set (from the Registration procedure) rather than the use of the Route header

- Routes emergency calls to the E-CSCF (pre-configured)

- Removes number portability information in the Request URI from the access/UE.

Provides a first point of contact for users and supports several P-CSCF features such as keeping registration states, identifying emergency calls, generation of P-Charging-Vector and translating between different address spaces.

Mobile/Cable access

The A-SBG in the A-ALG role, can be deployed in front of an Ericsson P-CSCF and act towards and Ericsson Mobile/Cable access network.

- SIP over TLS.

- Hosted NAT traversal (Adds a new 'a' line in SDP with IP/Port of UE.

SBG Features 3

- SIP Message Manipulation
- External BGF
- TISPAN SPDF
- IP-PBX Support
- User & Network Connectivity features
 - NAPT Signalling & Media
 - MSRP header modify
 - Overlapping address space in Access NW
 - Hosted NAT traversal
 - Local Media
 - SIP over SCTP
- Rx Interface
- SIP to H323 signalling conversion
- DNS for dynamic routing

SIP Message Manipulation

The SMM function enables an operator or network integrator to define rewriting rules for SIP messages. SIP message manipulation rules offer a way to add, remove, modify, and repair SIP headers if the message fulfills certain user-defined conditions.

The purpose of the function is to provide the operator an enhanced blacklist and whitelist functionality, protocol repair, and simple application enhancements.

External BGF

Support for distributed SBG configuration in which the controller, SGC and the BGF can be geographically distributed to different locations.

In SBG3.1 the only supported external BGF brand is the *Ericsson SmartEdge BGF*.

TISPAN SPDF functionality

Makes policy decisions using rules defined by the operator. Resource requests are sent to A-RACF and/or BGF.

IP-PBX support

BroadSoft Business Trunking (BT) and Ericsson BT IP-PBX are supported. SBG acts as Registration Surrogate for BroadSoft BT IPPBXs which do not send REGISTER.

H.323 and SIP IP-PBXs are supported. The SBG supports fast connect procedures on the H.323 side, and translates H.323 into SIP.

Recognizes traffic which is going to/from IP-PBXs and applies special handling to messages.

Limits the number of simultaneous sessions for each IP-PBX by operator configuration.

Connectivity to users and networks

NAPT is performed on both *signaling* and *media* streams to facilitate sessions across different address realms.

Modifying Message Session Relay Protocol (MSRP) headers to enable end-to-end inter-working.

Overlapping address spaces in the connected access networks.

Control plane hosted NAT/FW traversal: both SIP registration state management and User Agent (UA) initiated methods to keep ephemeral bindings open in NAT/FW at customer premises and thus ensuring that signaling bound for the UA can traverse NAT/FW at customer premises.

Media plane hosted NAT/FW traversal: enables media packets directed to the user to traverse customer NAT/FW. Makes use of RFC 4145 for TCP based media.

The **Local Media** feature enables SBG to refrain from anchoring media for sessions meeting operator-configured criteria. Saves scarce access network bandwidth.

SIP transport over User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and SCTP (Stream Control Transmission Protocol).

Rx Interface to PCRF

Bearer authentication using Diameter over the Rx interface (3GPP R8).

Network signaling conversion between SIP and H.323

When interfacing an H.323 network, the SBG performs SIP-H.323 and H.323-SIP inter-working using fast connect procedures.

DNS for Dynamic Routing

SIP and H.323 routing by dynamic location of SIP servers by using Domain Name System (DNS); Enables e.g. geographical redundancy on network level.

SBG Features 4

- Early media
- IPTV
- Display contact bindings
- Diameter-based off-line Charging
- Geographic location
- Monitoring session activity
- Geographic redundancy support of other nodes
- Overload protection
- High availability

Early media

Media can be through connected in one or both directions in the SBG prior to an established session. i.e. between INVITE and the final response. For example to allow announcements or tones from the foreign network to be transmitted to the user.

IPTV

Configured either in the A-ALG or in the P-CSCF role, the A-SBG supports IPTV by identifying feature tags in the signalling. The unidirectional media streams (the video) are not anchored in the MP, RTSP control streams are anchored in MP.

Display contact bindings

It is possible for an operator to retrieve from the SBG all Contacts which have been registered for a specific IMPU (IMS Public URI), and also to dump the entire registration database.

Diameter-based off-line Charging in IBCF, A-ALG and P-CSCF

Support of 3GPP/TISPAN Rf interface.

Both control plane information and media plane statistics are reported.

Support of redundant charging servers and buffering of charging data in the SBG if no charging server is available.

Geographic location

Support of Diameter-based TISPAN e2 interface (to CLF).

Location of each IP-PBX is configured in the SBG.

Insertion of geographic location information per user in SIP messages PANI header facilitates service restriction depending on the user's location (for example, Mobility Restriction).

Default Location can be configured.

Monitoring session activity

Both control and media plane activity are monitored in logs, statistics and Performance Measurements. e.g. Forced release of sessions – Reason for release in ACR.

Prevents over-charging and prevents resources being reserved but unused.

Geographic redundancy support of other nodes

Support of other core node geographic redundancy by monitoring the status of each node and selecting the highest prioritized available node.

DNS SRV gives a list of nodes, SBG selects highest priority. SBG supervises SIP to the node, if it fails, SBG switches to the next priority node BUT sends test traffic to failed node to see when it becomes available.

Overload protection

Protection from overloading the SBG with control plane traffic, for example, by message prioritization.

Protection from overloading the core network with control plane traffic, including rate limiting, prioritization of REGISTER messages containing authentication headers, message throttling, and using Retry-After.

High availability

Hot stand-by for redundancy of session handling and media transport.

SBG Features 5

- Architecture for flexible configuration
- Gigabit Ethernet/interfaces
- Performance Management (PM)
- QoS diagnostics and SLA monitoring
- Graphical User Interface
- Netconf interface

Architecture for flexible configuration

Separate signaling and media entities allow the SBG to be efficiently configured with the appropriate capacity, depending on how it is to be used. TISPAN Ia (H.248) is used between signaling and media entities.

The SBG can be configured to have both A-ALG (or P-CSCF) and IBCF roles simultaneously without additional hardware.

The SBG is managed as one functional unit. External BGF is managed separately.

Gigabit Ethernet/interfaces

Control plane, OAM, and DNS are accessed through the IS router function (ISER).

Media plane optionally through dedicated media ports or through IS router function.

Performance Management (PM)

Reporting according to 3GPP PM XML (Extensible Markup Language) format.

Control plane; Media plane, and Processor statistics.

QoS diagnostics and SLA monitoring

Configurable Qos & SLA monitoring.

Counters, gauges, and logs for specific users and aggregated per network.

Graphical User Interface

Easy-to-use Graphical User Interface for SBG OAM.

Netconf interface

Netconf interface for SGC application and for site common function management.

SBG Features 6 - Emergency Calls

SBG Emergency Call Handling Features:

- Session prioritization
- Caller geographic location (PANI)
- Calls from unregistered users
- Session retained at registration expiration
- Reserve media bandwidth
- Release of non-emergency calls

Emergency call handling

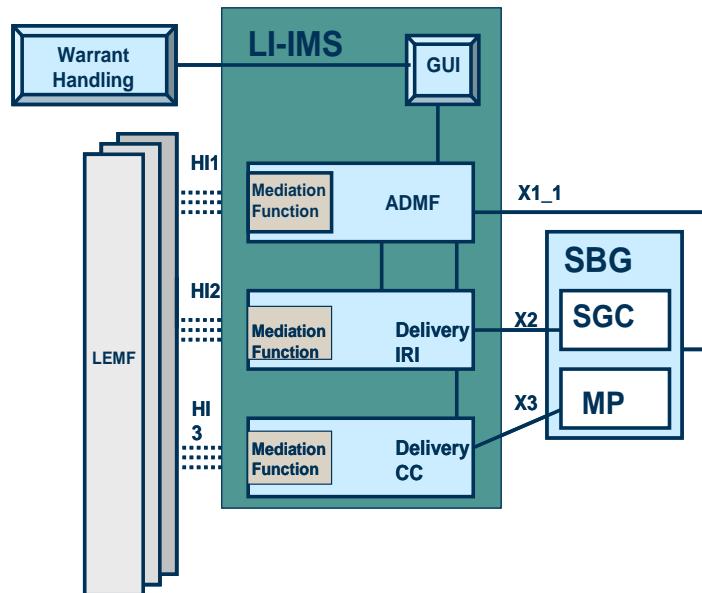
Emergency calls are identified and **prioritized** in both the control and the media planes.

The SBG ensures prompt treatment of emergency calls without affecting session quality.

Emergency telephone and SIP URIs are configured in the SBG and if the Request line matches an Emergency URI, the following is performed -

- **Session prioritization.** The SGC prioritizes processing of emergency call requests internally and includes the SIP Priority header when sending a message towards the IMS core network.
- Insertion of **geographic location** for the caller in SIP messages as received from CLF via the e2 interface.
- When the SBG is configured as a P-CSCF, emergency calls can be routed direct to a **configured E-CSCF**.
- Session establishment from **unregistered users**. The SGC accepts emergency call requests even if the user is not registered in the SGC database.
- Session retained at **registration expiration**. The SGC allows emergency calls to remain standing even if the user registration should expire during the call.
- A portion of the media bandwidth (e.g. 2%) in the MP can be configured as **reserved** for emergency calls. The SGC indicates to the MP via H.248 that a stream belongs to an emergency call.
- If the MP is unable to set up an emergency call due to lack of bandwidth, the SGC releases the longest non-emergency calls (up to seven calls) for the emergency call.

SBG Features 7 - Lawful Intercept



Lawful Intercept

The Lawful Intercept functionality is described in a restricted Function Specification.

The SBG used in both an access and network SBG role will support the Lawful Intercept functionality.

Basically the SBG supports the X1, X2, and X3 interfaces towards the LI Intercept Management System (LI IMS).

SBG Features 8 - TLS

Supports encryption of SIP messages between UE & SGC

- Configured per Access Network
- SBG – TLS Server Certificate
- UA – TLS Client
- SBG & UA Negotiate keys

TLSv1 supported

© Ericsson AB 2010

29

SBG 3.1 Operation and Configuration for IMS

ERICSSON 

TLS

The SBG supports TLSv1 for encryption of SIP messages between UE and SBG. It is configured per access network if TLS shall be applied.

IP-PBXs cannot be connected to access networks with TLS.

The server end (SBG) is configured with a server certificate, which is sent to the client side (UE) at TLS establishment so that the user can authenticate the SBG.

The SBG does not authenticate the user via TLS, as this is done after the TLS tunnel has been set up using the SIP authentication mechanism.

During establishment of the TLS tunnel, the SBG and UE negotiates keys to be used for encrypting SIP signalling.

SBG Features 9 - Accounting Support

- SBG supports the TISPAN defined Rf interface
- Uses Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages
- SBG may add media flow statistics information in ACRs
- Up to ten charging servers

Accounting Support

The SBG supports the TISPAN Rf interface for off-line charging.

Charging information is transferred between the SBG and the Charging Server using the Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages.

The SBG can be configured to add media flow statistics information in Diameter accounting request (ACR) messages. These statistics use Ericsson Vendor Specific AVPs

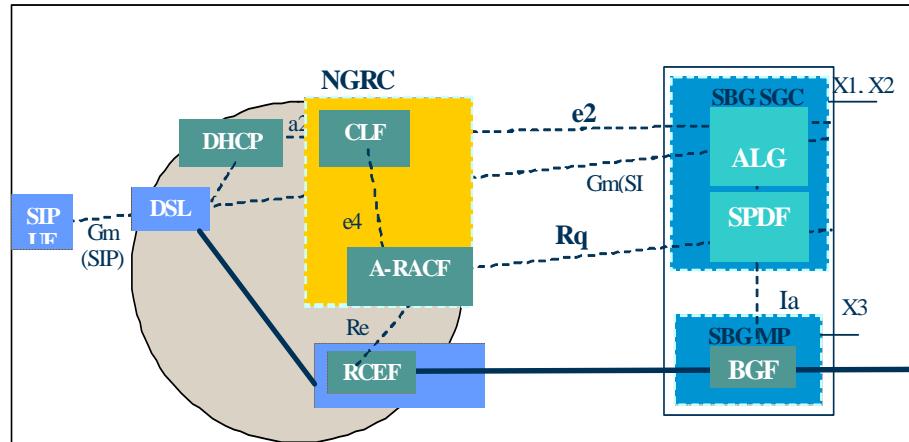
Up to ten charging servers can be configured on the SBG.

During the Capabilities Exchange Request/Answer procedure the charging servers Origin-Host and Origin-Realm are received and are stored on the SBG. These values will be used as Destination-Host and Destination-Realm when performing charging.

If a charging server goes down, the SBG will start buffering charging requests for the ongoing sessions which selected the particular charging server.

The SBG will buffer for one hour per charging server. If all selectable charging servers (obtained from the P-Charging-Function-Address) for a new session have been down for an hour, no charging will be performed but the session will continue.

SBG Features 10 - Location Information Support



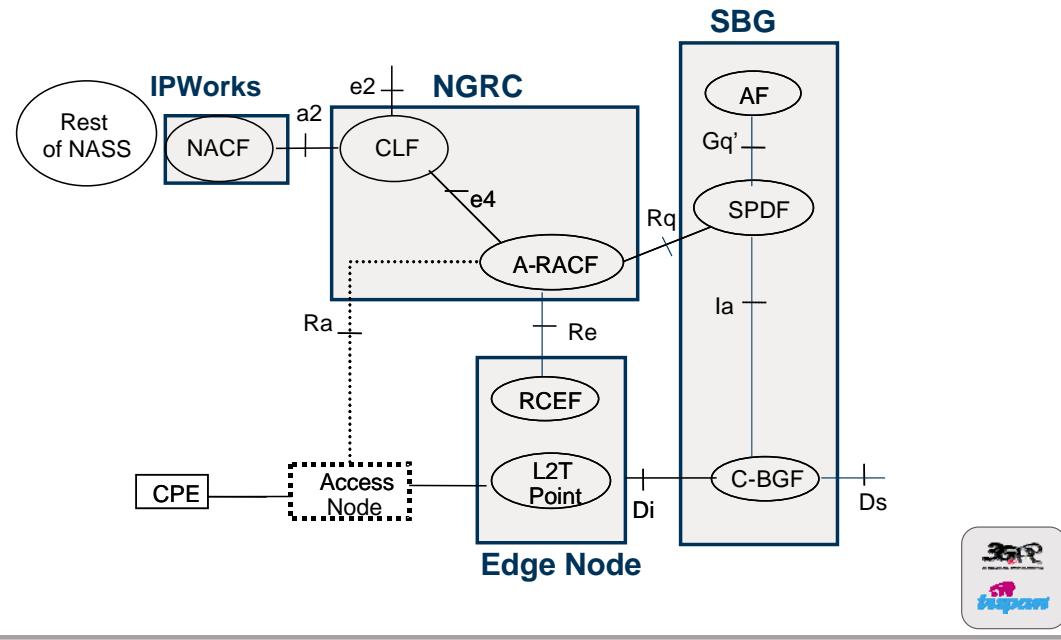
Resource Control Enforcement Function

Location Information Support – e2 support

The A-SBG can be configured to request geographical location information for all registered clients.

This information resides on the Connectivity Session Location and Repository Function (CLF), and the Diameter-based e2 interface is used to retrieve it.

Ericsson Wireline Access IMS Solution



SBG Features 11 - Network Admission Control

- TISPAN defines the Rq interface between the SPDF and the A-RACF. Diameter over SCTP.
- The Rq interface is used by the SBG SPDF functionality to reserve media plane resources in the access network with the A-RACF.
- The SPDF can request resources, modify reserved resources during a session, and release resources at session termination.

Network Admission Control

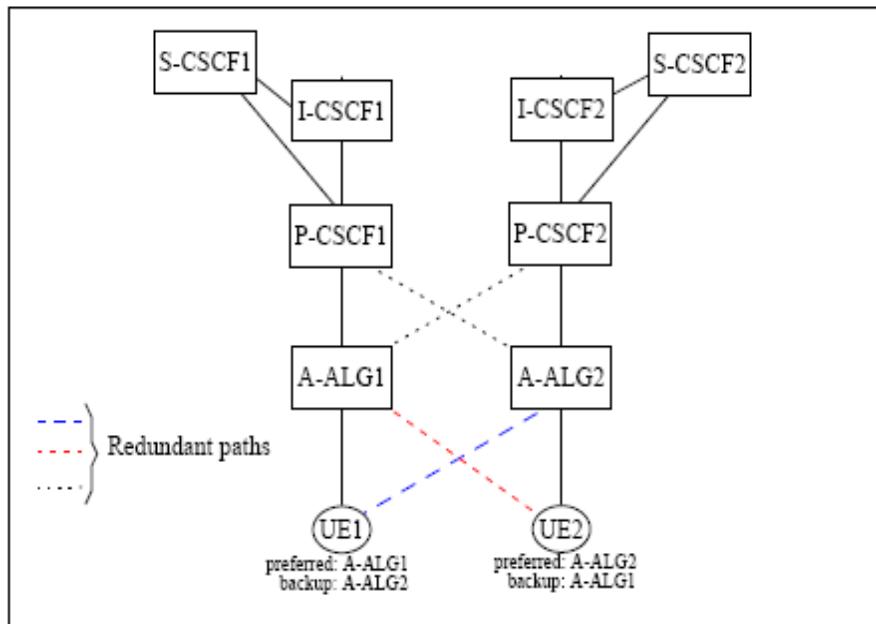
TISPAN defines the Rq interface between the SPDF and the A-RACF.

The Rq interface is used by the SBG SPDF functionality to reserve media plane resources in the access network with the A-RACF.

The SPDF can request resources, modify reserved resources during a session, and release resources at session termination.

The Rq interface is Diameter based and it is transported over SCTP.

SBG Features 12 - SBG geographic redundancy



SBG geographic redundancy

Geographically redundant A-ALGs are shown in the figure above.

A-ALG1 and A-ALG2 are individual blade systems and are geographically separated.

Each UE will have a preferred A-ALG and in the case where a UE loses connection towards the preferred A-ALG, the UE will change to a backup A-ALG.

The backup A-ALG is either locally configured in the UE or received by the UE in answer to a DNS SRV lookup.

P-CSCF Redundancy by DNS

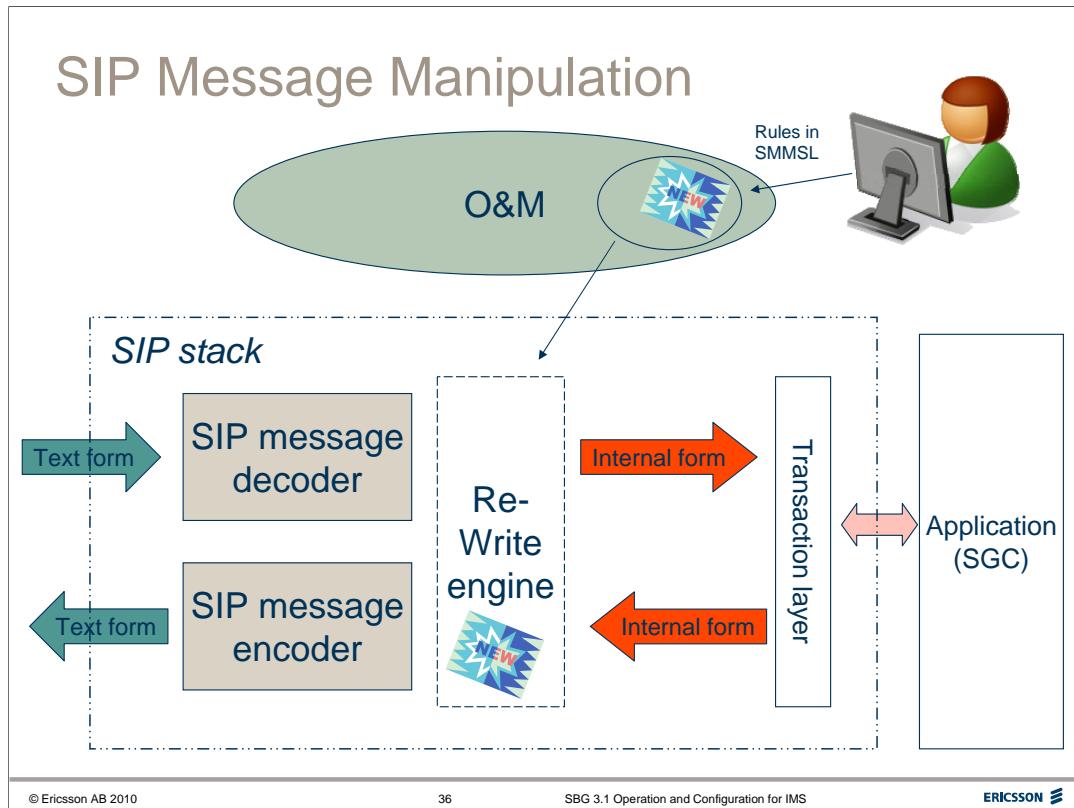
If multiple P-CSCFs are configured, when the SBG performs a DNS query for P-CSCF (using a configured domain for the P-CSCFs), DNS returns IP Address/Port for all P-CSCFs, with priorities. SBG the chooses the highest priority. If the highest priority P-CSCF fails, SBG will use the next highest priority.

SBG 3.1 Operation and Configuration for IMS

SIP Message Manipulation

This section briefly describes the main Principles of the SMM Function.

For more details refer to the SMMSL description.



SIP Message Manipulation

The function of *SIP Message Manipulation (SMM)* allows the operator to define rules that will manipulate incoming and outgoing SIP messages to/from the Session Gateway Controller (SGC).

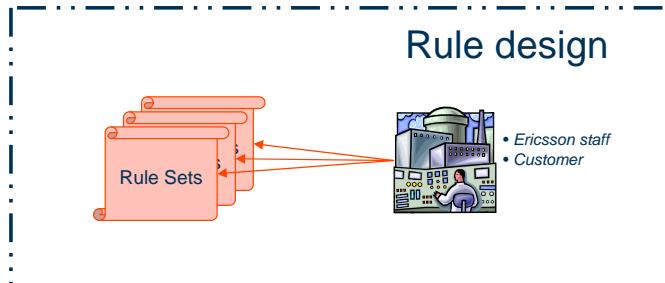
The rules are defined in a text file that will be loaded on the target system.

SIP message manipulation rule sets are written in the **SIP Message Manipulation Scripting Language (SMMSL)** in plain ASCII text files.

The SIP message manipulation is a new feature that has wider range of message handling than the existing Blacklist and Whitelist functions. The new feature can replace these functions if wanted.

The feature can also be used if there is a need to manage a situation where there is an incompatibility with other equipment.

SIP Message Manipulation



The operator defines rules containing matching criteria identifying a specific SIP message, called conditions. If the conditions are fulfilled, the message will be manipulated by specified actions. These actions can be inserting, removing or changing parts of the SIP message and/or the Session Description Protocol (SDP) body.

Rule Sets

Rules are grouped in rule sets. The rules in a set are tried one by one until a rule is triggered, the remaining rules will not be tried. Rule sets are grouped into filters. These filters can have references to the same rule sets. Each network can have two filters assigned to them, one for incoming traffic and one for outgoing traffic.

SIP Repair

As part of the SIP Message Manipulation feature is also a SIP protocol repair function. Currently without SMM, all SIP messages that do not have the correct syntax are rejected by the SIP stack.

The SIP Protocol Repair function extends the SMM feature so that it will be possible to write SMM repair rules specifically targeting messages containing parts that have not passed the SIP standard decoding. These messages will be modified according to SMM repair rules and sent on (if they pass the SIP decoding after repair) to the application.

If the repair fails, a logging function can be invoked to make it possible to see where the repair function failed, and take appropriate actions by changing or adding repair rules etc.

Simple SMMSL Ruleset

```
Ruleset "Add a phone-context to a local number"
  If
    not SIP.request.tel_uri.phone_number ~= '^+.*' and
    not SIP.request.tel_uri;phone-context exists
  Do
    add SIP.request.tel_uri;phone-context := "+46"
  End
End
```

The first condition tests the phone number in the tel URI of the request line
For example, if the request line of the incoming SIP request looks like this:
INVITE tel:087191234 SIP/2.0

Then the request line will look like this after the rule has been applied:
INVITE tel:087191234;phone-context=+46 SIP/2.0

More Examples of SMMSL

```
Ruleset "Reject local number without phone-context"
  If
    is_request and
    not SIP.request.tel_uri.phone_number ~= '^\\+.*' and
    not SIP.request.tel_uri;phone-context exists
  Do
    reject 400 "Bad Request"
  End
End

Ruleset "Check for existence of header fields and parameters"
  If
    SIP.response.code == 200 and
    SIP:required == "timer" and
    SIP:session-expires exists and
    not SIP:session-expires;refresher exists
  Do
    add SIP:session-expires;refresher := "uac"
  End
End
```



ERICSSON

SBG 3.1 Operation and Configuration for IMS

SBG Principles

This section briefly describes the main Principles of the SBG.

More detailed descriptions will be found later in the book, together with configuration and management details.

SBG Principles 1 – Media FW/NAPT

Media Anchoring and Dynamic Pinhole FW/NAPT

- Only passes media packets defined in SDP of existing SIP session – Dynamic Pinhole Firewall
- Media Anchoring – forces all media streams through the Media Proxy (except Local Media if configured)
- Performs address and port translation (NAPT)

Media Anchoring and Dynamic Pinhole FW/NAT for Media

A main feature of the SBG is that it only passes media packets through if they belong to a media stream defined in the SDP of an existing SIP session - i.e.. the SBG acts as a “*dynamic pinhole firewall*” for IP based media streams.

The SBG handles set-up of media streams in connection with the initial INVITE and release of these media streams in connection with BYE.

The SBG also handles mid-session set-up and release of media streams, as well as mid-session re-negotiation of SDP parameters which may result in change of bandwidth policing values.

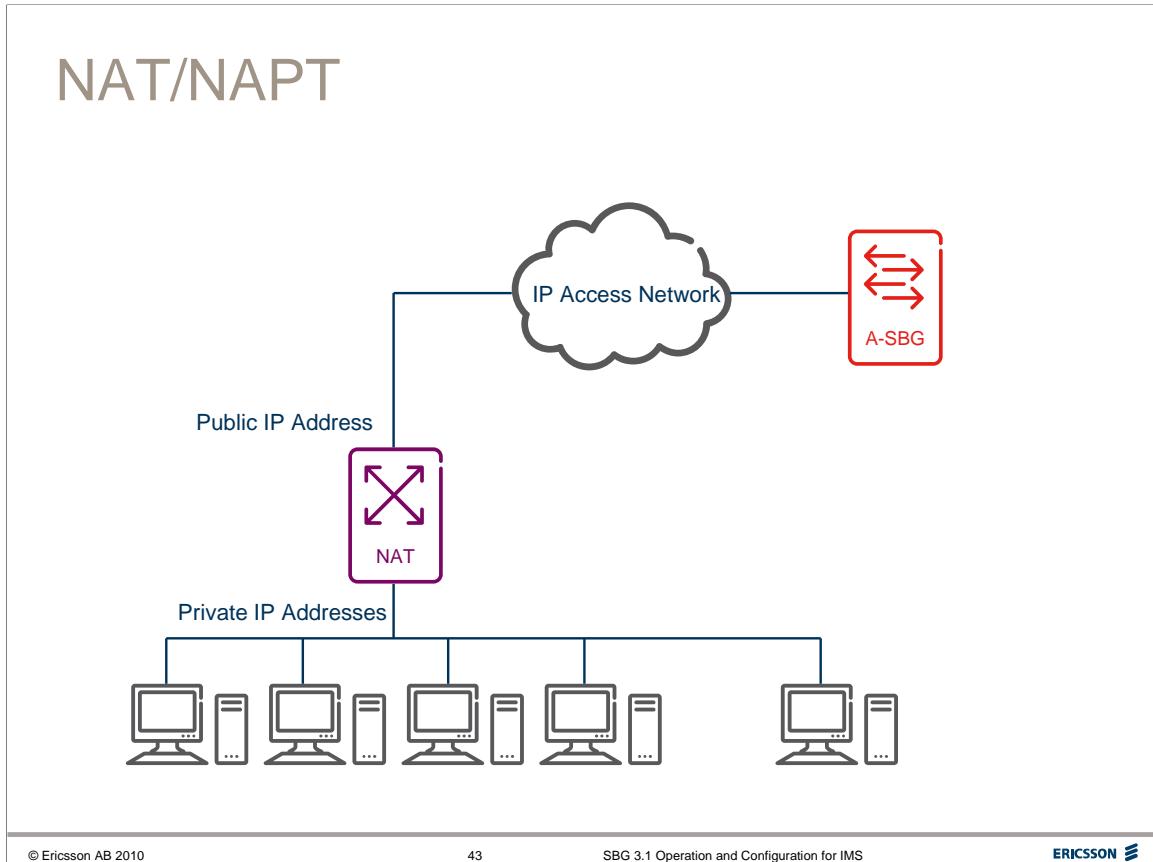
It is the Media Proxy that opens and closes media pinholes through the SBG, and there is therefore a need to drive all media stream paths through the Media Proxy.

In order to do this the SGC performs what is referred to as “*media anchoring*”, where the SGC acts as an SDP proxy by modifying address and port information, in order to allocate local Media Proxy address/port pairs for the incoming and outgoing directions of the media stream, in both directions. The selected proxy address/port pairs for media are then returned in the SDP of e.g. a 200 OK by the SGC

The result of the above is that the Media Proxy, in addition to dynamic pinhole firewalling also performs network address and port translation - NAPT - the SBG will be a “Dynamic Pinhole-FW/NAPT” for media.

Local Media

The A-SBG can be configured to allow media between certain users in the same access network not to be anchored.



Firewall

A **Firewall** protects the resources of a private network from users from other networks. The firewall examines each network packet to determine whether to forward it toward its destination. There are a number of firewall screening methods; basic packet filtering can be configured to **Allow** or **disallow** received IP packets based on, for example:

- The source **IP address**
- The destination **port**
- The **protocol**.

Network Address Translator (NAT)

NAT translates User Private IP Addresses to a single (or several) Public IP Address(es). This allows many Users to effectively ‘share’ a single Public IP Address and so save Public IP Addresses in the IP Network.

Network Address and Port Translator (NAPT)

NAPT is a variation of NAT. NAPT extends the functionality of NAT by also translating the transport identifier (eg TCP and UDP port numbers, ICMP query identifiers). This allows the transport identifiers of a number of private users to be multiplexed into the transport identifiers of a single public IP address.

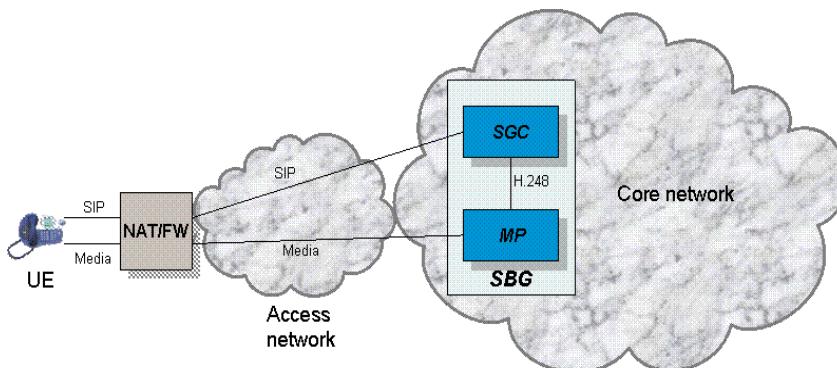
For packets outbound from the private network, NAPT would translate the source IP address, source transport identifier and related fields such as IP, TCP, UDP and ICMP header checksums.

For inbound packets, the destination IP address, destination transport identifier and the IP and transport header checksums are translated.

SBG Principles 2 – Hosted NAT Traversal

Hosted NAT/NAPT and FW Traversal

- The SBG ensures that signalling and media bound for the UE can traverse a NAT/FW located at customer premises
- NAT/FW detected when the A-ALG receives a SIP REGISTER message from the UE with different source addresses in the IP and SIP headers



Hosted NAT/NAPT and FW Traversal

SIP clients in home or enterprise networks are often located behind a customer premises NAT/FW. This poses problems for inbound SIP and Media traffic to the SIP clients, since inbound sessions (to clients) will be typically blocked; a NAT/FW can only be “opened” by outbound traffic.

To manage this, once a NAT binding is established during the SIP client Registration, this binding must then not be allowed to time out – which usually happens after 30 sec to 5 min (different for different NATs) if there is no IP traffic over this specific binding.

A-SBG therefore supports ‘Hosted FW traversal’ through the NAT/NAPT or ordinary firewalls (FW) by allowing or even forcing the SIP access UE to frequently re-register to A-SBG, for example every 1-5 minutes. The SBG discards these re-Registrations, only forwarding them with the frequency agreed with the IMS core nodes e.g. once an hour.

The effect is that the “pinhole” through the remote FW is kept open for SIP signalling - without causing the IMS core network S-CSCF and the HSS nodes to constantly process the SIP re-REGISTER messages sent only for keeping the remote FW pinhole open. The frequent re-registration can be forced, since re-REGISTER timeout towards the SIP UE is operator configurable.

Alternatively the SIP clients can send a SIP message containing only a CRLF character or send empty UDP packets. The two SIP client options are recommended since they cause much less load on the SGC blades than re-registrations.

Example Register Signalling

```

Internet Protocol, Src: NAT (147.215.1.99), Dst: SBG_SIP_Public_VIP (195.186.14.132)
User Datagram Protocol, Src Port: 64612 (64612), Dst Port: sip (5060)
Session Initiation Protocol
  Request-Line: REGISTER sip:edu.ims.se;transport=udp SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 192.168.1.34:2051;branch=z9hG4bK-qsoeilcobt5d;rport
    From: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>;tag=uh1l6irxms
    To: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>
    Call-ID: 3c26700f99cf-x4kkws5ejsgn@snom320-000413241F8A
    CSeq: 997 REGISTER
    Max-Forwards: 70
    Contact: <sip:+4687130151@147.215.1.34:2051>;q=1.0;
    User-Agent: snom320/SC0825
    Expires: 3600
    Content-Length: 0

Internet Protocol, Src: SBG_SIP_Private (192.168.3.150), Dst: P-CSCF (192.168.3.217)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Request-Line: REGISTER sip:edu.ims.se;transport=udp SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 192.168.3.150:5060;branch=z9hG4bKmlu892010g10acgm42o.1
    Via: SIP/2.0/UDP 192.168.1.34:2051;received=147.215.1.99;branch=z9hG4bK-qsoeilcobt5d;rport=64612
    From: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>;tag=SDpqbh501-uh1l6irxms
    To: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>
    Call-ID: SDpqbh501-164ec1f45ada2a65db45823f46076baf-cd44eb2
    CSeq: 997 REGISTER
    Max-Forwards: 69
    Contact: <sip:4687130151@192.168.3.150:5060;transport=udp>;q=1.0;
    User-Agent: snom320/SC0825
    Expires: 3600
    Content-Length: 0
    Route: <sip:192.168.3.217:5060;lr>

```

The signalling example above shows the REGISTER received by SBG from a user behind a NAT and proxied to the P-CSCF.

Notes:

1. The trace has been edited for the example.
2. The Contact header is changed to the SBG Private IP & Port.
3. The SBG adds the NAT Ip & Port to Alice's VIA header.
4. The Call-ID has changed as this is a new signalling leg.

Example Register Signalling – 200 OK

```

Internet Protocol, Src: P-CSCF (192.168.3.217), Dst: SBG_SIP_Private (192.168.3.150)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Status-Line: SIP/2.0 200 OK
  Message Header
    To: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>;tag=cce179b407a900819de354864634
    From: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>;tag=SDpqbh501-ulhl6irxms
    Call-ID: SDpqbh501-164ec1f45ada2a65db45823f46076baf-cd44eb2
    CSeq: 997 REGISTER
    Content-Length: 0
    Via: SIP/2.0/UDP 192.168.3.150:5060;branch=z9hG4bKmlu892010g10acgm42o0.1
    Via: SIP/2.0/UDP 192.168.1.34:2051;received=147.215.1.99;branch=z9hG4bK-qsoeilcoubt5d;rport=64612
    Contact: <sip:+4687130151@192.168.3.150:5060;transport=udp>;q=1;
    P-Associated-URI: <sip:+4687130151>
    P-Associated-URI: <tel:+4687130151>
    P-Charging-Function-Addresses: ccf="aaa://mm.edu.ims.se:3868;transport=tcp"
    P-Charging-Vector: icid-value=cce179b40b41770819de3546dc2e2
    Expires: 3600

Internet Protocol, Src: SBG_SIP_Public_VIP (195.186.14.132), Dst: NAT (147.215.1.99)
User Datagram Protocol, Src Port: sip (5060), Dst Port: 64612 (64612)
Session Initiation Protocol
  Status-Line: SIP/2.0 200 OK
  Message Header
    Via: SIP/2.0/UDP 192.168.1.34:2051;received=147.215.1.99;branch=z9hG4bK-qsoeilcoubt5d;rport=64612
    From: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>;tag=ulhl6irxms
    To: "ALICE" <sip:+4687130151@edu.ims.se;transport=udp>;tag=SDpqbh599-cce179b407a900819de354864634
    Call-ID: 3c26700f99cf-x4kkws5ejsgm@snom320-000413241F8A
    CSeq: 997 REGISTER
    Content-Length: 0
    Contact: <sip:+4687130151@147.215.1.34:2051>;expires=120;q=1;
    P-Associated-URI: <sip:+4687130151@edu.ims.se>
    P-Associated-URI: <tel:+4687130151>
    Expires: 120

```

The figure above shows the 200 OKs for the Register received by, and proxied on by SBG.

Notes

1. The trace has been edited for the example.
2. The SBG has enforced a reduced 'Expires' value.
3. Topology hiding of the Via and Contact headers.
4. P-Charging headers have not been forwarded.

SBG Principles 3 – Media Latching

Media Packet address Latching

- SGC controls the media flow through the MP
- SGC can only see the user's IP address & port for media in SDP
- SBG can request the MP to ***latch*** to the first media IP packet received from the user

Media Packet Address Latching

The SBG can determine the user's IP address and port for signalling from the SIP headers and, in the case of a user behind a NAT, from the IP packet source address & port. The SBG can also determine the user's IP Address and Port for media from the SDP body. However if the user is behind a NAT, this will not be identified in the SDP since a NAT cannot alter SDP.

Latching is used to obtain the IP address and port used by a NAT on behalf of a user behind the NAT.

When setting up media streams through the MP to a user behind a remote NAT/FW, the SGC orders the MP (in the H.248 signalling) to perform ***latching***. The source IP address and port of the ***first media packet received*** from that user is then used in the BGF for sending packets to the user and for the dynamic pinhole firewall when accepting packets from that user.

For security reasons, latching is only automatically ordered when a NAT/FW has been detected. However, if required, latching can be configured to be applied for all sessions.

SBG Principles 4 – DNS Routing

- **DNS based SIP and H.323 routing**

A-SBG

- If the address of the P-CSCF (the outgoing proxy) is configured as a service name in the A-SGC, it is resolved by DNS
- If the route set was built using a domain name of the user (from the Contact), the A-SGC looks up the domain name using DNS

N-SBG

- The routing decision is based on the Route header if present, otherwise on the SGC configured outgoing proxy, and if no outgoing proxy has been configured, the decision is based on the Request Uniform Resource Identifier (URI).
- If needed, service names are resolved by DNS
- The usage of service names and DNS rather than static IP addresses enables load distribution between CSCFs in the communication with foreign networks.
- The DNS server is located outside the IS infrastructure.

DNS based SIP and H.323 routing

Each SGC has signalling interfaces to two networks

The A-SGC has one or more interface(s) to the access network and one interface to the IMS core network.

The N-SGC has one interface to the IMS core network and one or more interface(s) to the foreign network.

The actual destination address to which SIP and H.323 messages are sent is resolved in different ways depending on the network and the phase of the dialog. For example:

A-SBG

At initial registration, the A-SGC performs DNS queries of the user's domain to obtain the IP address and port for the P-CSCF to use. Multiple P-CSCFs can exist, and their details and priorities are returned by DNS. SBG selects the highest priority and stores the route set between the NAT/FW address of the user (if the user is behind a NAT/FW) and the address of the P-CSCF.

If the user is not behind a NAT/FW, the A-SGC stores a route set between the *Contact* information provided by the user at the initial registration and the address of the selected P-CSCF.

If the address of the P-CSCF is configured as a service name in the A-SGC, it is resolved by DNS using NAPTR (Naming Authority Pointer) records, SRV records, and A records in accordance with RFC 3263.

SBG Principles 5

- **Proxy Registrar**
 - User must be Registered in IMS Core.
- **Registration**
 - SBG handles registration from Users
 - Also handles implicit registration
- **SIP REGISTER message throttling**
 - Prevents IMS core networks from being overloaded
 - 500 Server Internal Error with *Retry-After* field
- **Optimized authentication**
 - Allows S-CSCF to refrain from authenticating users at every SIP transaction

Proxy Registrar

The SBG will only allow a User access to IMS Services if the User Agent is Registered. Emergency calls are accepted from non-registered users, if configured in SBG.

Registration

The A-SBG **Proxy Registrar** function keeps track of the registration state of users in the access network served by the A-SCG.

To Register, a user sends a SIP REGISTER to the A-SBG, which forwards the message to the P-CSCF (or to the I-CSCF if the SBG is configured as a P-CSCF) if the user is not already registered. The IMS Network may require authentication which is also proxied through the SBG, and thereafter the user is registered.

When SBG forwards the 200 OK message to confirm the successful registration to the user, the SBG also stores the registration information in the SGC internal database.

Shorter re-registration timers may be used in the Access Network than in the IMS Core Network, for example to keep a hosted NAT/FW open. If a user re-registers with the same registration information while still having a valid registration with the core network, the SBG responds to the user with a 200 OK without forwarding any message to the IMS Core Network.

If a user with a valid registration, re-registers with a different set of information (for example, using a different source IP address) the SBG forwards the re-registration to the P-CSCF. If the re-registration is accepted, the SBG updates the SGC database.

Implicit Registration

Implicit registration means that a UE may send a REGISTER with a single public user identifier (PUI) but the IMS Core may respond with multiple PUIs which are all associated with the user.

The A-SGC then considers all PUIs received from P-CSCF as registered and reachable via the same UE as the REGISTER message was sent from.

SIP REGISTER message throttling

The throttling mechanism in SGC rate limits REGISTER messages to prevent IMS core networks from being overloaded.

If the REGISTER transaction window becomes full, the SGC does not accept new REGISTER messages to the IMS core network but rejects them with SIP final response **500 Server Internal Error** which includes a **Retry-After** header.

The N-SGC throttles all registration messages while the A-SGC throttles initial registration messages only.

Optimized authentication

The A-SGC Proxy Registrar provides support for optimized authentication by allowing the S-CSCF to refrain from authenticating users at every SIP transaction.

This is possible as the A-SGC checks the source IP address of every SIP message coming from the access network to ensure that the originator is registered in the proxy registrar. If the user is behind a NAT/FW, both address and port are checked.

If the operator, despite the optimized authentication function in the A-SGC, configures the S-CSCF to challenge authentication for certain SIP methods, the A-SGC relays the needed information.

SBG Principles 6

- Overlapping Address Space
- Connectivity Supervision
- Late Media Handling
- Mobility Restriction

Overlapping address space

SBG supports overlapping IP addresses on VPNs connected towards external networks (including IP-PBX's) without losing any SBG functionality.

SBG supports 500 overlapping address spaces in total

Connectivity supervision

If the client does not re-register within the defined time the connectivity will be seen as lost and the client will be de-registered both towards IMS Core and within A-SBG.

Late Media Handling

After the connection is released the used resources are put in quarantine for 20 seconds. During this time any received late media will be discarded. After the 20 seconds interval resources will be released and made available for new connections.

Any late media after 20 seconds will be treated as malicious packets

Mobility Restriction

SBG has the possibility to configure individual geographical locations for each connected access network. The geographical location information will be inserted into a PANI (P-Access-Network-Info) header for all INVITEs sent towards the core network.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

SBG 3.1 Security & QoS

This section describes some of the main SBG Security features and QoS in more detail.

Security 1 – Topology Hiding

- SIP headers can be hidden:
 - Via
 - Contact
 - Record-Route
 - Path
 - Service-Route
- Media Proxy
 - c- line IP address
 - m- line IP port

Topology Hiding

Topology hiding means that no IP addresses concerning one network are allowed to be forwarded in signalling messages to another network.

The A-SBG hides the core network topology from the access network nodes, but lets the SIP access network information topology through to the IMS core network.

The N-SBG allows the operator to define separately, for each network, if the topology information from the Core network shall be revealed or hidden towards the Foreign network and vice-versa.

The topology hiding can be configured in A-ALG and IBCF to remove the following headers to hide the network topology:

- Via
- Contact
- Record-Route
- Path
- Service-Route

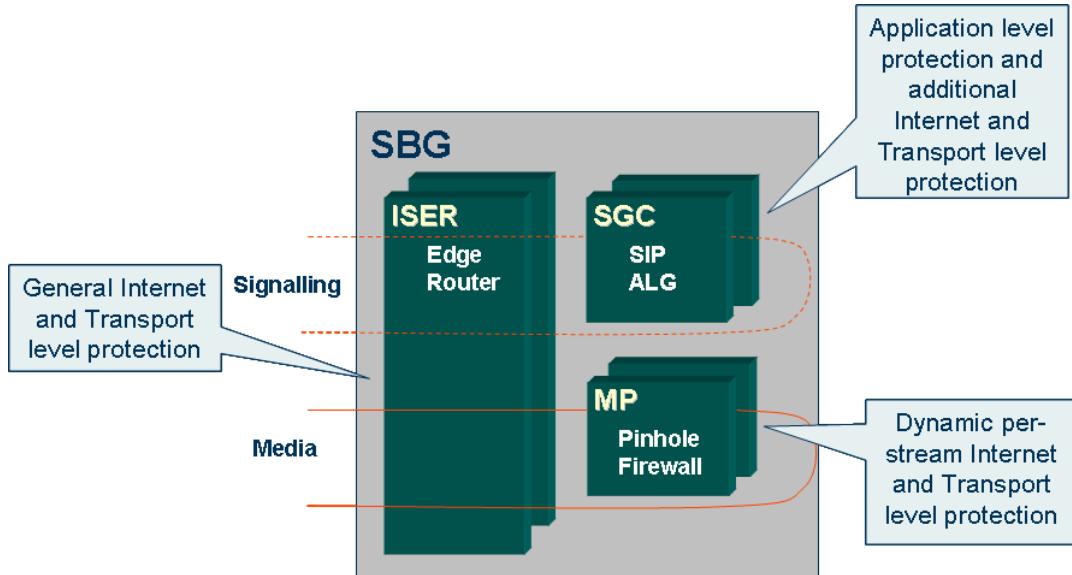
Topology hiding for each header can be switch on or off individually per network.

Note if the A-SBG is in P-CSCF mode, topology hiding cannot be changed. Topology hiding to the Access network is on for all headers and off towards the Core network.

The **Media Proxy** function hides the network topology by proxying the media packets between the two networks and so hides the real senders/receivers for the media packets. Topology hiding is achieved by modifying the following in SDP:

- Connection IP address (c- line)
- Connection IP port (m- line)

Security 2 – DoS Attacks



Protection against IP DOS attacks

The IS-based SBG protects the perimeter of the network and so is itself a prime target for attacks. The DOS protection functionality is distributed over the node as shown in the figure above.

ISER

The packet filter on ISER provides a stateless packet filter function. Packet filter can be applied to an interface as ingress, egress or both.

This is fully described in the Integrated Site training courses.

SGC

The SGC performs additional **IP packet filtering**. Incoming traffic is filtered based on SGC local address and port. Incoming traffic can be rate limited per client in the A-SBG (source IP address & port and destination address & port).

Protection against **TCP SYN** attacks is also supported using TCP SYN cookies.

Application level protection is achieved by topology hiding, a SIP parser checking the syntax of SIP messages, and a number of SIP user checks/filters (when acting as an A-SBG).

Overload protection is performed and incoming SIP requests are rejected at overload. Priority is applied by e.g.. having SIP REGISTER, and other messages not related to ongoing calls, on a lower priority.

Security related events are **logged**.

Other DoS Protection Features in SGC Include:

SIP Header Blacklists

Media Anchoring

Check of IP addresses in Messages

Transmission Timers

Control Plane (Signalling) Flooding

The SBG contains features for protecting the core network from traffic flooding.

The following steps are taken to block control plane traffic attacks:

- The ISER rate limits the total amount of traffic received from each network to SGCs.
- The SGC performs rate limitation for each source address and port in all networks. If too many packets arrive within a certain time from a single source address and port or single address only, it is assumed to be an attack attempt. Packets exceeding the rate limits are discarded.
- If the SGC detects flooding from an access or foreign network and the blocking policy is set, the SGC blocks all traffic from the offending address and port for a configurable time.

In addition, if the SGC detects flooding from an *Access Network*, the UE registered on the offending address and port is deregistered and put into quarantine so that the user cannot register again for a configurable time.

Blocking Media Plane IP Flooding

For media traffic, the MP dynamic pinhole firewall performs ***bandwidth policing*** on a per-stream basis, which means that any excessive media traffic due to IP flooding is effectively stopped. The MP blocks flood attacks from single IP source, discards excessive packets, logs details and generates alarms.

Other Media Proxy Features

Actions are taken for media by the MP on a per-stream basis.

TLS

IPSec

NAT is applied for topology hiding.

Source and destination filters are applied on internet and transport levels.

Security 3 – Malicious and Late Media

- Late Media
- Invalid Source
- Detection of media stop
- SIP session timer
- Alarms

Handling of Malicious and Late Media

Late Media

When a media stream is removed or a pinhole is closed in the MP, the end user may still send packets for a while. This traffic is called *late media*.

These packets are only discarded, not treated as malicious. The closed TCP/UDP port remains in quarantine for 20 to 40 seconds. If late media arrives after the quarantine it is regarded as malicious and logged in mpMaliciousTrafficLog

Invalid Source

For security reasons, a Media Proxy will discard all packets arriving on an open pinhole if the source IP/port of the packet is not the one negotiated through SDP (or the one latched to in the NAT traversal case).

If media packets from multiple sources are received on the same pinhole, the packets with illegal source address/port will be discarded.

Detection of Media Stop

Media Stop Detection can be configured in the SBG per network.

The BGF will be instructed to supervise each termination to detect if media has stopped for a configured time in a specified direction.

Different timer values will be used depending on whether the session is on hold or not.

If the BGF detects that no media has passed through the dynamic pinhole firewall for a time it notifies the SGC via H.248.

When the SGC receives a media stop notification it will see if the Media Stop Client Check is active, and if so:

- The SGC will send a SIP Options message towards each client in order to determine if the session is still active on the client. Note that this additional check does not really confirm that the client is generating media or that media is not being lost elsewhere in the network but it does confirm that the client is active with the session for which the media stop was reported.
- If positive responses are received to both SIP client checks (2xxOK values) then the media stop is ignored.
- If a negative response is received to either SIP client check (timeout, any non-positive response) then the media stop event is actioned i.e. the session is released.

SIP session timer

The SGC supports the RFC 4028 SIP session timer and monitors that the user agents comply with SIP session timer values if the user agents negotiated to use this functionality.

If the SGC detects session expiry, it sends **SIP BYE** in both directions and orders the MP to release the resources.

Alarms

In the case of ongoing late media, malicious media or invalid source, there is an option to raise an alarm, to allow the operator to follow up by checking the logged information.

QoS Assurance

- **Bandwidth reservation**
 - Based on Codec definitions.
 - Tells MP with 'b=' parameter in SDP.
 - Unknown Codecs – remove or assign generic bandwidth
- **QoS marking**
 - DiffServ
 - SBG sets DiffServ priority.
 - VLAN
 - SBG sets VLAN ID and p-bits (Priority Markers in Ethernet frames)

QoS Assurance

Bandwidth reservation per media stream

For each media stream, the SBG B2BUA function sets a bandwidth parameter for Connection Admission Control purposes when reserving resources for media pinhole from the MP function. The bandwidth decision from the SBG B2BUA function is communicated to the MP function with H.248 signalling.

It is set on media stream level with the ***b= parameter*** in the H.248 Local SDP descriptor.

For each media stream the SBG B2BUA function also defines the maximum sustainable data rate for policing purposes. The sustainable data rate decision from the SBG B2BUA function is communicated to the MP function with H.248 signalling. It is set on media stream level with the ***msf-tman/sdr*** and ***msf-tman/pol*** properties included in the H.248 Local Control.

For RTP and T.38 media, policing parameters in the form of peak bandwidth allowed for the media stream are calculated by the SGC from the information received in SDP. The policing bandwidth value is then sent down to the Media Proxy through the H.248 communication.

Calculating what bandwidth value to use for call admission control and for policing for a specific media stream can often only be done for media encoding types that are known by the SGC, since the SDP does not normally carry information on needed bandwidth.

Unknown Codecs

It is possible by configuration to add information for new codecs and their bandwidth needs in order not to wait for an SBG software update.

If SDP in a SIP INVITE lists a codec not known to the SGC, the SGC can handle this by either

- Removing the codec from the SDP codec negotiation
- Assigning generic bandwidth values for call admission control respectively for bandwidth policing for the media stream. The values are based on generic provisioned system parameters. If no values have been provisioned the media stream is rejected.

QoS marking

QoS marking is performed to enforce operator QoS marking policies, to provide real-time critical traffic with priority transport.

DiffServ

The SBG set DiffServ marking in outgoing packets. Possible QoS remarking is then performed in the ISER. The re-marking should be according to a provisioned scheme, which can be different towards the access network respectively towards the core network.

The SBG is able to provide differentiated QoS marking for the different traffic types listed below.

Since different operators may have different schemes for QoS marking, the actual QoS markings used by SBG will be configurable (default settings will be provided):

- RTP audio and T.38 fax
- RTP video
- SIP
- MSRP

VLAN

When interfacing to a VLAN based access network, the SBG must set the VLAN ID and the p-bits.

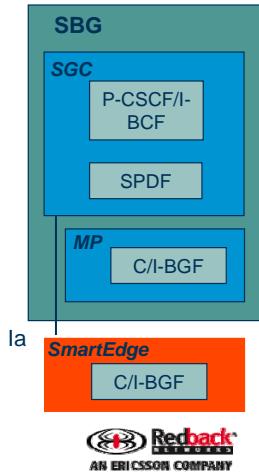
In this case this marking is done according to a provisioned scheme.

Distributed SBC

Redback SmartEdge – SBG
SBG 3.1

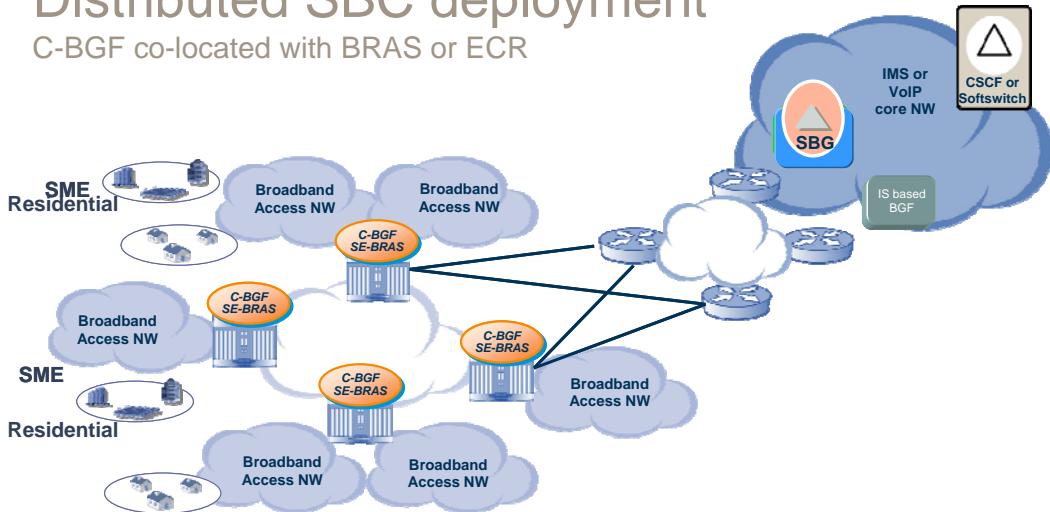
High Level Solution Description

- Distributed SBC utilizes the strength of 2 standalone products:
 - Redback Access Edge router – **High throughput**
 - Ericsson Session Border GW - **Signaling intelligence**
- Standard compliant Ia interface.
- SmartEdge is not a replacement for the IS based MP.
- The BGF is an Optional SW on SmartEdge – requires no HW upgrade.



Distributed SBC deployment

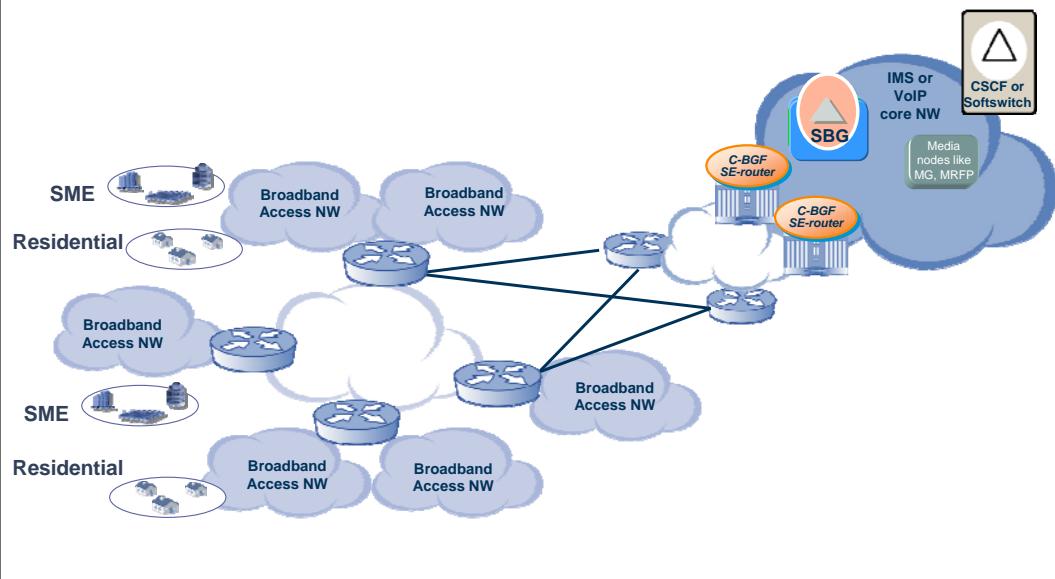
C-BGF co-located with BRAS or ECR



- Customer advantage
 - no media tromboning,
 - no added Jitter/latency,
 - no wasted bandwidth/ports on line cards and in transport network

Distributed SBC deployment

C-BGF co-located with general router



SBG 3.1 Operation and Configuration for IMS

SBG 3.1 Roles

The SBG can be configured to perform three roles in the IMS Network:

A-ALG - Access Application Level Gateway between Access Networks and the IMS Core Network.

P-CSCF – Proxy Call Session Control Function. This is a combined A-ALG & P-CSCF Functionality between Access Networks and the IMS Core Network.

N-SBG – Network Application Level Gateway between Foreign SIP/H323 Networks and the IMS Core Network.

Roles of A-SBG

- **Security**
 - Dynamic pinhole firewalling
 - Bandwidth policing
 - Topology hiding
 - Protection against DOS attacks
 - TLS encryption of signalling traffic
- **QoS assurance**
 - Perform specific admission control
 - Enforce operator policies for QoS packet marking
- **Hosted NAT/FW traversal**
 - To ensure that inbound signalling and media can traverse to customer premises FW/NAT
- **Regulatory requirements**
 - Emergency call handling, location information and Lawful Intercept
- **Charging**
- **P-CSCF**

Roles of A-SBG

When interfacing between the SIP core network and a home/enterprise based SIP clients in an IP access network, it is essential to be able to funnel the SIP signalling and media streams via an A-SBG in order to obtain:

Security

- *Dynamic pinhole firewalling*
- *Bandwidth policing* per media stream
- *Topology hiding*
- *Protection against DOS (Denial of Service) attacks*
- *TLS encryption of signalling traffic*

•QoS assurance

•Hosted NAT/FW traversal

•Charging

•Regulatory requirements

Emergency calls

Lawful Intercept

•e2 reference point support to CLF

P-CSCF functions

The A-ALG can be configured to perform the TISPAN P-CSCF role in IMS

Roles of N-SBG

- **Inter-operator peering**
 - Recognizes and knows parameters related to RTP media
 - Recognizes and knows parameters related to MSRP media
- **Network signalling conversion between carriers and corporate networks**
 - At a border to an external H.323 network, the N-SBG performs SIP-H.323 inter-working between the networks using *Direct Gateway-Gateway Routing* model.
- **IP address translation**
 - When necessary, the N-SBG performs translation between public and private IPv4 addresses.

Roles of N-SBG

At the border between different carriers IP networks, the N-SBG provides a generic IMS NNI for VoIP, video and messaging. In addition to previously described A-SBG functionality, the N-ABG supports:

Inter-operator peering

Recognizes and knows parameters related to video and voice codec-s (RTP) used in WeShare and PTT.

Recognizes and knows parameters related to MSRP media.

Network signalling conversion between carriers and corporate networks

At a border to an external H.323 network, the N-SBG performs SIP-H.323 inter-working between the networks using *Direct Gateway-Gateway Routing* model.

From the H.323 network point of view it acts as a *remote H.323 gateway* (GW).

IP address translation

Charging

Rf Diameter.

Roles of P-CSCF

The A-SBG can perform the TISPAN P-CSCF functions:

- Forwarding of the SIP REGISTER request received from the UE
- Forwarding of SIP messages received from the UE to the SIP server
- Forwarding of the SIP request or response to the UE
- Detection of and handling an emergency session establishment requests
- Maintain a Security Association between the P-CSCF and each UE using TLS
- Authorization of bearer resources and QoS management
- Changing the appropriate SIP/SDP parameters in order to translate addresses into the same or different IP version addresses

P-CSCF

A-ALG can be configured to perform the role of P-CSCF functions specified by TISPAN.

The A-ALG and 3GPP P-CSCF together provide the P-CSCF functions needed to serve a TISPAN access network.

The main functions performed by the SBG based P-CSCF are:

- *Forwarding of the SIP REGISTER request received from the UE to an entry point determined using the home domain name, as provided by the UE.* The A-ALG routes REGISTER messages to the separate P-CSCF using the A-ALG configuration or the home domain name provided by UE.
- *Forwarding of SIP messages received from the UE to the SIP server (e.g. S-CSCF) whose name the P-CSCF has received as a result of the registration procedure.* The A-ALG routes messages according to route set stored at registration. This will typically point at the separate P-CSCF.
- *Forwarding of the SIP request or response to the UE.* The A-ALG routes requests and responses to the UE according to the route set stored at registration.
- *Detection of and handling an emergency session establishment requests.*
- *Acting as an ALG by changing the appropriate SIP/SDP parameters in order to translate addresses into the same or different IP version addresses.*

Compliance with ETSI TISPAN

- A-SGC performs P-CSCF and SPDF functions
- MP in A-SBG performs the role of C-BGF
- N-SGC performs IWF, IBCF and SPDF functions
- MP in N-SBG performs the role of I-BGF

TISPAN NGN/IMS Functional Architecture

The SBG3.1 supports P-CSCF functionality for TISPAN defined access to IMS, i.e. for access to/from IMS through fixed broadband access networks.

The P-CSCF functionality is defined by 3GPP for mobile access to IMS and is mainly described in 3GPP TS 24.229.

P-CSCF functionality for broadband access to IMS (TISPAN P-CSCF) differs in some aspects from 3GPP P-CSCF functionality. The main differences are the following:

- For broadband access the SGC supports the P-CSCF functionality described by 3GPP with the exceptions of the mobile access specific features of IPsec security associations, SigComp and Rx interface towards a mobile access policy control system.
- The SGC also supports the TISPAN I-BGF and IWF functional entities for the IMS NNI; the IWF supporting interworking with H.323 networks
- The Media Proxy supports the TISPAN C-BGF and I-BGF functionalities.
- The H.248 control interface in-between SGC and MP conforms to the TISPAN Ia specification.

Additional P-CSCF functionality

- P-Charging-Vector
- The P-CSCF allows only one Via header in the messages received from the access network.
- Number portability parameters in Req-URI removed before sending it to core.
- Path headers in REGISTER requests are not allowed.

P-Charging-vector

The P-CSCF will generate a P-Charging-Vector (with icid)

Via headers

Handling of Via headers are changed compared with the SBG in an A-ALG role.

The P-CSCF allows only one Via header in the messages received from the access network.

If more than one Via header is received from the UE, the P-CSCF rejects the request with 403 (Forbidden) final response.

This behavior cannot be configured.

Number portability

Number portability parameters in Req-URI are removed before sending it to core.

Path header

Path headers in REGISTER requests are not allowed. If the path header is received from the UE, the SBG P-CSCF rejects the request with 403 (Forbidden).

The SBG P-CSCF adds itself as an entry in the Path header when sending the REGISTER to the core network.

All Path headers received from the core network side (S-CSCF) in 200 OK are then removed before forwarding the 200 OK to the UE.

P-Associated-Identity header

Authorizes users and includes a P-Associated-Identity header.

Default topology hiding

Default hard coded topology hiding for P-CSCF role.

The topology hiding is always off towards core and always on towards access.

This is not possible to change by configuration.

E-CSCF as outgoing proxy

It is possible to specify an E-CSCF as outgoing proxy for emergency calls using UDP and/or TCP as transport protocol.

Geographical redundancy for E-CSCF

To enhance geographical redundancy for E-CSCFs a dummy-REGISTER message is sent on a regular basis to the E-CSCFs in order to detect E-CSCF availability.

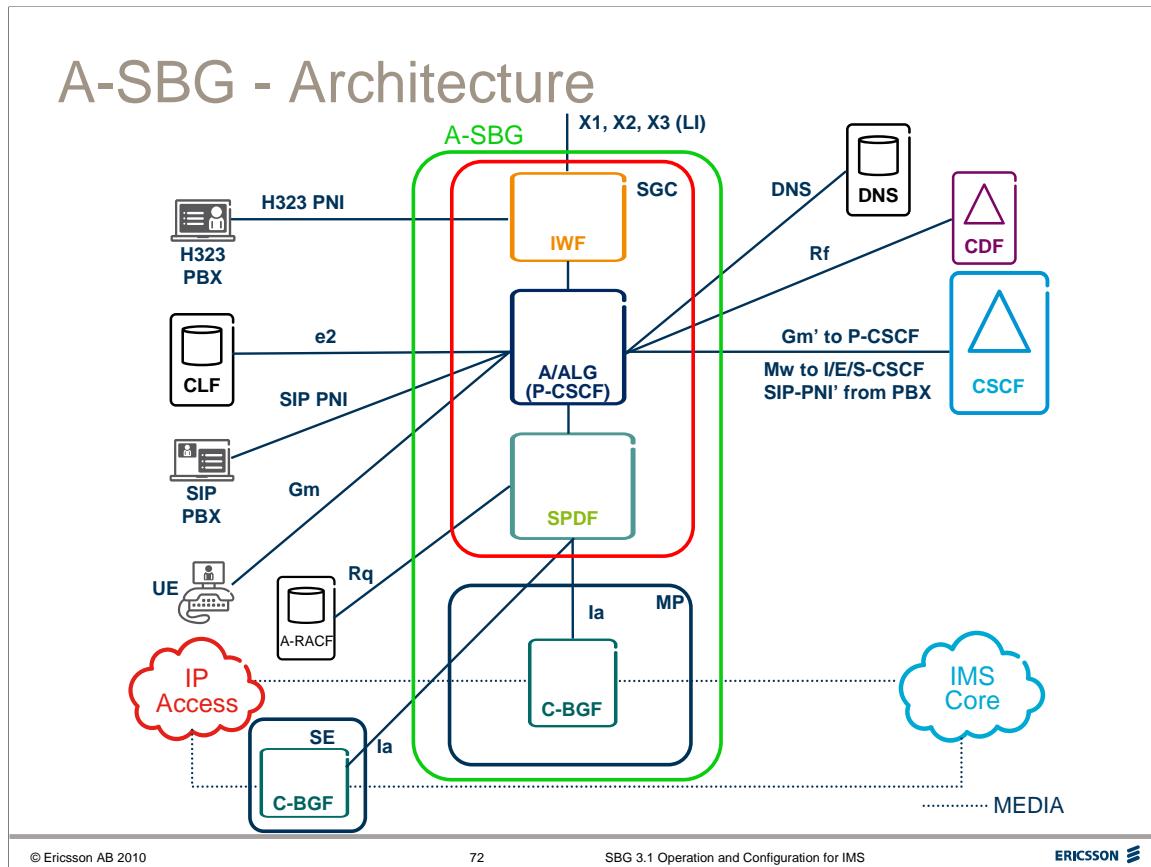
This enhances the probability that emergency INVITEs will be sent to a working E-CSCF.

P-Preferred-Identity assertion for A-ALG

In the SBG 3.1 the received P-Preferred-Identity is checked for all initial requests with the registrar database.

If no match is found, the SBG will add the default IMPU and send it in the INVITE.

If a match of the received P-Preferred-Identity is found, the received P-Preferred-Identity is considered valid and is sent in the INVITE.



The **A-SBG Session Gateway Controller** comprises three main functions:

Access Application Level Gateway (A/ALG)

The A/ALG acts as the B2BUA between the Access Networks and the CSCFs in the IMS core. The A/ALG has SIP Registrar functionality to support registration of users and to support routing of SIP to the Access Networks.

Service-based Policy Decision Function (SPDF)

The SPDF decides which Media streams are allowed to be set-up and the characteristics of the streams. The SPDF requests required resources from BGFs & A-RACF.

Inter-Working Function (IWF)

The IWF is defined by TISPAN as the entity which performs the inter-working in the SBG between H.323 and SIP.

The **Media Proxy (MP)** includes the:

Core Border Gateway Function (C-BGF)

The BGF is a packet-to-packet gateway for media plane traffic.

BGF performs the following functions under SPDF control:

- *Opening/closing pinholes*
- *Packet marking. DSCP*
- *Resource allocation per flow. bandwidth CAC*
- *NAPT*
- *Policing of downlink and uplink traffic & Usage metering; reports to the SGC*
- *Hosted NAT/FW traversal.*

The BGF can be either integrated or distributed on ERICSSON RedBack SmartEdge.

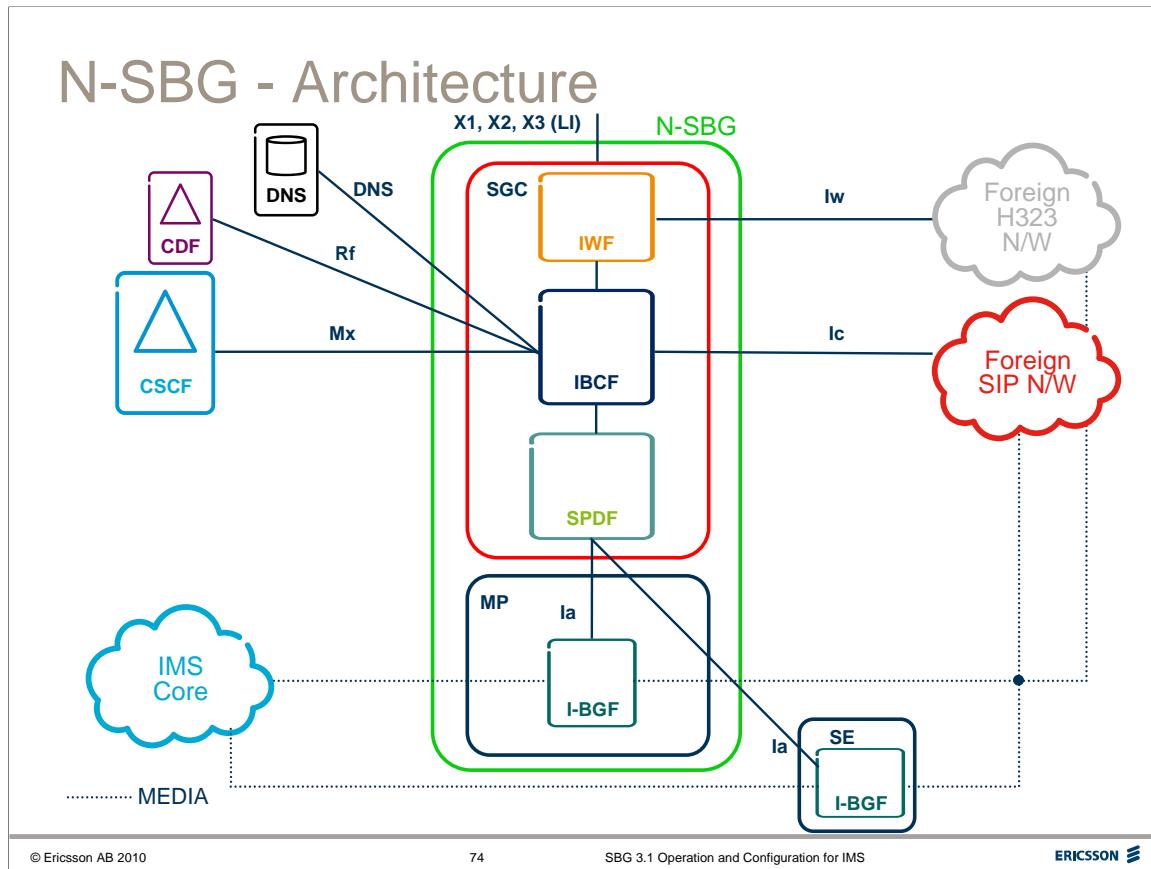
SPDF

- The Service Policy Decision Function (SPDF) is a logical policy decision element for service-based policy control and performs the following functions:
 - Checks if the request information received from the AF is consistent with the policy rules defined in the SPDF
 - Authorizes the requested resources for the AF session
 - Determines the location of the BGF and/or A-RACF in accordance with the transport capabilities required
 - Requests resources of the A-RACF
 - Requests one or more services from the BGF
 - Hides the details of the RACS from the AF
 - Performs resource mediation by mapping requests from an AF towards an appropriate A-RACF and/or BGF

SPDF

The Service Policy Decision Function (SPDF) is a logical policy decision element for service-based policy control and is defined by TISPAN. The SPDF is controlled by the IBCF or A-ALG (Called ‘AF’s in TISPAN). According to TISPAN, an SPDF performs the following functions:

- Checks if the request information received from the AF is consistent with the policy rules defined in the SPDF. The IBCF and A-ALG always request services from SPDF according to SGC internal policies.
- Authorizes the requested resources for the AF session. The SPDF in SGC applies policy rules defined by the network operator (for example, early media, RTCP policy, local media, allowed codecs, allowed bandwidth per codec, and QoS policy per traffic type).
- Determines the location of the BGF and/or A-RACF in accordance with the transport capabilities required.
- Requests resources of the A-RACF.
- Requests one or more services from the BGF. The SPDF in SGC requests services as specified by TISPAN (open/close pinholes, packet marking, resource allocation, NAPT, hosted NAT/FW traversal, policing of down/uplink traffic, usage metering).
- Hides the details of the RACS from the AF. The SPDF hides policies and A-RACF communication from IBCF and A-ALG in SBG.
- Hides the details of the transport layer from the AF. The SPDF hides media plane specifics and BGF communication from IBCF and A-ALG in SBG.
- Performs resource mediation by mapping requests from an AF towards an appropriate A-RACF and/or BGF. The SPDF in SGC translates requests from IBCF and A-ALG into Rq and Ia requests when needed.



The **N-SBG Session Gateway Controller** comprises three main functions:

Interconnection Border Control Function (IBCF)

The IBCF acts as a B2BUA between the IMS core network and ‘foreign’ SIP and H323 networks

Service-based Policy Decision Function (SPDF)

SPDF in the N-SBG performs the same function as described for the A-SBC.

The SPDF decides which Media streams are allowed to be set-up and the characteristics of the streams. The SPDF requests required resources from media plane entities.

Inter-Working Function (IWF)

The IWF in the N-SBG performs the same function as described for the A-SBC, it performs inter-working between H.323 foreign networks and IMS.

The **Media Proxy (MP)** includes the:

Core Border Gateway Function (C-BGF)

The BGF in the N-SBG performs the same function as described for the A-SBC:

- *Opening/closing pinholes.*
- *Packet marking. DSCP*
- *Resource allocation per flow. bandwidthCAC*
- *NAPT.*
- *Policing of downlink and uplink traffic.*
- *Usage metering. gathers statistics and reports to the SGC.*
- *Hosted NAT/FW traversal.*

The BGF can be either integrated or distributed on ERICSSON RedBack SmartEdge

IBCF

- Controlling transport plane functions.
- Topology Hiding
- Blacklist screening of SIP signalling information based on source, destination, and operator policy
- Generation of Charging Data Records (CDRs).
- Selecting the appropriate signalling interconnect

IBCF

The Interconnection Border Control Function (IBCF) controls the border between two operators' domains. The functions of the IBCF include:

- *Controlling transport plane functions.* Each time the IBCF in the SBG receives an SDP request to set up a media stream, the request is given to the SPDF and I-BGF in the SBG. The SPDF and I-BGF decides if the stream is acceptable from policy and QoS perspective and then anchors it in the I-BGF and apply appropriate QoS settings.
- *Topology Hiding*
- The IBCF in the SBG contains a fully configurable SIP header blacklist function.
- Foreign networks can be configured as trusted or untrusted so that the SBG can apply separate procedures. Bodies of SIP messages are also screened for disallowed content.
- *Generation of Charging Data Records (CDRs).*
- *Selecting the appropriate signalling interconnect.* The IBCF selects the foreign network based on the operator configuration and DNS lookup.



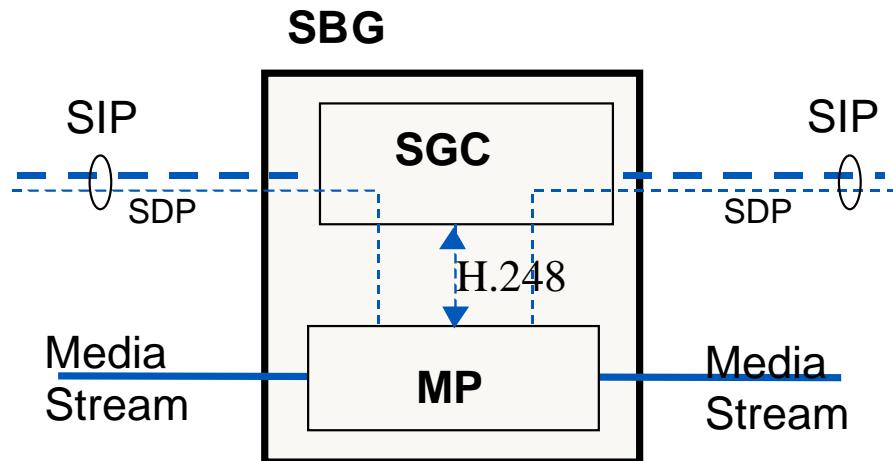
ERICSSON

SBG 3.1 Operation and Configuration for IMS

Hardware & Software Structure

This section describes the hardware and Software structure of the SBG.

SBG Logical Architecture



SBG Logical Architecture

As can be seen from the figure above, the SBG consists of a Session Gateway Controller (SGC) and a Media Proxy (MP).

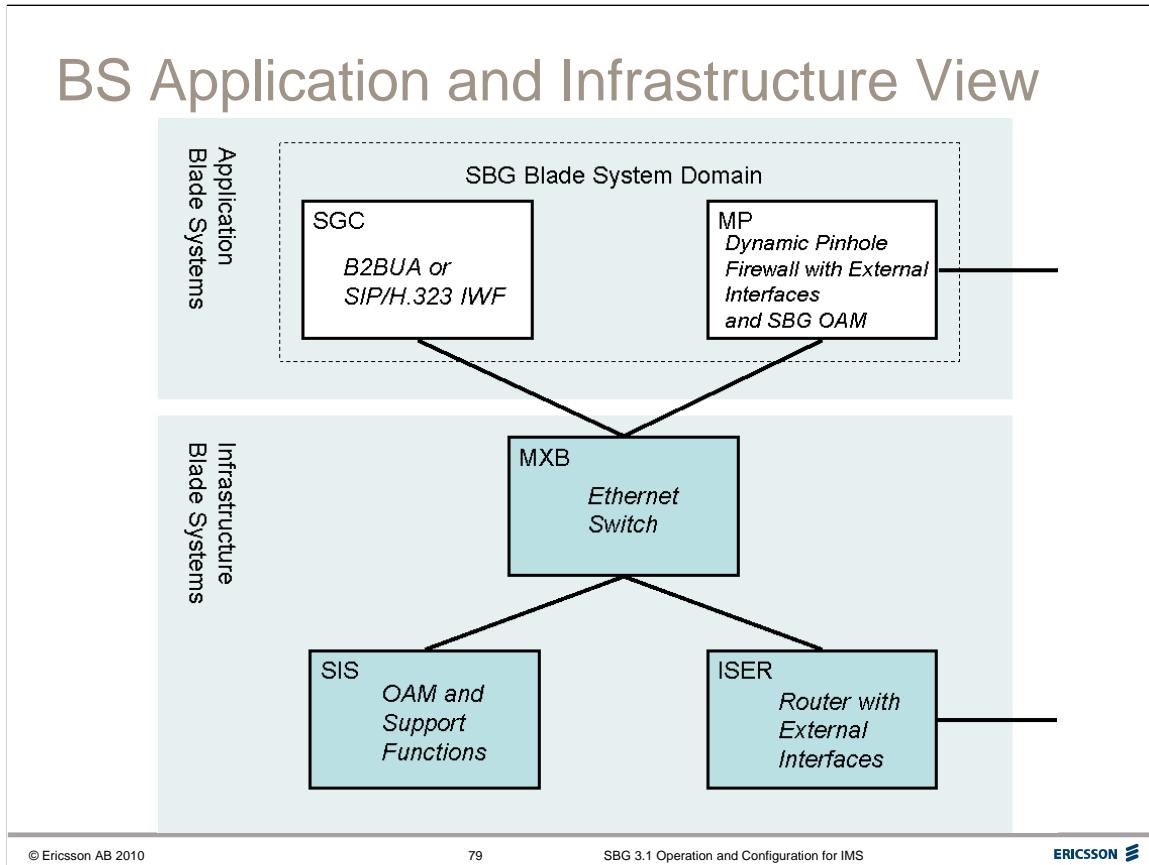
The SBG is based on the Ericsson IS framework and is composed of two types of IS application blade systems, the Session Gateway Controller (SGC) and the Media Proxy (MP), and employs the standard IS infrastructure blade systems. SBG 3.1 is implemented on IS 2.0.

The Integrated Site provides standard O&M tasks such as management, layer 2 and layer 3 transport and resiliency, and perimeter protection. The IS framework is designed so that new software and hardware can be used, as new and more powerful technologies become available. This is true for payload processing as well as control processing.

The availability of open source and open standards, such as:

- Institute of Electrical and Electronics Engineers (IEEE) Ethernet
- Internet Engineering Task Force (IETF)
- Network Processing Forum
- Service Availability Forum
- Advanced Telecommunications Computing Architecture (ATCA)
- Open Source Development Labs (OSDL)

facilitates the use of new technologies and provides multiple open third-party systems for these technologies. The IS takes advantage of the new technologies, and the application blade systems provide the actual node functionalities.



BS Application and Infrastructure View

The SBG utilizes switching, routing, and support functions provided by the IS infrastructure blade systems:

- Main Switch Blade (MXB)
- IS Edge Router (ISER)
- Site Infrastructure Support (SIS):
 - IS common OAM and support functions
 - Graphical User Interface (GUI) support
 - Netconf support
 - Inter-subrack links.

The SGC and MP blade systems contain the main SBG functions for the control plane and the media plane, respectively. The SGC implements the B2BUA function and the SIP-H.323 inter-working function, which control the dynamic pinhole firewall function implemented on the MP. The MP also implements SBG OAM functions and inter-works with the IS common OAM function.

The SBG blade system domain consists of a set of application blades that are grouped into application blade systems:

- two or more SGC blades. The SGC blades are grouped in pairs, where each pair forms an SGC blade system.
- two or more MP blades. The MP blades are grouped in pairs, where one pair forms is defined as the Operation and Maintenance and Media Proxy (OMMP) and all others are MP blade systems.

SBG3.1 Hardware – IS 2.0



ISER – Firewall & Virtual Router, Connection to IP Network.
 MXB – Ethernet Switch (Layer 2 internal switching)
 SIS – O&M, Sub-network Management, Hard Disks.
 EXB – LAN connection for non-IS nodes (not used in IS PSTN GW)

Features:
 Redundant Power
 Redundant O&M bus
 Gigabit Ethernet to all blades

Hardware – IS 2.0

The SBG3.1 is implemented on IS 2.0.

The Infrastructure (IS) Blade Systems provide the common resources for the SBG. These include Blade Systems for site management, network configuration, O&M, hardware and software management, layer 2 switching, shelf management, layer 3 routing, and the connection of externally attached LAN systems. The different Infrastructure Blade Systems are described below.

Site Infrastructure Support (SIS)

The SIS provides many common support functions, called Services, mostly to do with Internal O&M for the other Blade Systems including a Netconf and O&M GUI portal. It also provides functions for LAN fault management, Shelf management, Sub-network management and site security (user administration, authentication and authorization).

Main Switching Blade (MXB)

The MXB provides the IS switching function providing Layer 2 switching to all blades via the backplane connections. Functions include Resilient Ethernet switching and Virtual LAN for traffic separation.

Integrated Site Edge Router (ISER)

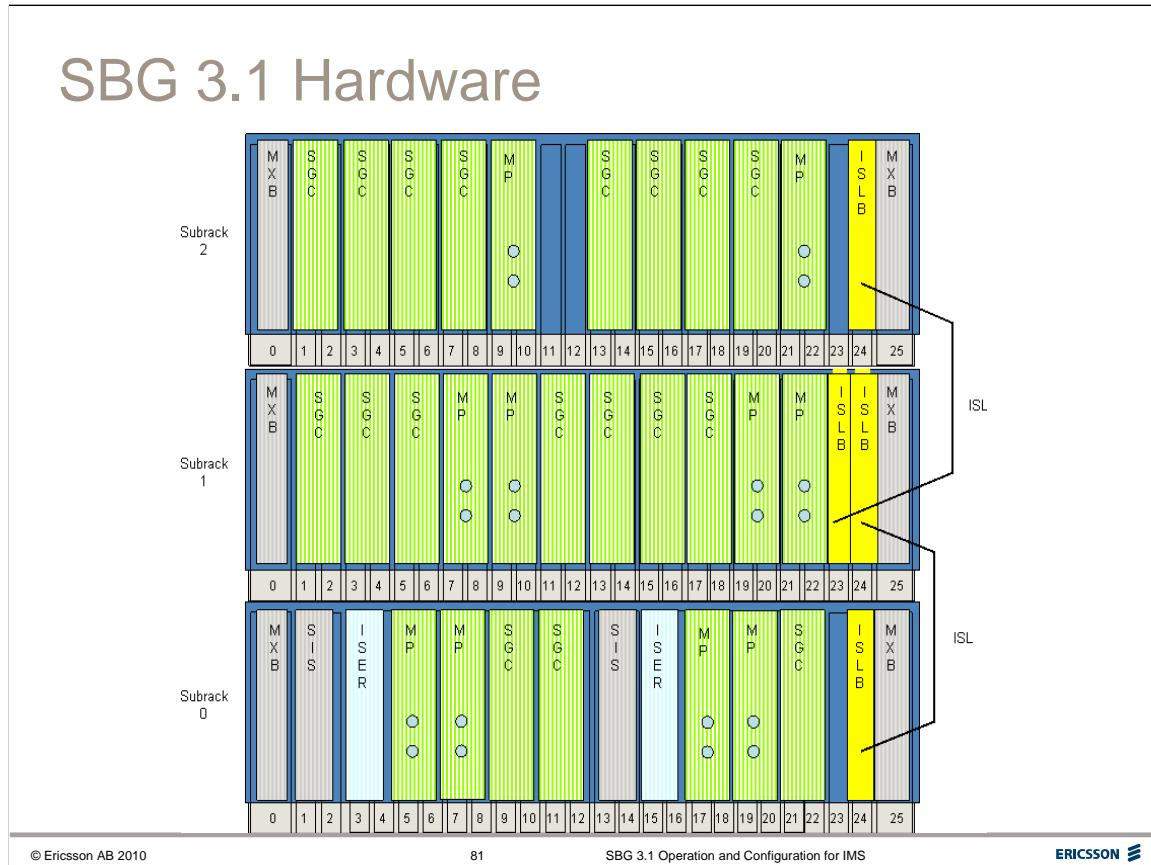
The ISER provides Layer 3 IP connectivity to connect the IS site to the backbone network in a secure manner. The L3 services can also be provided to connect Attached Systems on L3 and protect IS from potential threats on attached devices. ISER also provides Firewall and Virtual Router Instances and supports Virtual Private Networks and QoS based on DiffServ.

Extension Switching Blade (EXB)

This is an optional Blade System not used in SBG.

IS Features:

- Redundant power to all blades
- Redundant O&M maintenance bus to all blades
- Gigabit Ethernet to all blades on backplane



The SBG can be employed in a single-subrack or multisubrack configuration.

The Figure above shows a multisubrack configuration example. In a multisubrack configuration, ISLBs are also needed to cascade the subracks. All blades except ISLB are duplicated to provide redundancy.

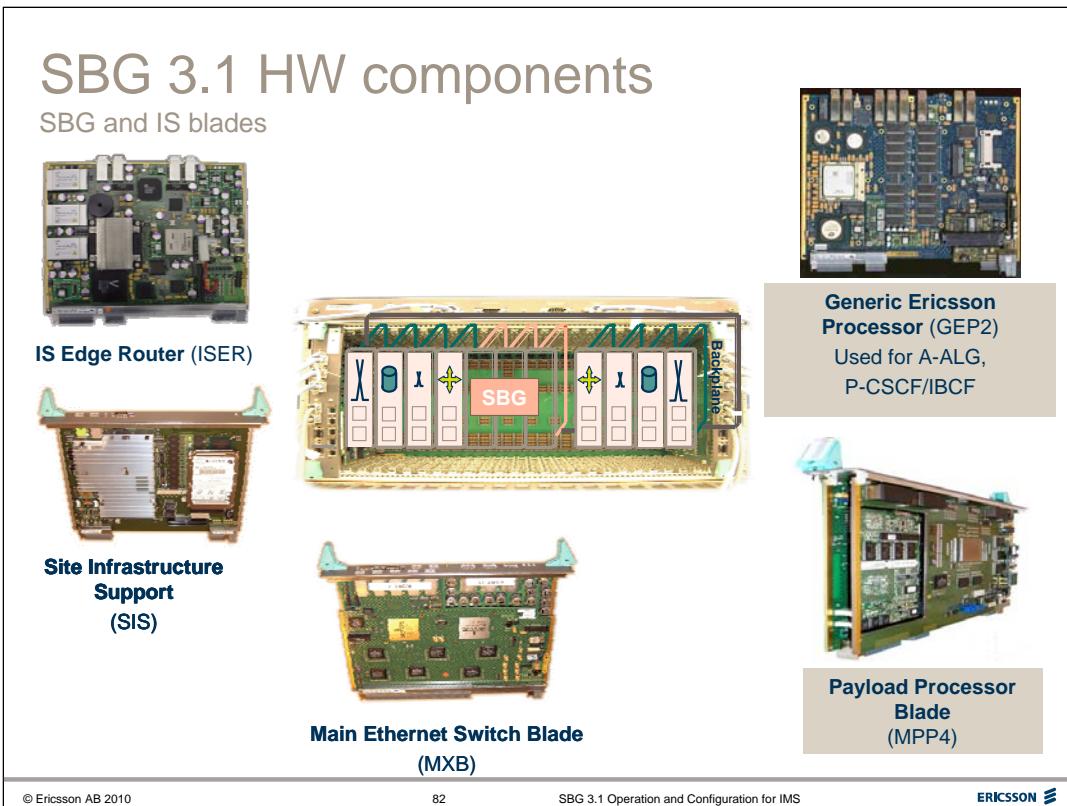
The IS building practice is the Enhanced Generic Ericsson Magazine (EGEM), which provides 26 slots per subrack. Slot 0 and 25 are reserved for the MXBs and are 30 mm wide. Slots 1 to 24 are all 15 mm wide.

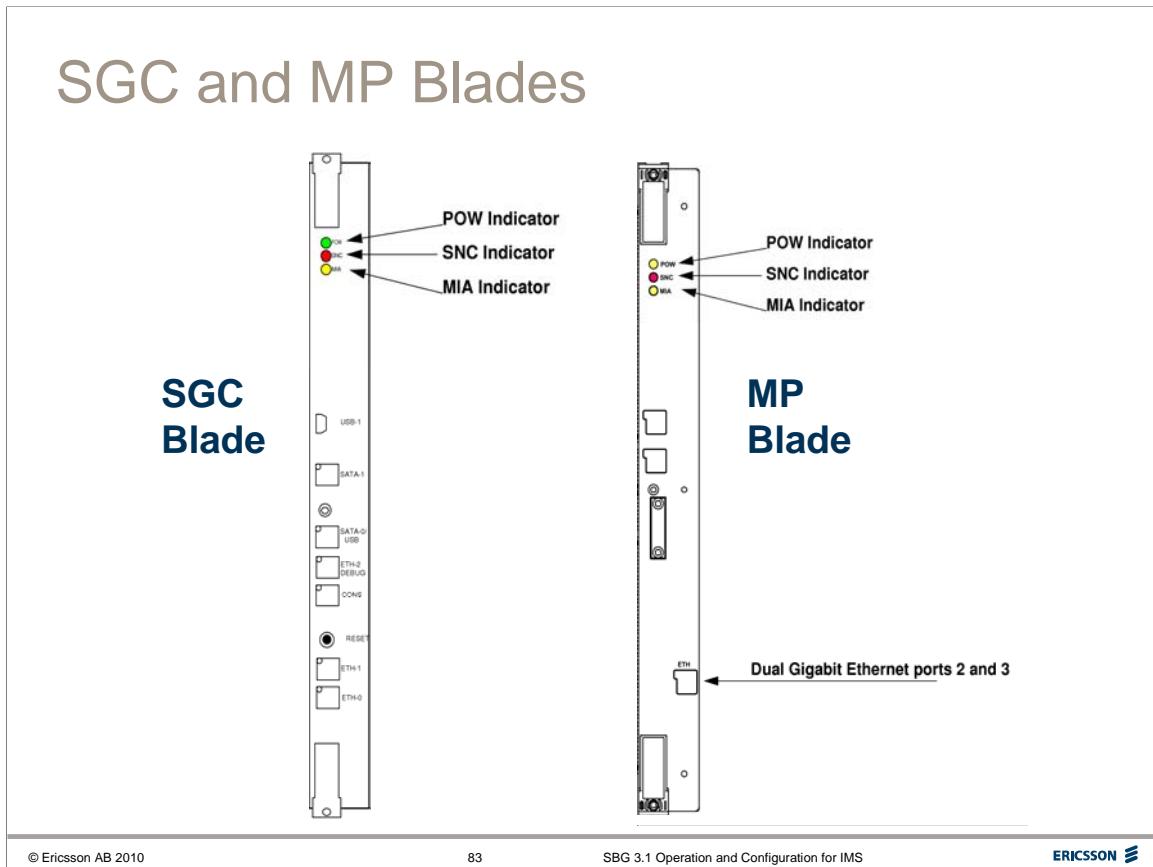
The subrack has a redundant Gigabit Ethernet backplane with a redundant 1 Gbit/s interface per slot, OAM backplane, duplicated power etc.

SBG 3.1 Hardware

The SGC & MP PIUs are each 30 mm wide, so occupy two slots.

At least two SGC and two MP blades are needed, both in a single-subrack and in a multisubrack system. The usage of the remaining slots can be customized for the site's specific requirements for capacity and function.



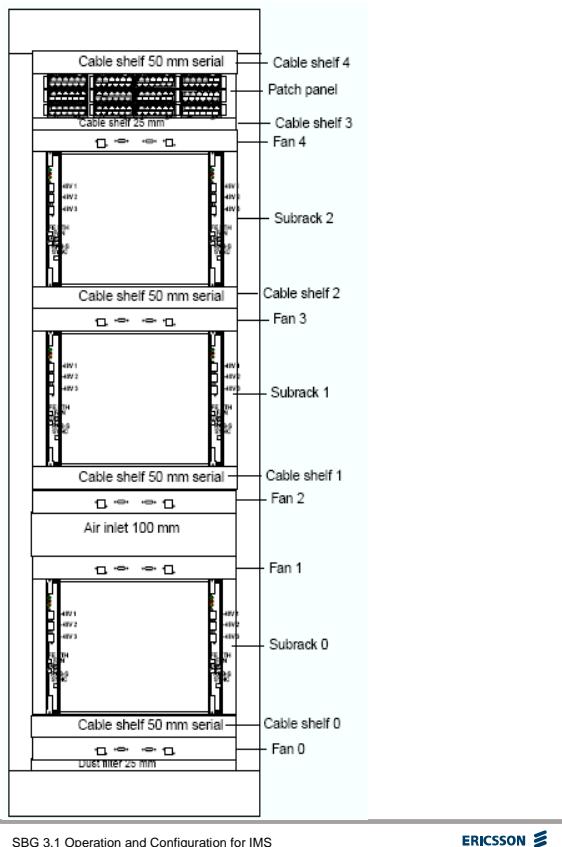


The SGC Blade has a Gigabit Ethernet port on the backplane.

The MP Blade has two Gigabit Ethernet ports on the backplane and two on the front of the board (in a single connector).

BYB 501 180/14

3 IS Subracks with overhead cabling



© Ericsson AB 2010

84

SBG 3.1 Operation and Configuration for IMS

ERICSSON

IS EGEM subracks are shown above.

Multiple subracks can be placed in a single cabinet. For example, in an Ericsson BYB 501 180/14 cabinet there is room for three subracks as shown above.

The BYB 501 180/14 cabinet is used for overhead cabling, whereas the BYB 501 180/13 cabinet is used for underfloor cabling.

HW and SW of SBG

Session Gateway Controller (SGC) Blade System

- The Hardware for SGC BS is the GEP-4GBD Board(s)
- SGC software group: sbg-sgc-swg, CXS101109 Rxxxx

SBG O&M and Media Proxy (OMMP) Blade System

- The Hardware for OMMP BS is the MPP3-GE Board(s)
- OMMP software group: sbg-ommp-swg, CXS10130 Rxxxx

Media Proxy (MP) Blade System

- The Hardware for MP BS is the MPP3-GE Board(s)
- MP software group: sbg-mp-swg, CXS10129 Rxxxx

Note: xxxx = release

Software management of the SBG follows the software management of the IS. That means the software required for SGC BS, OMMP BS and MP BS is identified by software group.

Session Gateway Controller (SGC) Blade System

- The Hardware for SGC BS is the GEP-4GBD Board(s)
- SGC software group: sbg-sgc-swg, CXS101109 Rxxxx

SBG O&M and Media Proxy (OMMP) Blade System

- The Hardware for MP BS is the MPP3-GE Board(s)
- OMMP software group: sbg-ommp-swg, CXS10130 Rxxxx

Media Proxy (MP) Blade System

- The Hardware for MP BS is the MPP3-GE Board(s)
- MP software group: sbg-mp-swg, CXS10129 Rxxxx

The GEP (Generic Ericsson Processor) is from the new GEP family of processors and the MPP3-GE is from Payload Processing Blade family.

All SBG blades are 30mm wide and occupy 2 slots of the EGEM subrack.

Software Groups

Software Groups

Name	Product number	Version	Name	Name	Status	Delete
sbg-mp-swg	CXS 101 29	R11A71	MP	SBG	Complete	<input type="checkbox"/>
sbg-ommp-swg	CXS 101 30	R11A72	MP	SBG	Complete	<input type="checkbox"/>
mp-bl-swg	CXS 101 31	R11A74	MP	SBG	Complete	<input type="checkbox"/>
sis-bl-swg	CXS 101 37	R4L05	SIS	N/A	Complete	<input type="checkbox"/>
sis-bs-swg	CXS 101 38	R4L06	SIS	N/A	Complete	<input type="checkbox"/>
mxb-bs-swg	CXS 101 44	R4A10	MXB	N/A	Complete	<input type="checkbox"/>
iser-bl-swg	CXS 101 63	R4A24	ISER		Complete	<input type="checkbox"/>
iser-bs-swg	CXS 101 64	R4A24	ISER		Complete	<input type="checkbox"/>
mgw-swg	CXS 101 76	R10A08	MGW	N/A	Complete	<input type="checkbox"/>
mgw-bl-swg	CXS 101 059	R10A01	MGW	N/A	Complete	<input type="checkbox"/>
sgc-bl-swg	CXS 101 108	R11A75	SGC	SBG	Complete	<input type="checkbox"/>
sgc-swg	CXS 101 109	R11A75	SGC	SBG	Complete	<input type="checkbox"/>
mxbl-bl-swg	CXS 101 231	R4A89	MXB	N/A	Complete	<input type="checkbox"/>
mgw-c6mb-bl-swg	CXS 101 233	R10A01	MGW	N/A	Complete	<input type="checkbox"/>
mp-c6mb-bl-swg	CXS 101 358	R11A70	MP	SBG	Complete	<input type="checkbox"/>
sgc-gep2-bl-swg	CXS 101 366	R11A75	SGC	SBG	Complete	<input type="checkbox"/>

[Table as text](#) [Next](#)

Software Groups

Application Software is contained in Software Groups. For SBG or MP there is one Software Group for the Blade System and one for the Blades

To view the Software Groups in the system, go to *Integrated Site Services* → *Software* and click the *View Software Groups* link.

A software group is identified by its name, product number and version. These attributes are defined by Ericsson and cannot be changed.

A software group is included in the **Software Group** inventory when a blade or blade system information package has been downloaded, which contains information about software delivery packages included in the software group, and information about which Blade System and, if applicable, which Integrated system it is a part of.

Software Delivery Package Files

Each **Software Group** consists of several **Software Delivery Packages**.

A software group cannot be used until all of its software delivery packages have been downloaded. Until then, the system presents the status of the software group as **Incomplete**.

To view which software delivery package files are available in the Integrated Site. Click the *View Software Files* link in the Software service submenu to view.

A software delivery package is identified by its name, product number and version. These attributes are set by Ericsson and cannot be changed.

SGC Software Delivery Packages

Integrated Site Services Software

Software Overview SGC 1-19-23

Blade Systems

Blade System
▶ SIS
▶ MXB 0-0
▶ MXB 0-25
▶ ISER 0-3
▶ ISER 0-23
▶ MGW 0-5-8
▶ MXB 1-0
▶ MXB 1-25
▶ MGC 0-11-17
▶ OMMP 1-17-21
▶ SGC 1-19-23

Software Delivery Packages in use

Name	Product number	Version	Type
gbs-gep-rootfs	CXP 901 2387	R11A07	Application
gbs-gep-kernel	CXP 901 2388	R11A07	Kernel
sgc-swg-si	CXP 901 2485	R11A64	Blade system information
sgc-bl-swg-si	CXP 901 2486	R11A64	Blade information
gbs-sgc	CXP 901 4753	R11A70	Application
sgc-scp	CXR 101 0438	R11C35	Correction

Software Groups in use

Name	Product number	Version	Name	Name	Status
sgc-bl-swg	CXS 101 108	R11A75	SGC	SBG	Complete
sgc-swg	CXS 101 109	R11A75	SGC	SBG	Complete

SGC Software

To view the Software for a Blade System, go to *Integrated Site Services* → *Software*; select the Blade System from the list on the left and then click *View Software Files*.

The figure above shows the software groups of SGC and its Software Delivery Packages.

A software delivery package can be of six types:

- Application - Contains software and data files common to the entire blade system.
- Kernel - Specific to a certain hardware type.
- Root file system - Specific to a certain hardware type.
- Blade information - Contains information on the software group.
- Blade system information - Contains information on the software group.
- Correction.

Each software group has one information package.

MP Software

The software groups for OMMP/MP are shown in the next page.

OMMP Software

Integrated Site Services Software

Software Overview OMMP 1-17-21

Blade Systems

Blade System
▶ SIS
▶ MXB 0-0
▶ MXB 0-25
▶ ISER 0-3
▶ ISER 0-23
▶ MGW 0-5-8
▶ MXB 1-0
▶ MXB 1-25
▶ MGC 0-11-17
▶ OMMP 1-17-21
▶ SGC 1-19-23

Software Delivery Packages in use

Name	Product number	Version	Type
gbs-syf-rootfs	CXP 901 1071	R11A12	Root file system
gbs-syf-kernel	CXP 901 1072	R11A12	Kernel
mp-bl-swg-si	CXP 901 1075	R11A63	Blade information
sbg-ommp-swg-si	CXP 901 1117	R11A63	Blade system information
gbs-ommp	CXP 901 4749	R11A70	Application
gw-scp	CXR 101 0132	R11B14	Correction

Software Groups in use

Name	Product number	Version	Name	Name	Status
▶ sbg-ommp-swg	CXS 101 30	R11A72	MP	SBG	Complete
▶ mp-bl-swg	CXS 101 31	R11A74	MP	SBG	Complete

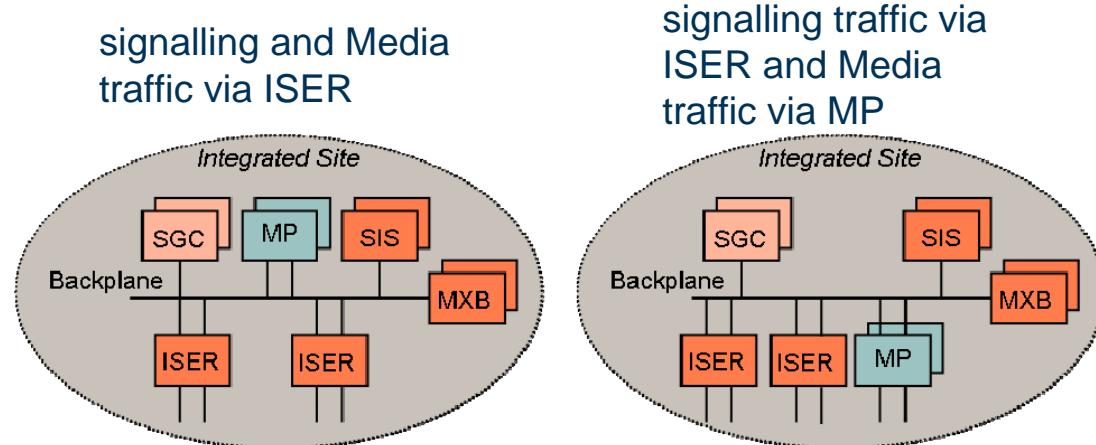
OMMP Software

The first MP blade system also performs OAM functions, so the Blade System software group here is the OMMP software.

The Blade Software is for all MP types.

Software Management is covered in more detail in a later section of the book.

SBG External Connectivity



SBG 3.1 External Connectivity

Signalling and Media traffic via ISER

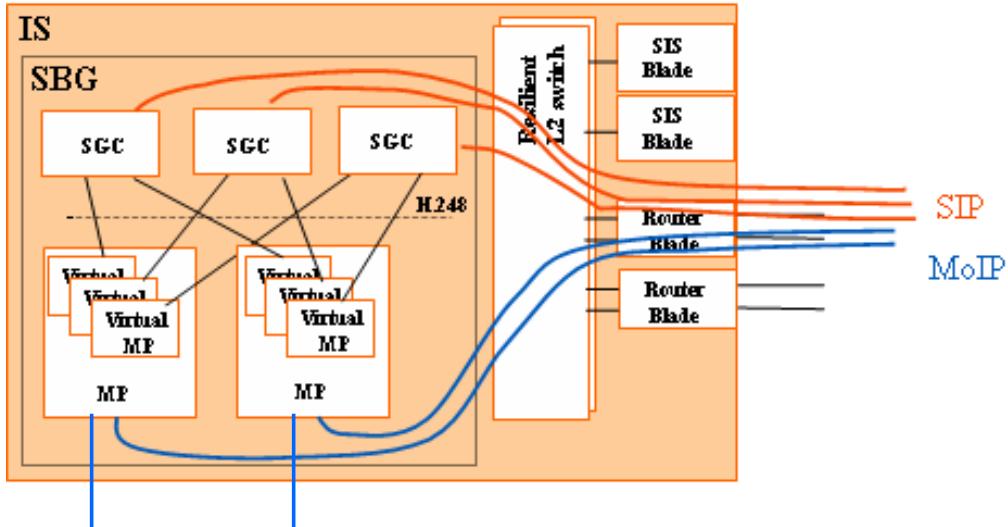
The figure on the left shows the physical connectivity view of the SBG, showing how the boards that make up the SBG (MP and SCG) are connected to the IS. The boards are all connected via the backplane of the E-GEM. The SIS, MXB, ISER are common IS functions. Each line connecting the blades to the backplane also indicates 1 Gbit/s Ethernet connection. 1 MP blade system has 2 Gbit/s Ethernet towards backplane and SGC blade system has 1 Gbit/s Ethernet towards backplane. ISER is also having 2 Gbit/s Ethernet connection towards backplane. In this configuration, both signalling and media traffic will be configured via ISER, which means that the SBG external interface is via ISER only.

Signalling Traffic via ISER and Media Traffic via MP

The figure on the right shows another possibility of connecting the SBG to an external network. In this configuration, only signalling traffic will be configured via ISER. As for the media traffic, the external Gigabit Ethernet interface available from the MP hardware front port is used for the media external connectivity.

There are 2 Gigabit Ethernet interface available at the front side of the MP hardware. This is preferred configuration especially if configuring the SBG with more than 1 MP blade system.

Virtual MP concept



Virtual MP Concept

One SGC and one MP require one H.248 connection. In this case, the SGC communicates directly with the MP.

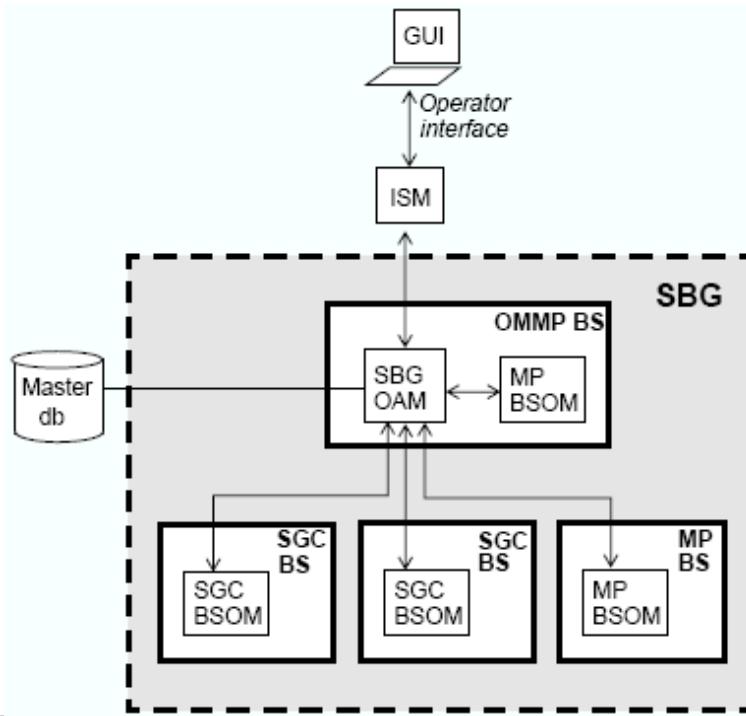
Some configurations may have more than one MP or more than one SGC. In the figure above, there are three SGCs and two MPs. In this configuration, to enable the SGCs to control all MPs, the H.248 control connection is not directed towards the MP itself. The connection is made towards a logical entity within the physical MP called a Virtual MP.

To enable each SGC to be connected to all MPs, virtual MPs are created within each MP. So, the SGC is actually connected to the virtual MP. Each virtual MP will have one H.248 connection towards SGC.

SBG 3.1 Operation and Configuration for IMS

User interface

SBG User Interface



SBG User Interface

The operator interface for the management of the SBG functions and the IS common services is provided through the IS Management system (ISM) which has a graphical user interface accessible from a web browser on a locally or remotely connected terminal.

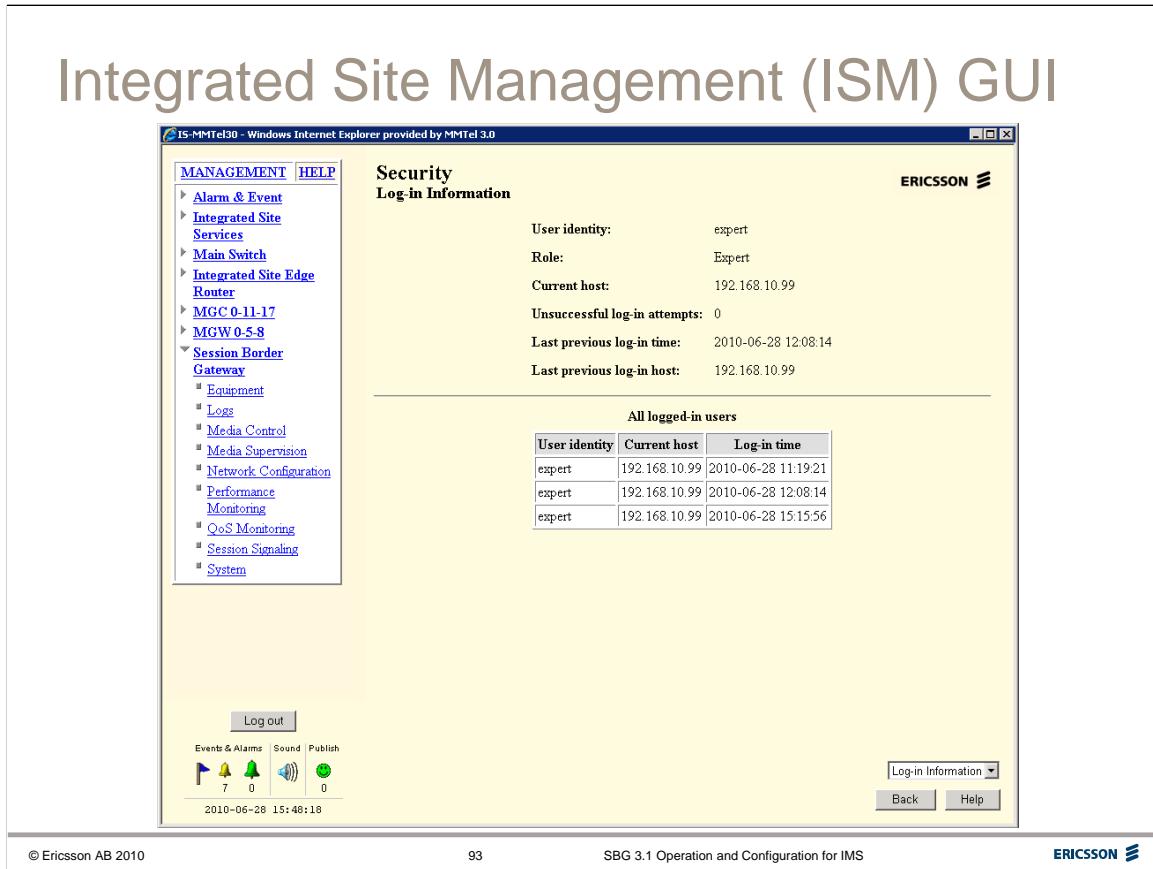
When performing management operations in the GUI, the ISM forwards the operations to the OMMP blade system (i.e. the MP blade pair defined for O&M). The OMMP will coordinate the management operations for the SBG and other MPs, and forward the management operations to all Blade Systems affected by the particular operations.

All SBG configuration data specified through the ISM is stored in the master configuration database of the OMMP blade system as well as in the local database of the associated MP or SGC blades.

Certain management operations affect a single blade system, others affect all blade systems of a particular type, for example, all SGC blade systems.

The operator interface for IS common services includes:

- Hardware management
- Software management
- Fault management
- IS common network configuration, remote management for IP address and SNMP configuration, and central user management with LDAP
- Administration of In Service Performance
- Logs
- Performance Measurement



Accessing the Integrated Site Management (ISM) GUI

To access the ISM GUI:

1. Enter the Uniform Resource Locator (URL) of the Integrated Site in a web browser Location field. The ISM introduction page is displayed.
2. Click the *Log in* link. A pop-up window appears, requesting the user name and password (default: expert/expert).
3. The ISM main window is displayed, as shown above. The ISM main window displays the Security Management – Login Information data in the Operation frame.
4. The user now has access to the ISM GUI.

The ISM GUI functionality is fully described in the IS O&C Course and will not be described in detail here.

SBG Management Function Area

At startup, the blade systems are automatically integrated into one functional unit, SBG, with its management interface to the ISM located on the OMMP blade system, and internal interfaces between OMMP and the other MP and SGC blade systems. The necessary internal IP addresses are obtained from the IS DHCP server.

Each ISM GUI action towards the SBG results in requests from the ISM to the SBG OAM function on the OMMP, where it is processed and depending on the managed object, forwarded to the SGC or MP Blade System OAM interface (BSOM).

SBG Management Function Area

IS-MMTel30 - Windows Internet Explorer provided by MMTel 3.0

MANAGEMENT **HELP**

- Alarm & Event
- Integrated Site Services
- Main Switch
- Integrated Site Edge Router
- MGC 0-11-17
- MW 0-5-8
- Session Border Gateway**
- Equipment
- Logs
- Media Control
- Media Supervision
- Network Configuration
- Performance Monitoring
- QoS Monitoring
- Session Signaling
- System

Security
Log-in Information

User identity: expert
Role: Expert
Current host: 192.168.10.99
Unsuccessful log-in attempts: 0
Last previous log-in time: 2010-06-28 12:08:14
Last previous log-in host: 192.168.10.99

All logged-in users

User identity	Current host	Log-in time
expert	192.168.10.99	2010-06-28 11:19:21
expert	192.168.10.99	2010-06-28 12:08:14
expert	192.168.10.99	2010-06-28 15:15:56

Log out

Events & Alarms Sound Publish

2010-06-28 15:48:18

Log-in Information Back Help

The addition, restart, or removal of individual blade systems in SBG is automatically handled by the SBG OAM:

- A new blade system is added to the SBG master database when it registers to SBG OAM at startup, and it is configured with the master database configuration.
- A restarted blade system is synchronized with the master database and any new SBG configuration will be downloaded to the local database.
- A removed blade system is deleted from the master database.

The configuration data in the SBG master database is persistently stored on the SIS disk.

The SBG MFA (Management Function Area) Menu provides information and instructions about how to handle the services within the SBG in the IS.

The services provided within the SBG MFA are:

- **Equipment**
- **Logs**
- **Media Control**
- **Media Supervision**
- **Network Configuration**
- **Performance Monitoring**
- **Quality of Service Monitoring**
- **Session signalling**
- **System**

SBG MFA - Equipment

Session Border Gateway Equipment

Open

[Ethernet interfaces](#)

[Admission control](#)

Equipment service

The **Equipment** service provides the following management functions:

- *Ethernet interfaces*
- *Admission Control*.

Ethernet Interfaces

The MP only has one type of interface, Gigabit Ethernet. The four interface ports are located on the back of the blade and connect to the dual Gigabit Ethernet connections on the IS backplane

Two interfaces connect the blade system to an outside network (external interface), and the remaining two connect to the Main Switch Board (MXB) blade systems via the IS backplane (internal interface).

The four Interfaces are created automatically at the creation of a blade, numbered 0 – 3.

Interfaces 0 and 1 are the internal interfaces and 2 and 3 are the external interfaces.

IP traffic through the Ethernet interfaces can be monitored from the Ethernet interface statistics page.

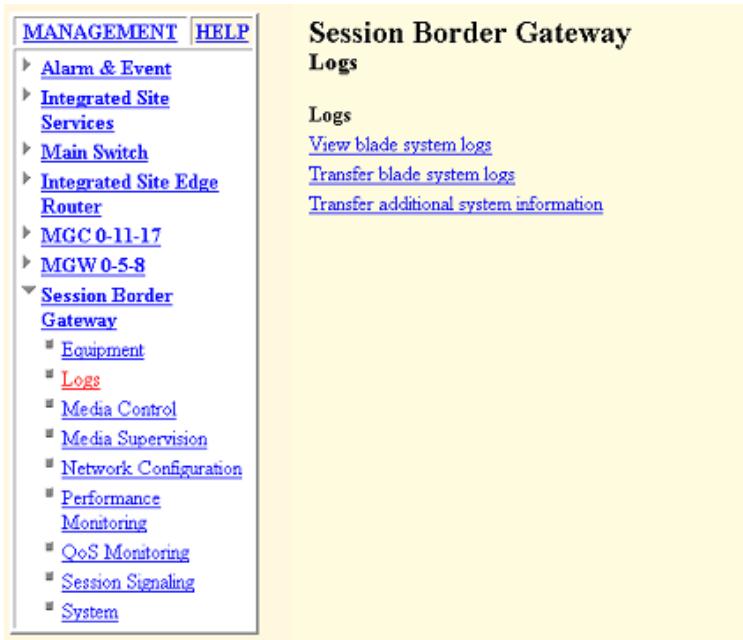
Admission Control

The allowed media bandwidth per Ethernet interface, and the emergency bandwidth margin as a percentage of the available bandwidth, can be set in the Admission Control page. This page also displays the current bandwidth utilization.

The type of traffic and the network configuration affect the maximum throughput, and can be configured to maximize the throughput without sacrificing quality.

For further information, see the *Equipment Service Guide*.

SBG MFA - Logs



Session Border Gateway Logs

Logs

[View blade system logs](#)
[Transfer blade system logs](#)
[Transfer additional system information](#)

Logs Service

The Logs service in the SBG MFA enables the operator to view the SBG-specific logs, by selecting the ***View blade system logs*** link.

The SBG logs are:

- Excessive traffic log
- H.248 error log
- Malicious MSRP log
- Malicious Traffic log
- Hanging Resources log
- Network QoS log
- signalling log
- User QoS log
- Performance file transfer failures.

In addition to viewing the SBG blade system logs, the logs can also be transferred by ftp using ***Transfer blade system log*** option.

The link ***Transfer additional system information*** is used to send logs and system information to Ericsson when raising a CSR.

More information can be found in *Logs Service Guide*.

SBG MFA – Media Control

Media Control service

The Media Control service provides the following functions:

- **Media type definitions**
- **Payload type definitions**, including bandwidth specification
- **Local media domain** configuration
- **MP control links**
- **IMS Communication Service Identifiers (IP-TV)**

To define up to five identifiers (ICSI) used as trigger points for IPTV-specific behavior.

If an initial INVITE has a feature tag *g.3gpp.app_ref* or *g.3gpp.icsi_ref* in the Accept-Contact header, the feature tag value is compared to the ICSI identifier string and if the tag matches, the session is considered as an IPTV session.

- **External BGF control interfaces**

The external BGF control interface is used for H.248 communication toward external BGFs. One external BGF control interface is supported per SGC. For network specific configurations for external BGFs, see the service guide Network Configuration: signalling network connection configuration

- **Codec policy profiles** (This is a Trial-only feature and is not described further).

- **Transcoding resource definitions** (This is a Trial-only feature and is not described further).

For further information, see the *Media Control Service Guide*.

SBG MFA – Media Supervision

MANAGEMENT HELP

- ▶ [Alarm & Event](#)
- ▶ [Integrated Site Services](#)
- ▶ [Main Switch](#)
- ▶ [Integrated Site Edge Router](#)
- ▶ [MGC 0-11-17](#)
- ▶ [MGW 0-5-8](#)
- ▶ **Session Border Gateway**
 - [Equipment](#)
 - [Logs](#)
 - [Media Control](#)
 - [Media Supervision](#)
 - [Network Configuration](#)
 - [Performance Monitoring](#)
 - [QoS Monitoring](#)
 - [Session Signaling](#)
 - [System](#)

Session Border Gateway Media Supervision

[Open](#)
[Supervision](#)
[Network statistics](#)
[Stream statistics](#)
[MSRP statistics](#)
[ARP monitoring](#)

Media Supervision service

The purpose of the Media Supervision service is to only permit traffic that has been set up via signalling. Incoming packets are compared with what the SGC has requested the MP to forward. Source and Destination addresses and Ports are checked. Packets are discarded if the requested bandwidth is exceeded.

Supervision

The operator can view and set parameters for threshold; hysteresis; and the logging of malicious and excessive traffic; and can turn on or off malicious Message Session Relay Protocol (MSRP) logging.

Network statistics

On the Network statistics page the network counters are displayed.

Stream statistics

On the Stream statistics page the media stream counters are displayed .

MSRP Statistics

On the MSRP Statistics page the MSRP data message counters are displayed

ARP monitoring

On the ARP monitoring page the operator can inspect and set Address Resolution Protocol (ARP) parameters for detecting network problems such as IP address collision and failures contacting a next hop address.

More information can be found in *Media Supervision Service Guide*.

SBG MFA - Network Configuration

Network Configuration service

The Network Configuration service provides the following functions:

- **Networks** Includes IP interface configuration for media, route and next hop configuration for media, and configuration of signalling Network connections (SIP/H.323).
- **Domains** The operator can configure the domains to which the SBG is connected. The use of domains is optional and it is not necessary to configure a complete view of the network, it is sufficient to configure only the part of the network that is of interest. There is a many to many relationship between networks and domains. A network can contain many domains and a domain can contain many networks.
- **Next hop groups** optimizing the ARP monitoring
- **Faulty next hops** Contains a list of the next hops used for media that have been found to be faulty by the next hop supervision.
- **Address-to-network mapping** that is, signalling routing for Interconnection Border Control Function (IBCF).
- **DSCP to P-bit mapping** for external interfaces on MP

For further information, see the *Network Configuration Service Guide*.

SBG MFA – Performance Monitoring

Job Id	MO Class	Measurement family	Administrative state	Job status	Delete
1	EthernetInterface	Ethernet_interface_statistics	On	Active	<input type="checkbox"/>
2	EthernetInterface	Bandwidth_statistics	On	Active	<input type="checkbox"/>

Performance Monitoring service

To view a list of configured performance measurement jobs select *Performance Measurement Jobs* in the Performance Monitoring service of the SBG.

The list shows:

Job ID – the job identity, which was assigned to the job by the system when the job was created

MO class – the managed object class chosen by the operator when the job was created

Measurement family – the measurement family chosen by the operator when the job was created

Administrative state – the job administrative state, which is an operator-assigned value

Job status – the job status, either of Idle, Suspended, Active, Scheduled.

Each job is selectable, taking the operator to a detailed job information page. On this page the operator can reassign the FTP destination used for transmitting performance job data files.

Note:

If a measurement job is removed, pending performance data transfers will be aborted. If the operator wants to allow the system to finish transmitting data, suspend a job for some time before deleting it.

SBG MFA - QoS Monitoring

MANAGEMENT [HELP](#)

- ▶ [Alarm & Event](#)
- ▶ [Integrated Site Services](#)
- ▶ [Main Switch](#)
- ▶ [Integrated Site Edge Router](#)
- ▶ [MGC 0-11-17](#)
- ▶ [MGW 0-5-8](#)
- ▼ [Session Border Gateway](#)
 - [Equipment](#)
 - [Logs](#)
 - [Media Control](#)
 - [Media Supervision](#)
 - [Network Configuration](#)
 - [Performance Monitoring](#)
 - [QoS Monitoring](#)
 - [Session Signaling](#)
 - [System](#)

Session Border Gateway QoS Monitoring

User QoS Monitoring

[Configure user QoS monitoring](#)
[Open monitored users](#)

Network QoS Monitoring

[Configure network QoS monitoring](#)
[Open network QoS statistics](#)

QoS Monitoring service

From this service the operator can configure and control the gathering of quality of service (QoS) statistics data from the media flowing through the SBG.

The Quality of Service Monitoring service provides the following functions:

- ***User QoS monitoring***

A User's SIP URI or telephone URL can be added for QoS monitoring.

- ***Network QoS monitoring***.

In this service, the Exponential Weighted Moving Average (EWMA) % is set and what proportion of sessions are monitored (by specifying every Nth session to be monitored).

Network QoS statistics can also be viewed.

QoS Monitoring will be further described in the *Performance Management* section of this book.

SBG MFA - Session Signalling

Session Border Gateway

Session Signaling

Session Border Gateway

Session Signaling

Create

[SIP network connection](#)
[H.323 network connection](#)
[Trunk context](#)
[IP-PBX](#)
[Emergency number](#)
[Blacklist profile](#)
[Blacklist header](#)
[SMM filters](#)

Open

[SIP network connections](#)
[H.323 network connections](#)
[SIP registrars](#)
[Registrar contact bindings](#)
[SIP throttling definitions](#)
[Trunk contexts](#)
[IP-PBXs](#)
[Emergency numbers](#)
[Emergency settings and counters](#)
[Signaling parameters](#)
[Resource statistics](#)
[DNS configuration](#)
[Blacklist profiles](#)
[Blacklist headers](#)
[User agent whitelists](#)
[SMM rule sets](#)
[SMM filters](#)

Logout

© Ericsson AB 2010 102 SBG 3.1 Operation and Configuration for IMS ERICSSON

Session Signalling service

The user interface of the Session signalling service consists of configuration sections for protocol-specific connections, signalling routes, SIP registrars, IP-PBXs, and DNS configuration.

In addition protocol-specific statistics are available for viewing.

SBG MFA - System

System

The System service provides the following functions:

Blade system administration - the installed and configured blade systems can be seen. Call handling state of a blade system can be changed. Critical resources are also available, showing processor load and memory usage.

This is further described in the node management section.

Distinguished names are used to identify instances of managed object classes in performance measurement data files.

Diameter realms - Charging (Rf); Geographical location (e2) and Admission control (Rq) realms can be viewed/defined.

MP Control links – the status and statistics of the control links can be viewed. **Transfer/Load configuration file** The function can be used to transfer the configuration data file from the SBG to an external server and to load from an external server.

Import TLS certificate In order to use TLS in SIP network connections for signalling in an access network a TLS certificate must be imported. This certificate is used for all SIP network connections defined with TLS. The certificate file must be a combined server certificate and private key file.

Import/Export SIP rule sets

SIP Message Manipulation rule sets can be created using SMMSL. See *Session signalling: SIP Message Manipulation*

Exercise 1

SBG 3.1 Operation and Configuration for IMS

Node Management

This section describes Node Management tasks:

How to check and monitor: System Status; Blade Systems Status; Blade Status; Critical Resources.

How to perform Backups and how to restore Backups.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Status Checks

This section describes Node Management tasks:

How to check and monitor: System Status; Blade Systems Status; Blade Status; Critical Resources.

SBG System Status – Blade Systems

Blade system	BSOM IP address	Call handling state	Management availability
OMMP 1-17-21	169.254.64.11	unlocked	available

Blade system	BSOM IP address	Call handling state	Operational state	Management availability
SGC 1-19-23	169.254.64.12	unlocked	enabled	available

SBG System Status

The status of the SBG can be viewed at **SBG → System → Blade System Administration**

There will be at least two blade systems displayed on the page:

- Media Proxy Blade System
- Session Gateway Controller Blade System

The SBG is in correct working condition when:

- The OMMP blade system *Call Handling State* is “*unlocked*” and the *Management availability* is “*available*”.
- The SGC blade system *Call Handling State* is “*unlocked*”; the *Operational state* is “*enabled*” and the *Management availability* is “*available*”.

If additional SGC blade systems and Media Proxy (MP) blade systems are installed, they can be seen on this page. Their statuses should be the same as those described for the SGC blade system and OMMP blade system.

Click on the red triangle by Media Proxy Blade Systems for more details about the Blade System, as shown on the following page.

Media Proxy Blade System Page

The screenshot shows the 'Media Proxy Blade System Page' from the SBG 3.1 interface. The page title is 'SBG - System Media Proxy Blade System'. The left sidebar contains a navigation menu with items like 'Management', 'Help', 'Alarm & Event', 'Integrated Site Services', 'Main Switch', 'Integrated Site Edge Router', 'MGCC 0-11-17', 'MGW 0-5-8', 'Session Border Gateway', 'Equipment', 'Logs', 'Media Control', 'Media Supervision', 'Network Configuration', 'Performance Monitoring', 'QoS Monitoring', 'Session Signaling', and 'System'. The main content area displays system status information and a table of blade details.

System Status:

- Blade system: OMMP 1-17-21
- Blade system ID: bt_SBG_35
- Blade A: 1-17
- Blade B: 1-21
- BSOM IP address: 169.254.64.11
- BSOM port: 161
- Last change: 2010-03-19 14:25:09
- Management availability: available
- Active blade: 1-21
- Call handling state: unlocked

Blade System Details Table:

Blade position	Blade system	Blade processor load (%)	Blade processor memory (Mbytes)	Used blade processor memory (Mbytes)	Used blade processor memory (%)
1-17	OMMP 1-17-21	0	1011	393	38
1-21	OMMP 1-17-21	1	1011	368	36

Buttons and Links:

- Table as text
- Lock gracefully
- Lock forcefully
- Open hardware management for this blade system
- Open hardware management for blade A
- Open hardware management for blade B

Log out

Events & Alarms: 6 Events, 0 Alarms

Statistics: 0 Events, 0 Alarms

2010-06-29 13:03:22

Media Proxy Blade System

Delete Reload Back Help

Media Proxy Blade System Status

This screen displays more details of the Media Proxy Blade System, including:

- **Blade system name** – the name configured by the operator.
- Blade system ID – unique ID used by the IS to identify the MP blade system.
- Active blade – which MP blade is primary and communicating with SGC.
- **Management availability** - is the blade system available for OAM operations
- **Call handling status** – should be unlocked for normal call handling

Locking the Blade System

The MP blade system can be locked/unlocked from this page:

- **Lock gracefully** – No new calls will be processed. Existing calls will not be terminated immediately. Once all calls are cleared, the blade system will be locked.
- **Lock forcefully** – All existing calls will be dropped and the blade system will be locked.

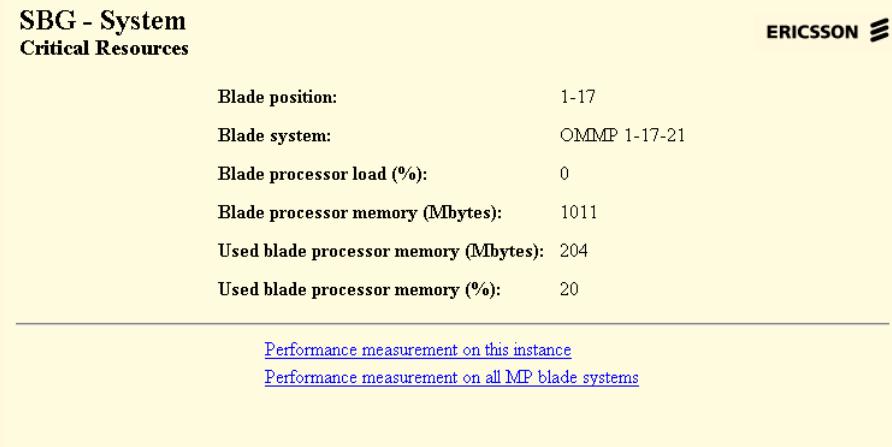
Statistics

The table displays important statistical information of the Media Proxy blades.

Hardware Management

There are also links to open hardware management for the blade system and the individual blades (to lock/unlock, check details, start performance measurements etc).

MP Blade System Critical Resources



SBG – System – Media Proxy Blade System Critical Resources

The statistics gauges in the previous figure show instantaneous current values.

These gauges can also be included in an SBG Performance Measurement job where they are written periodically to file.

To do this, click on the red triangle next to the required blade and the screen above opens.

It shows the ‘critical resources’ for the blade. Then click on one of the *Performance measurement* links to start periodic Performance Measurements on the blade or blade system.

Performance Measurements are described in more detail in a later section of this book.

Media Proxy Blade System Status

Hardware Configuration

Open blade system

ERICSSON

BS identifier: bs_SBG_18
User-defined name: OMMP 1-17-21
Blade system alias: OMMP 1-17-21
Administrative state: Unlocked
Operational state: Enabled
Availability status: Available
Open Blades: [Open Blades](#)
Blade system domain name:

[Shut down](#) [Lock](#)

[View blade system logs](#)
[Transfer blade system logs](#)
[Transfer additional system information](#)

MP Blade System Status

The Hardware status of the Media Proxy Blade System and Blades can be viewed by selecting the link on the *SBG → System → MP Blade System* page, or from *Integrated Site Services → Hardware*.

The OMMP Blade System can also be Locked and Shut down from this page.

Note: Locking and unlocking from this page is not the same as the blade system administration page of the SBG MFA. If the OMMP BS is locked from this page, all SBG traffic handling and O&M functionality is lost.

MP Blade Status

The status of the individual Blades can be seen by clicking the “Open Blades” link on the screen above. The screen shown on the next page is displayed.

Media Proxy Blade Status

Hardware Configuration

Open Blade

Subrack:	1
Slot:	17
Slot label:	X56
Blade type name:	MPP
Blade type number:	CNA12801
BS identifier:	bs_SBG_18
User-defined name:	<input type="text"/>
Administrative state:	Unlocked
Operational state:	Enabled
Availability status:	Available
BS OAM candidate:	True
Manual product data:	False
Product number:	ROJ 208 371/3
Product name:	MPP3-GE
Product revision state:	R4B
Serial number:	A063467045
Vendor:	Ericsson AB
Manufacturing date:	20070123
MAC address (Aggregate):	00:01:EC:B4:39:00
MAC address (Left):	00:00:00:00:00:00
MAC address (Right):	00:00:00:00:00:00
Change date:	2010-08-24 09:55:10 UTC
Redundancy Group:	
Knockout preference:	Normal

Actions:

© Ericsson AB 2010 112 SBG 3.1 Operation and Configuration for IMS ERICSSON

Media Proxy Blades Status

On this page, the status of the selected individual Media Proxy Blade is displayed.

The blade type is indicated as MPP.

The Administrative status and Operational state are shown.

The product name and other details of the blade are displayed.

Knockout Preference: Determines whether the blade is protected from isolation in the event of a link failure:

Protected: If a switch-to-link failure occurs, one of the MXB blades will be isolated.

Normal: If a switch-to-link failure occurs, the blade will be isolated.

Shutting down or locking operations performed from this page will only lock the individual blade not the complete blade system.

Session Gateway Controller Blade System Page

Blade system: SGC 1-19-23
 Blade system ID: bt_SGC_36
 Blade A: 1-19
 Blade B: 1-23
 BSOM IP address: 169.254.64.12
 BSOM port: 161
 Last change: 2010-06-29 12:35:37
 Management availability: available
 Active blade: 1-19
 Call handling state: unlocked
 Operational state: enabled

Blade position	Blade system	Blade processor load (%)	Blade processor memory (Mbytes)	Used blade processor memory (Mbytes)	Used blade processor memory (%)
1-19	SGC 1-19-23	0	3 292	226	6
1-23	SGC 1-19-23	0	3 292	230	6

[Table as text](#)

[Lock gracefully](#) [Lock forcefully](#)

[Open hardware management for this blade system](#)
[Open hardware management for blade A](#)
[Open hardware management for blade B](#)

[Log out](#)

Events & Alarms: 6 | Sound: 0 | Publish: 0

2010-06-29 13:15:36

Session Gateway Controller Blade System

© Ericsson AB 2010

113

SBG 3.1 Operation and Configuration for IMS

ERICSSON

Session Gateway Controller Blade System

On the *SBG → System → Blade System Administration* screen click the red triangle by the SGC to display more details of the status of the Session Gateway Controller.

Other important information that can be seen on this page:

- Blade system name – the configured name of the blade system
- Blade system ID – the ID used by the IS to identify the SGC blade system
- Blade A and Blade B – The position (subrack-slot no) of the blade
- BSOM IP address – IP address for O&M connection with SIS
- The Active Blade – indicates which blade communicates with the Media Proxy and handles signalling.

The SGC blade system can be locked from this page:

- *Lock gracefully* – No new calls will be processed. Existing calls will not be terminated immediately. Once all calls are cleared, the SGC blade system will be locked.
- *Lock forcefully* – All existing calls will be dropped and the SGC blade system will be locked.

SGC Blade Status

The status of the individual Blades can be seen by clicking the “Open Blades” link on the screen shown on the next page is displayed.

SGC Critical Resources

SBG - System Critical Resources

ERICSSON 

Blade position:	1-19
Blade system:	SGC 1-19-23
Blade processor load (%):	0
Blade processor memory (Mbytes):	3292
Used blade processor memory (Mbytes):	226
Used blade processor memory (%):	6

[Performance measurement on this instance](#)[Performance measurement on all SGC blade systems](#)

SGC Critical Resources

The statistics gauges in the previous figure show instantaneous current values.

These gauges can also be included in an SBG Performance Measurement job where they are written periodically to file.

To do this, click on the red triangle next to the required blade and the screen shown above opens. It shows the ‘critical resources’ for the blade. Then click on one of the *Performance measurement* links to start periodic Performance Measurements on the blade or blade system.

Performance Measurements are described in more detail in a later section of this book.

SGC Blade System Status

Hardware Configuration

Open blade system

BS identifier:	bs_SGC_19
User-defined name:	SGC 1-19-23
Blade system alias:	<input type="text" value="SGC 1-19-23"/>
Administrative state:	Unlocked
Operational state:	Enabled
Availability status:	Available
Open Blades:	Open Blades
Blade system domain name:	<input type="text"/>

[Shut down](#)

[Lock](#)

[View blade system logs](#)

[Transfer blade system logs](#)

[Transfer additional system information](#)

SGC Blade System Status

The Hardware status of the SGC Blade System and Blades can be viewed from *Integrated Site Services* → *Hardware*. This page can also be reached by clicking an “Open Hardware Management for this Blade System” link on the SGC Blade System page.

The SGC Blade System can also be Locked and Shut down from this page.

Note: Locking and unlocking from this page is not the same as the blade system administration page of the SBG MFA. If the SGC BS is locked from this page, all SBG traffic handling and O&M functionality is lost.

SGC Blade Status

The status of the individual Blades can be seen by clicking the “Open Blades” link on the screen above; from the *Integrated Site Services* → *Hardware* page; or from the SGC Blade System page.

SGC Blade Status

Hardware Configuration		ERICSSON
Open Blade		ERICSSON
Subrack:	1	
Slot:	19	
Slot label:	X62	
Blade type name:	SGC	
Blade type number:	CNA12821	
BS identifier:	bs SGC_19	
User-defined name:	<input type="text"/>	
Administrative state:	Unlocked	
Operational state:	Enabled	
Availability status:	Available	
BS OAM candidate:	True	
Manual product data:	False	
Product number:	ROJ 208 811/1	
Product name:	GEP-4GBD	
Product revision state:	RSA	
Serial number:	A063682071	
Vendor:	Ericsson AB	
Manufacturing date:	20080527	
MAC address (Aggregate):	00:13:5E:A2:73:C0	
MAC address (Left):	00:13:5E:A2:73:C1	
MAC address (Right):	00:13:5E:A2:73:C2	
Change date:	2010-08-24 09:55:10 UTC	
Redundancy Group:		
Knockout preference:	Normal	

© Ericsson AB 2010
116
SBG 3.1 Operation and Configuration for IMS
ERICSSON

SGC Blades Status

The status of the individual Blades can be seen by clicking the “Open Blades” link on the screen shown on the next page is displayed.

On this page, the status of the selected individual SGC Blade is displayed.

The blade type is indicated as SGC.

The product name of the hardware is indicated as GEP-4GBD. GEP (Generic Ericsson Processor). 4GBD is indicates the amount of memory on the board. This is a variant of the Generic Ericsson Processor family.

Additional information about the blade hardware is displayed.

Knockout Preference: Determines whether the blade is protected from isolation in the event of a link failure:

Protected: If a switch-to-link failure occurs, one of the MXB blades will be isolated.

Normal: If a switch-to-link failure occurs, the blade will be isolated.

Shutting down or locking operations performed from this page will only lock the individual blade not the complete blade system.

Exercise 3

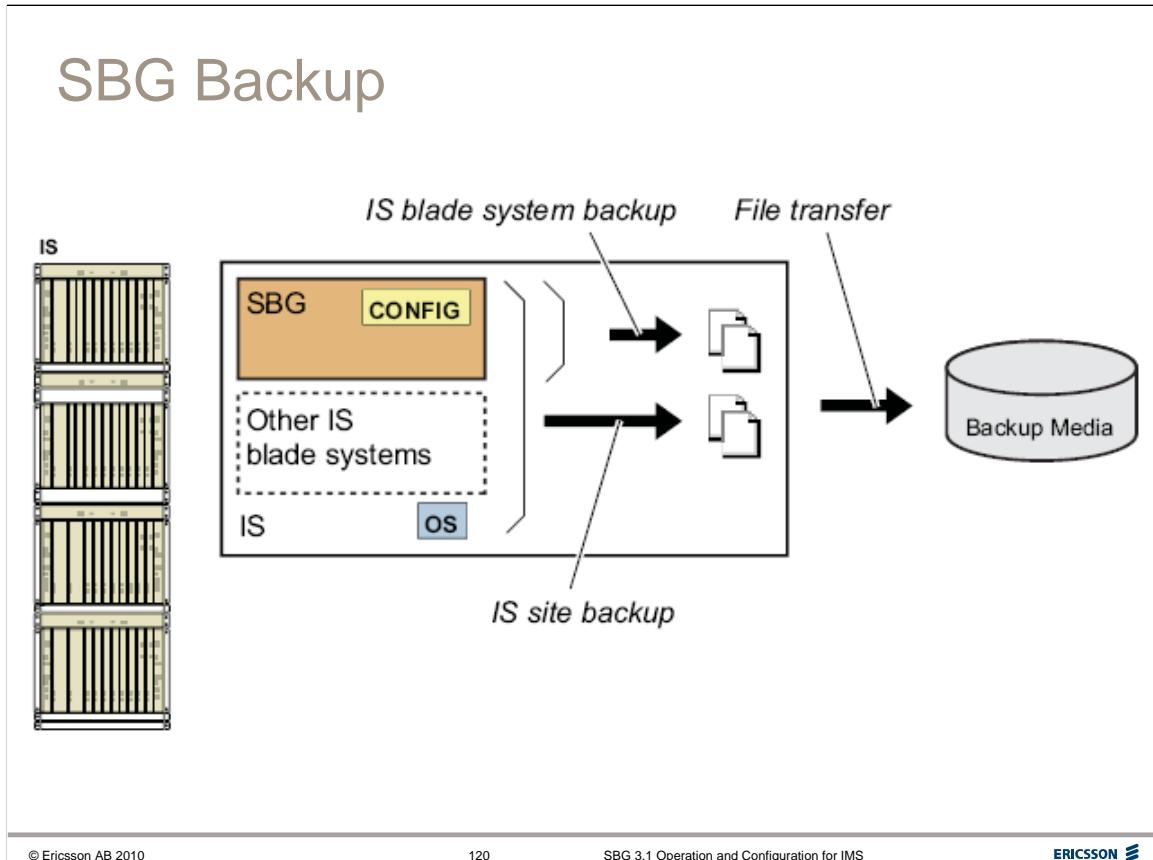


ERICSSON

SBG 3.1 Operation and Configuration for IMS

Backups

This section how to perform Backups and how to restore Backups.



SBG Backup

The SBG uses the Integrated Site *Software* function for backup.

There are two types of backup:

- blade system backup
- site (SIS) backup.

A **blade system backup** backs up all the configuration data stored in a specific blade system. This backup can be used to restore errors in configuration, or to revert software upgrades on a blade system.

A **site backup** backs up all configuration data from all the blade systems, including the Site Infrastructure Support (SIS) blade system. This backup can be used to restore an Integrated Site from a catastrophic failure. It is also used to revert software upgrades on the site infrastructure blade system.

Restoring a backup will cause a service interruption.

Since the SBG has two blade systems (OMMP and SGC), backups must be made for each individually (or perform a site backup).

Creating a Backup 1

Integrated Site Services Software

Software Overview SIS

Blade Systems

Blade System	Name	Product number	Version	Type
► SIS	sis-olp	CXP 901 0874	R4H01	Application
► MDC 0-0	sis-app	CXP 901 0875	R4L04	Application
► MDC 0-25	sis-kernel	CXP 901 0876	R4L05	Kernel
► ISER 0-3	sis-os	CXP 901 0877	R4L05	Root file system
► ISER 0-23	sis-bl-ni	CXP 901 1057	R4L05	Blade information
► MGW 0-5-8	sis-bs-ni	CXP 901 1058	R4L06	Blade system information
► MDC 1-0	sis-ds	CXP 901 1059	R4L02	Application
► MDC 1-25	mb-base	CXP 901 1089	R4A38	Application
► MGIC 0-11-17	sis-ipmi	CXP 901 3851	R4G01	IPMI firmware
► OMMP 1-17-21	sis-scp	CXR 101 0168	R4AB04	Correction
► SOC 1-19-23				

Software Delivery Packages in use

Name	Product number	Version	Name	Name	Status
► sis-bl-rwg	CXK 101 37	R4L05	SIS	N/A	Complete
► sis-bs-rwg	CXK 101 38	R4L06	SIS	N/A	Complete

Software Groups in use

Name	Product number	Version	Name	Name	Status
► sis-bl-rwg	CXK 101 37	R4L05	SIS	N/A	Complete
► sis-bs-rwg	CXK 101 38	R4L06	SIS	N/A	Complete

Software Operations

Inventories	Actions	Jobs
View software files	Download software files	View file jobs
View software groups	Change software for SIS	View upgrade jobs
View backups	Create Site Backup	View backup jobs
Software alarms	Remove Site Backup	Export backup for SIS
		Import backup

Log out

Events & Alarms Sound Publish

2010-06-28 16:11:37

Software Reload Back Help

© Ericsson AB 2010

121

SBG 3.1 Operation and Configuration for IMS

ERICSSON

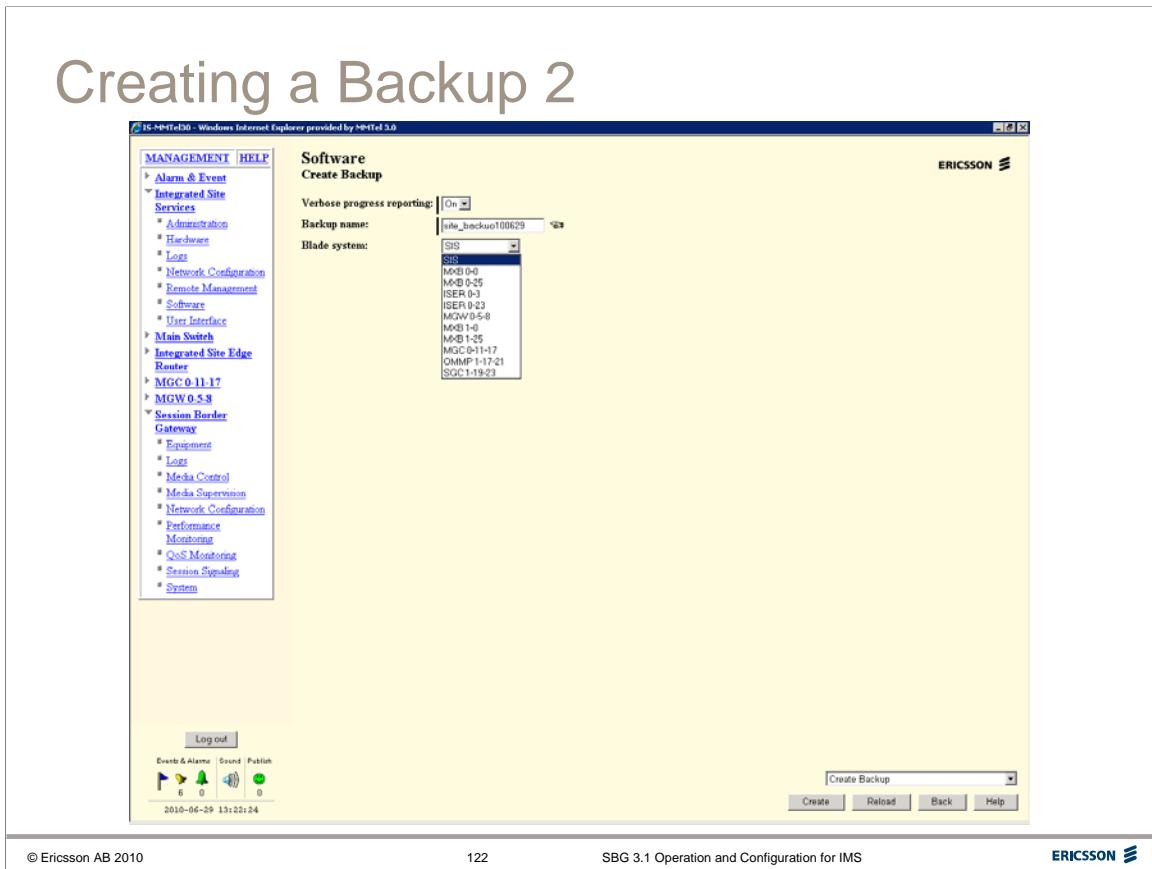
Creating a Backup

Backups are performed from the **Integrated Site Services → Software** link, shown above.

Select the Blade System to backup from the Blade Systems table.

This will display the Software Overview of the selected Blade System. (Select SIS to perform a site backup)

Under **Software Options** select **Create backup for ..** to backup the Blade System, or **Create Site Backup** if SIS is selected.



Specify a **Name** for the backup.

If Verbose progress reporting is On, the system will report its progress in four separate steps.

- Preparing – The Site Infrastructure blade system prepares for receiving a backup from the blade system.
 - Waiting for blade system – The chosen blade system is preparing a backup.
 - Packing backup – The Site Infrastructure blade system is storing the data received from the blade system.
 - Backup complete – The job is finished.

Select the Blade System to backup.

Click ‘Create’ button to start the backup job.

When the Backup is complete, an Event will appear.

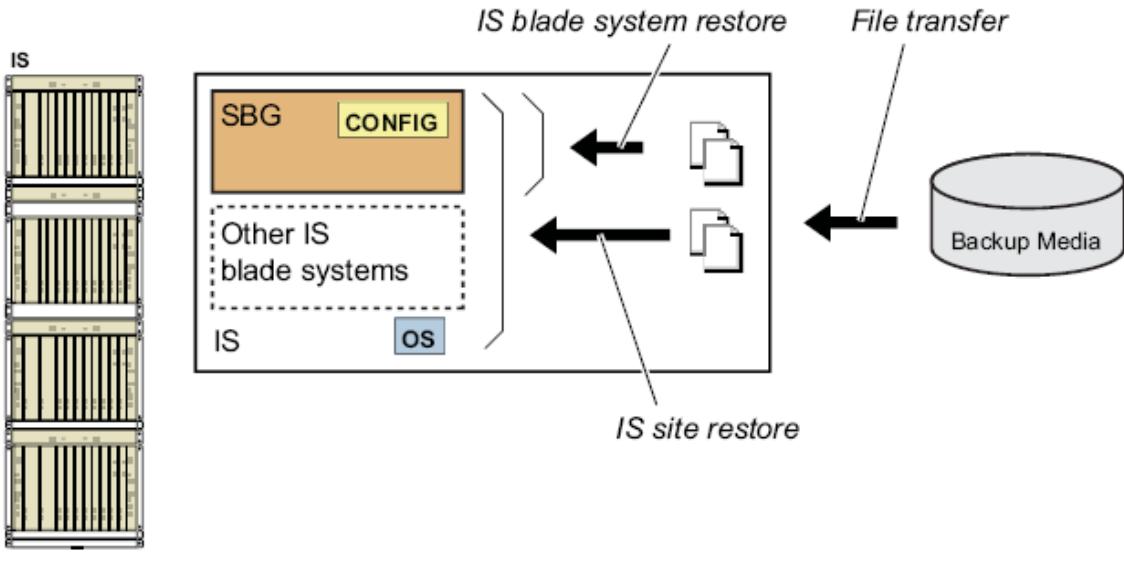
Select SIS to perform a Site backup. A site backup includes an individual backup of each blade system, and a complete site backup (SIS blade system). This will result in a larger backup file.

Transferring a Backup

The screenshot shows the 'Software Overview SIS' page. The left sidebar has a tree view with nodes like 'MANAGEMENT', 'HELP', 'Alarm & Event', 'Integrated Site Services', 'Administration', 'Hardware', 'Logs', 'Network Configuration', 'Remote Management', 'Software', 'User Interface', 'Main Switch', 'Integrated Site Edge Router', 'MGW 0.11.17', 'MGW 0.5.8', 'Session Border Gateway', 'Equipment', 'Logs', 'Media Control', 'Media Supervision', 'Network Configuration', 'Performance Monitoring', 'QoS Monitoring', 'Session Signaling', and 'System'. The main area has three tables: 'Blade Systems', 'Software Delivery Packages in use', and 'Software Groups in use'. The 'Software Operations' section at the bottom has links for 'View software files', 'Download software files', 'View software groups', 'Change software for SIS', 'View upgrade jobs', 'View backups', 'Create new backup', 'Software alert', 'Restore Site Backup', 'Export backup for SIS', and 'Import backup'. The 'Import backup' link is circled in red.

To transfer (FTP/SFTP) a backup between the Integrated Site and an external file server, click the **Export backup** or **Import backup** link in the Software service menu.

Restoring a Backup



© Ericsson AB 2010

124

SBG 3.1 Operation and Configuration for IMS

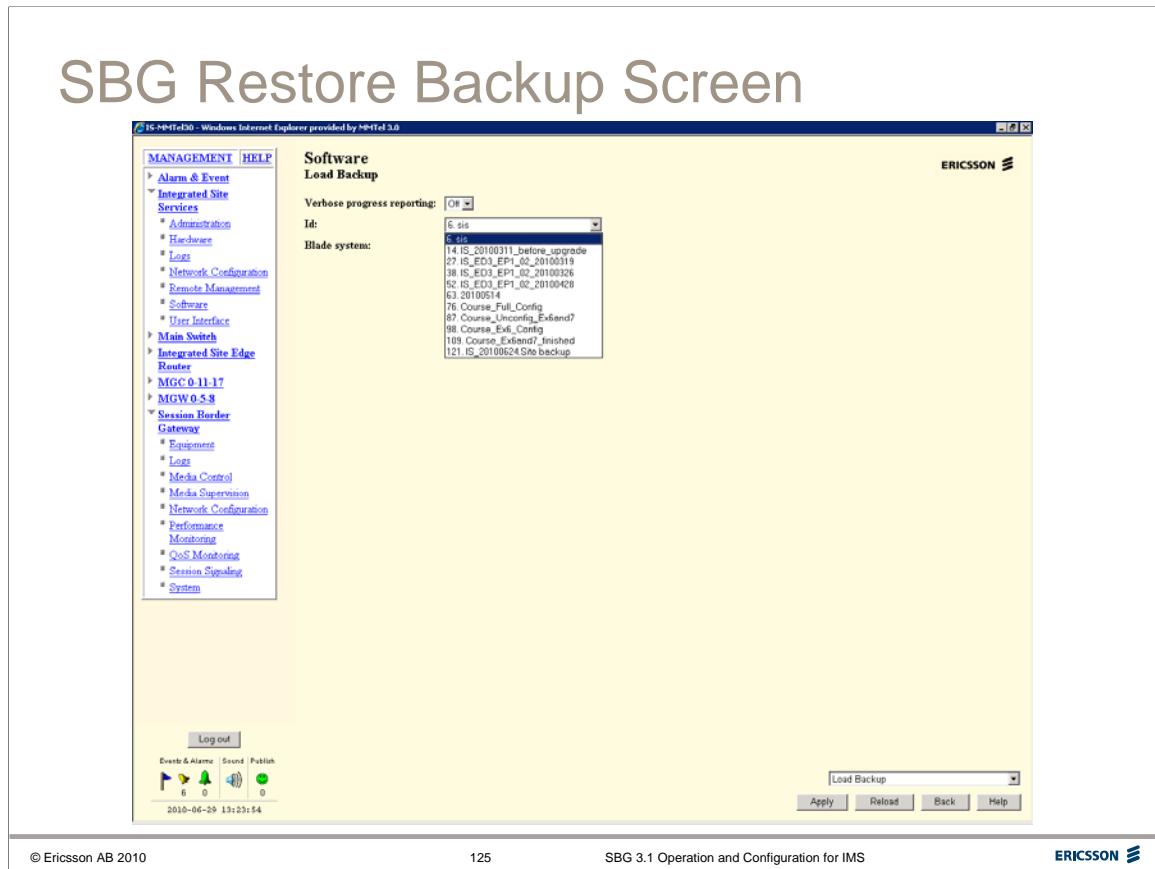
ERICSSON

SBG Restore

To restore a blade system from a backup, go to the Software service submenu and click the *Restore Backup* link.

Select the Blade System to backup from the Blade Systems table. This will display the Software Overview of the selected Blade System. (Select SIS to perform a site backup)

Under ‘Software Options’ select “Create backup for ..” to backup the Blade System, or “Create Site Backup” if SIS is selected.



SBG Restore Backup

Backups are restored from the **Integrated Site Services** → **Software** → **Restore Backup** link, the Load Backup page is shown above.

First select the blade system (SIS will perform a complete site restore)

Only the backups for the blade system chosen will be available in the pull down list.

If Verbose progress reporting is set to On, the system will report its progress in four steps:

- Unpacking –the Site Infrastructure blade system is unpacking the backup data
- Shutting down blade system –the blade system for which the backup is intended is shutting down.
- Restoring blade system –the chosen blade system is starting up with restored data.
- Restore complete –the job is finished.

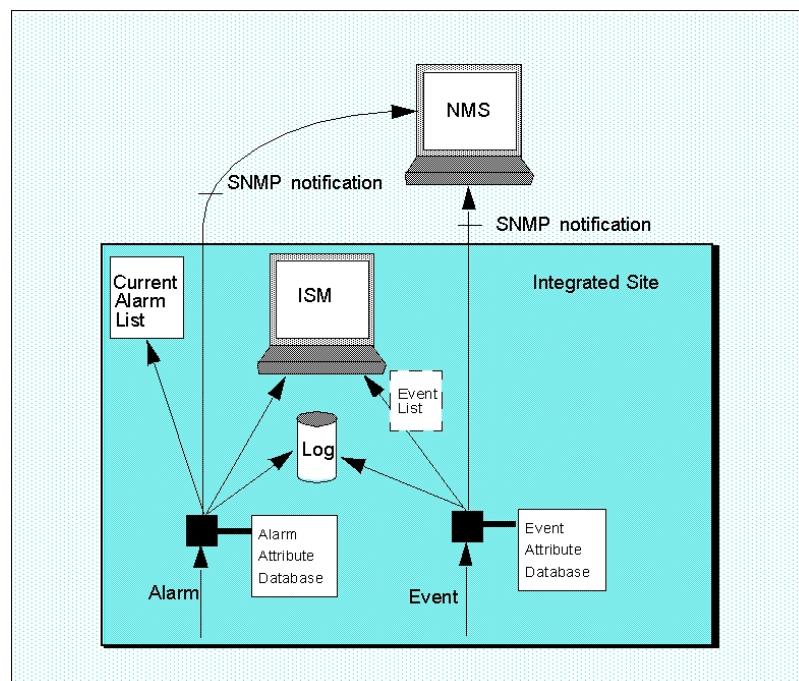
Click Apply to start the restoration.

Exercise 4

SBG 3.1 Operation and Configuration for IMS

SBG Alarms and Events

Alarm and event propagation in IS



Fault Management for SBG

The SBG alarms and events are generated by the SGC and MP blade systems and sent to the IS Fault Management function on the SIS blade system.

From SIS the alarms and events are forwarded northbound to OSS in IS FM SNMP notifications.

The purpose of the Fault Management function is to:

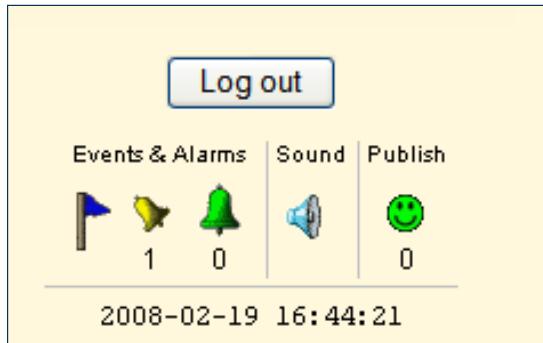
- provide the Alarm and Event northbound interfaces for blade systems in IS
- provide operator and northbound interfaces to read the current IS alarm status; change the alarm severity for a specific alarm type; and change the event handling for individual event types
- maintain the alarm log, event log, and other site logs for IS
- make the logs available via operator and northbound interfaces.

An Alarm generated by an SBG Blade System is sent to SIS. SIS checks the Alarm settings and, depending on the settings SIS can change the severity of the Alarm if configured by the user. It then adds the Alarm to the Alarm log; Displays the Alarm on the current Alarm list; and Sends a northbound trap if configured.

Events are treated in a similar way, in addition the user can configure whether the Event is discarded, logged, displayed, sent northbound.

The management and configuration of Alarms & Events is fully covered in the prerequisite training (IS Operation & Configuration course) and will not be described more here.

The Event and Alarm Status frame



	Red or yellow, swinging	One or more new alarms are waiting for you to acknowledge.
	Red or yellow, hanging	One or more alarms have been acknowledged and are waiting to be cleared.
	Green, hanging	There are no outstanding alarms in the Integrated Site.

The Event and Alarm Status Frame

The Events and Alarms of the SBG are displayed on the IS Alarm and Event status frame as shown in the figure above; and logged as configured.

There is no dedicated display for the SBG alarms and events.

The status frame is located at the bottom left hand corner of the ISM GUI.

Bell Icon colour codes

The position and colour of the bell indicates the different statuses of the alarms as shown in the figure above.

Name	Severity	Fault ID	Time
mgcSs7ItuMtpLinkOutOfServAlarm	major	bs_MGC_33:3077029	2010-06-23 16:42:41
mgcSs7ItuMtpLinkOutOfServAlarm	major	bs_MGC_33:18077029	2010-06-23 16:42:41
mgcSs7ItuMtpLinkOutOfServAlarm	major	bs_MGC_33:16077029	2010-06-23 16:42:41
mgcSs7ItuMtpLinkOutOfServAlarm	major	bs_MGC_33:7077029	2010-06-23 16:42:41
mgcSs7ItuMtpLinkOutOfServAlarm	major	bs_MGC_33:20077029	2010-06-23 16:42:41
nexthopAlarm	minor	bs_SBG_35:4	2010-06-29 13:42:52
mgcUnsavedDataExistAlarm	warning	bs_MGC_33:1001046	2010-06-30 13:18:42
perfDnPrefixAlarm	warning	bs_SBG_35:5	2010-07-01 10:55:00
sisNtpSecondaryUnreachAlarm	minor	bs_SIS_1:3891	2010-08-01 5:44:57

Alarm List

The SBG Alarms appear on the IS Alarm list, together with Alarms from all IS Blade systems.

The Current Alarm List can be opened by double clicking one of the alarm bells in the previous figure, or by selecting *Alarm & Event* → *Current Alarm List* from the Menu Bar.

A list of all current alarms is displayed, with details of Severity, Fault ID and Date/Time.

If an individual alarm is selected, more details are displayed in the lower window, and the HELP button takes the user to the place in the documentation describing the alarm in more detail and describing the steps to take to resolve the fault.

SBG Alarms

SBG system alarms are categorized as follows:

- O&M
- Session Gateway Controller
- Network Configuration,
- Equipment
- Media Supervision
- Media Proxy, Connection Control
- System
- Performance Monitoring

SBG Alarm Categories

SBG Alarms belong to SBG System notifications, which includes alarms and event.

They are categorized by the source of the system notifications.

- **O&M** – Alarms and events related to O&M and OMMP
- **Session Gateway Controller** – Alarms and events related to SGC
- **Network Configuration, Equipment and Media** – Alarms and events related to system configuration administration and maintenance of SBG
- **Media Proxy, Connection Control** – Alarms and events related to connection control (H.248).
- **System** – Alarms and events issued by the System Service
- **Performance Monitoring** – Alarms and events related to Performance Measurement function of the SBG.

The Alarms are described in the CPI Fault Management documents based on the category of the Alarm and are entitled ***System Notifications*** documents. Each alarm has a description as to the cause of the alarm; the default Alarm Severity; and the procedure for examining and resolving the Alarm.

The Alarms are listed on the next page.

SBG OAM Alarms

sbgBsMgmtOpFailedAlarm

Session Gateway Controller Alarms

chargingAlarm

diameterServerAlarm

sgnSgcConfigurationAlarm

sgcExtBgfCtrlLinkDownAlarm

sgcFwBlockingAlarm

sgcNetworkUnavailableMediaAlarm

sgcOutOfServiceAlarm

Network Configuration alarms

nexthopAlarm

addressCollisionAlarm

Equipment alarms

physicalLinkAlarm

physicalLinkQosAlarm

Media alarms

maliciousTrafficAlarm

excessiveTrafficAlarm

Connection control alarms

h248LinkDownAlarm

System alarms

endToEndAlarm

equipmentAlarm

hwIncompatibilityInfoAlarm

plcCpOverloadAlarm

rcmSequentialRestartAlarm

rcmSystemClockAlarm

Performance Monitoring alarms

perfDnPrefixalarm

perfFileTransferAlarm

Example: SBG O&M Alarm Information

2.1 **sbgBsMgmtOpFailedAlarm**

Cause: The Operation and Maintenance & Media Proxy (OMMP) blade system cannot update a managed object in a particular blade system when the corresponding attribute has been changed from the Integrated Site Management system (ISM).

The **Cause** attribute specifies the blade system on which an object cannot be updated. One reason for this alarm could be that the particular blade system has been locked from the **Integrated Site Services** management function area (MFA) and therefore is not available for management operations.

The ITU-T X.733 cause for this alarm is *Underlying resource unavailable* (56).

Severity: Major

Action: If the blade system specified in the **Cause** attribute of the alarm notification is locked, you must unlock it to make it available for management operations again (**Integrated Site Services** → **Hardware** → **Blade systems**).

The unlocking of the blade system will initiate an audit of the blade system database from the OMMP blade system. If the audit is successful, the alarm will be cleared.

If the alarm remains, . . . (truncated for the presentation)

SBG O&M Alarm Information

The SBG O&M notification issued as an alarm is:

sbgBsMgmtOpFailedAlarm

The MP blade system cannot update a managed object in a particular underlying blade system.

The figure above is an example of the information for each alarm and is taken from the Fault Management document:

SYSTEM NOTIFICATIONS 1/190 83-CNA 113 062 Uen K

Operation and Maintenance Session Border Gateway – Integrated Site

The alarm has a description as to the cause of the alarm; the default Alarm Severity; and the procedure for examining and resolving the Alarm (Truncated).

Example SGC and System Alarms

Session Gateway Controller Alarms

- `sgcOutOfServiceAlarm`
- `diameterServerAlarm`

SBG System Alarms

- `equipmentAlarm`
- `plcCpOverloadAlarm`
- `rcmSequentialRestartAlarm`
- `rcmSystemClockAlarm`

Session Gateway Controller Alarms

Example SBG Session Gateway Controller Alarm:

- *sgcOutOfServiceAlarm* - The SGC Operational state has changed to Disabled. The SGC is out of service and no longer available for traffic. This happens when all H.248 control links are out of service, one of the network connections is out of service, or when no signalling routes have been defined between the incoming and the outgoing network connections.

- *diameterServerAlarm* - The connectivity to a diameter server is lost . The alarm is cleared when connection to the diameter server has been reestablished.

System Alarms

Example SBG System Alarms are:

- *equipmentAlarm* - There is a hardware or software-related fault on the board which must be attended to. Inspect the **Cause** attribute to gain information on the fault situation and to find out which blade caused the alarm.
- *plcCpOverloadAlarm* - A control processor (CP) in the blade system is overloaded and rejects requests. The alarm will cease when the CP has been working without overload during a time period of 100 seconds. Make changes to the network configuration, for example, add a CP pair to the Gateway Controller blade system.
- *rcmSequentialRestartAlarm* - A sequential restart was ordered to the blade system. The alarm will be cleared automatically when the sequential restart has been completed. the operator do not have to do anything.
- *rcmSystemClockAlarm* - A large time step has occurred (more than 60 seconds) on the blade system in order to keep up with the time references.

Network Configuration, Equipment and Media Alarms

Network Alarms

- `NexthopAlarm`
- `AddressCollisionAlarm`

Equipment Alarms

- `physicalLinkAlarm`
- `physicalLinkQosAlarm`

Media Alarms

- `maliciousTrafficAlarm`
- `excessiveTrafficAlarm`

Network Configuration, Equipment and Media Alarms

Network Configuration Alarms:

- *nexthopAlarm* - The supervision of a next-hop router failed.
- *addressCollisionAlarm* – An address collision has been detected.

Equipment Alarms :

- *physicalLinkAlarm* – A link error condition has been detected on the external Ethernet link. The type of failure is shown in the Cause attribute of the alarm.
- *physicalLinkQosAlarm* – The percentage of frames with CRC error during a 20-second period exceeds the CRC error threshold. The threshold is configurable via the Media Supervision service.

Media Alarms :

- *maliciousTrafficAlarm* – The received number of malicious packets during a 20-second period has reached or exceeded the **Malicious traffic threshold**. The threshold is configurable via the **Media Supervision** service.
- *excessiveTrafficAlarm* – The threshold for excessive traffic bandwidth has been reached or exceeded. Excessive traffic bandwidth is the average bandwidth of excessive traffic (traffic discarded due to policing), summed up for all media streams in the Media Proxy with policing activated.

Connection Control & Performance Monitoring Alarms

Connection Control Alarm

- `h248LinkDownAlarm`

Performance Monitoring Alarms

- `perfDnPrefixAlarm`
- `perfFileTransferAlarm`

Connection Control Alarm

The Connection Control Alarm is:

- *h248LinkDownAlarm* - H.248 link failure alarm

A H.248 control link for signalling between a Session Gateway Controller (SGC) blade system and a Media Proxy (MP) blade system has failed to function for 30 seconds.

The alarm is issued by the MP side of the control link. This means that no H.248 link alarm will be sent when the MP blade system is not operational.

Performance Monitoring Alarms

The Performance Monitoring Alarms are:

- *perfDnPrefixAlarm* - At least one measurement report has been created, which does not include a distinguished name prefix.
- *perfFileTransferAlarm* - At least one measurement job has failed to transfer its performance data report file to the FTP server's performance data collecting service

Alarm Settings

Name	Severity	Blade system
addressCollisionAlarm	Minor	MGW 0-5-8
addressCollisionAlarm	Minor	OMMP 1-17-21
aspSctpDownAlarm	Major	MGW 0-5-8
chargingAlarm	Major	SGC 1-19-23
cpdRestartAlarm	Critical	SIS
diameterServerAlarm	Major	SGC 1-19-23
dqmHardDiskAlarm	Critical	SIS
dqmHardLimitReachedAlarm	Critical	SIS
dqmSoftLimitReachedAlarm	Critical	SIS
endToEndAlarm	Minor	OMMP 1-17-21
endToEndAlarm	Minor	MGW 0-5-8
endToEndAlarm	Minor	SGC 1-19-23
equipmentAlarm	Major	MGW 0-5-8
equipmentAlarm	Major	OMMP 1-17-21
equipmentAlarm	Major	SGC 1-19-23
excessiveTrafficAlarm	Minor	MGW 0-5-8
excessiveTrafficAlarm	Minor	OMMP 1-17-21
h248LinkDownAlarm	Major	OMMP 1-17-21
h248LinkDownAlarm	Major	MGW 0-5-8
hwIncompatibilityInfoAlarm	Minor	SGC 1-19-23
hwIncompatibilityInfoAlarm	Minor	OMMP 1-17-21
hwIncompatibilityInfoAlarm	Minor	MGW 0-5-8
hwHardwareNotFoundAlarm	Major	SIS
hwNoContactWithBoardAlarm	Major	SIS
hwProductIdentityFaultAlarm	Major	SIS
hwSntNodeDownAlarm	Major	SIS
hwWrongBisSwgAlarm	Major	SIS

SBG Alarm Setting

Select **Alarm & Event → Settings → Alarms** to display the settings for all alarms.

Click on the red triangle for a specific alarm to change its settings.

This allows the user to Change the severity of the Alarm, for example.

Alarms are logged in the default Alarm-Log and this cannot be changed.

Alarm Filter

In order to prevent excessive alarm sending for a repetitive alarm, alarms can be filtered and blocked if excessive alarms occur within the Alarm filter time, defined in the figure above.

The Alarm filter time specifies the time period during which it is allowed to send an alarm *five* times having the same sender, name and cause. The default time is three hours (10800 seconds).

The figure above shows one alarm blocked.

Reset Alarm Filter

The Reset alarm filter function is used to unblock alarms that are blocked due to frequent sending.

It is also used to remove already ceased alarms from the alarm list, because if an alarm has been blocked, and an alarm cease for that alarm has been issued, the alarm will still remain in the alarm list until the alarm filter has been reset.

Name	Administrative state	Operational state	Log size (kbyte)	Delete
Default Log	Up	Up	1 024	<input type="checkbox"/>
Alarm Log	Up	Up	1 024	<input type="checkbox"/>

Alarm & Event Logs

The Alarm and Event Logs can be seen from the **Alarm & Event** → **Alarm & Event logs** link, as shown above.

Alarms are logged in the **Alarm Log**; Events are logged in the **Default Log**.

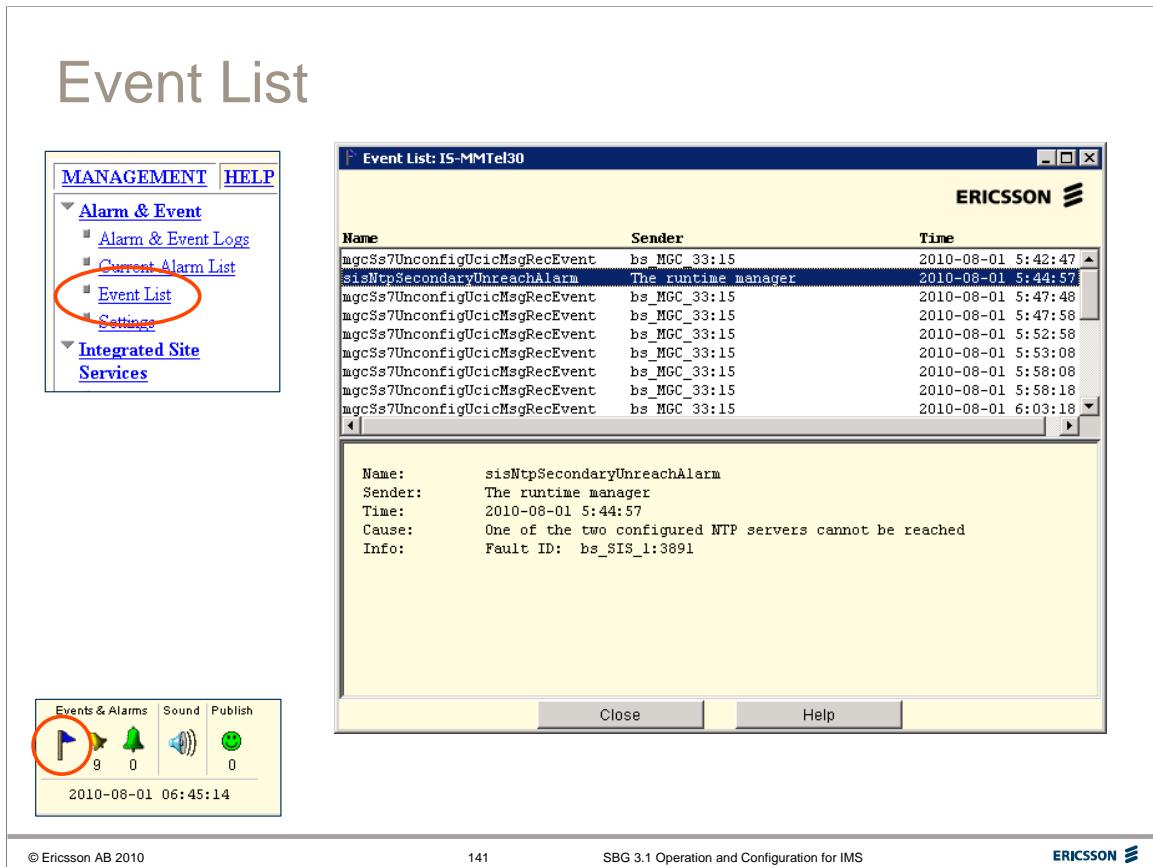
New logs can be created and specific Alarms and Events sent to them, but the Alarms and Events will always be logged to these default logs as well. (Specific Events can be set to no logging, see later).

Alarm Log Status

Click the red triangle on the previous figure to open the screen above. The status of the log can be seen, together with Log size and number of records.

Alarm Log Search

The links can be used to perform searches of the Alarm Log and ftp the results, as well as displaying to screen.



Events

Events are notifications rather than Alarms (which notify a fault situation). Events are managed in a similar way as already described for Alarms.

Examples of SBG Events are: SGC Locking; a Control Link Locked; Unknown SIP Payload received.

See the following page for a complete list of SBG-generated Events. Refer to the Fault Management documentation for detailed descriptions of each.

Event List

The Event List shows a list of recent Events. Selecting an Event displays details of the Event and the HELP button opens the documentation describing the Event in detail.

SBG EVENTS

SBG OAM Events

sbgBsInitialConfigFailedEvent
sbgBsConfigCompletedEvent
sbgContactDatabaseUploadEvent
sbgSmmRuleSetImportEvent
sbgSmmRuleSetExportEvent

Session Gateway Controller Events

sgcBlockingIPTrafficEvent
sgcCallRelDueToEmergCallEvent
sgcContactDatabaseUploadEvent
sgcControlLinkLockedEvent
sgcDeblockingIPTrafficEvent
sgcDestReachEvent
sgcDestUnreachEvent
sgcExceedingRateLimitEvent
sgcExtBgfCtrlLinkDisabledEvent
sgcExtBgfCtrlLinkEnabledEvent
sgcExtBgfCtrlLinkRemLockedEvent
sgcH323NetConnLockedEvent
sgcLockedEvent
sgcRegUserInQuarantineEvent
sgcSipNetConnLockedEvent
sgcSipReqRejByNwThrottlingEvent
sgcSipUnknownPayloadEvent

System events

omsLicenseEvent
rcmSequentialCpRestartEvent
sysCufFtpEvent

Performance monitoring events

perfMeasJobStatusChangedEvent

Event Settings

Event Settings

Event	Treatment	Notes
sbgBsConfigCompletedEvent	Display and log	OMMMP 1-17-21
sbgContactDatabaseUploadEvent	Display and log	OMMMP 1-17-21
sbgSmmRuleSetImportEvent	Display and log	OMMMP 1-17-21
sbgSmmRuleSetExportEvent	Display and log	OMMMP 1-17-21
perfMeasJobStatusChangedEvent	Display	OMMMP 1-17-21
rcmSequentialCpRestartEvent	Display and log	OMMMP 1-17-21
sysCuffFtpEvent	Display and log	OMMMP 1-17-21
omsLicenseEvent	Display and log	OMMMP 1-17-21
perfMeasJobStatusChangedEvent	Display	SGC 1-19-23
rcmSequentialCpRestartEvent	Display and log	SGC 1-19-23
sysCuffFtpEvent	Display and log	SGC 1-19-23
omsLicenseEvent	Display and log	SGC 1-19-23
sgcCallRelDueToEmergCallEvent	Log and trap	
sgcLockedEvent	Log and trap	
sgcH323NetConnLockedEvent	Log and trap	
sgcControlLinkLockedEvent	Log and trap	
sgcRegUserInQuarantineEvent	Log and trap	
sgcDestUnreachEvent	Display and log	

Event Settings
perfMeasJobStatusChangedEvent

Blade system: SGC 1-19-23

Treatment:

Notify name:

User note:

Event Management & Settings

As already described, Events are normally logged in the DefaultLog and displayed on the Event list.

The Treatment of specific Events can be changed in the *Alarm & Event* → *Settings* → *Event Settings* page, as shown above.

Events can be

Discarded;

Logged only;

Displayed on the Event List only;

sent as a trap;

or a combination of treatments.

The default setting is usually “*Display and Log*”



ERICSSON

SBG 3.1 Operation and Configuration for IMS

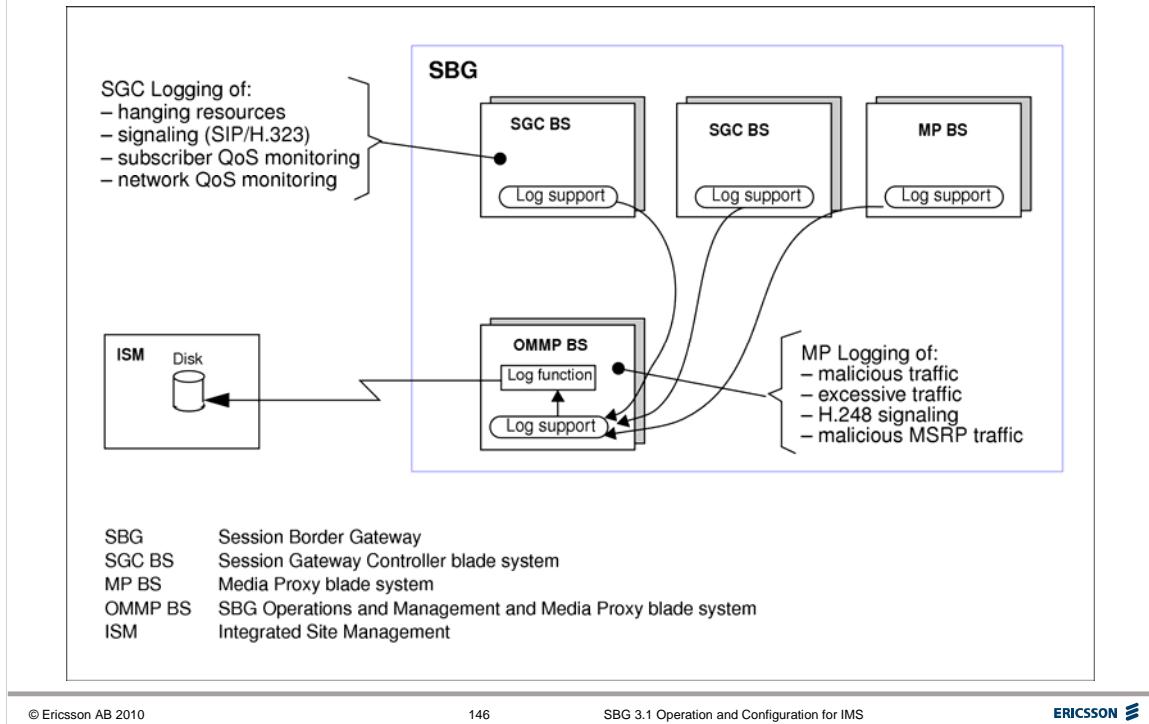
SBG Logs

This section gives an overview of the SBG Logging function, for more details, refer to the document:

SERVICE GUIDE 8/154 43-CNA 113 062
Logs - Session Border Gateway – Integrated Site

IS function logs for IS Blades and Audit Trail logs are not described, as these are covered in detail on the IS Training courses.

SBG Logging Mechanism



SBG Logging Mechanism

The SBG specific logs are coordinated through the OMMB blade system.

The OMMB blade system hosts the central log function for the SBG that stores the log data on the disk of the ISM. The logs use the disk space associated with the OMMB blade system.

The Session Gateway Controller (SGC) blade systems send their log records through the OMMB blade system as illustrated above.

Each log record contains a time stamp - the date and time when the record was written. There is also information in each log record about which blade system it came from.

All the logs are wrap-around logs, when they become full the oldest log data is lost and overwritten by new log data.

SBG Logs

MANAGEMENT **HELP**

- ▶ [Alarm & Event](#)
- ▶ [Integrated Site Services](#)
- ▶ [Main Switch](#)
- ▶ [Integrated Site Edge Router](#)
- ▶ [MGC 0-11-17](#)
- ▶ [MGW 0-5-8](#)
- ▶ [Session Border Gateway](#)
 - [Equipment](#)
 - [Logs](#)
 - [Media Control](#)
 - [Media Supervision](#)
 - [Network Configuration](#)
 - [Performance Monitoring](#)
 - [QoS Monitoring](#)
 - [Session Signaling](#)
 - [System](#)

Session Border Gateway Logs

Logs

[View blade system logs](#)
[Transfer blade system logs](#)
[Transfer additional system information](#)

SBG Logs

The SBG blade system can supply Blade system logs and/or Additional system information.

Blade system logs contain information about events of interest to the operator, such as excess traffic, malicious traffic and QoS.

Transfer Additional system information is a collection of files which can be transferred to a remote ftp server for use by Ericsson personnel when investigating an operator reported issue. See IS Training course for details.

The View **Blade system logs** link provides management operations that allow the user to:

- Transfer a copy of all logs or a subset of logs associated with a given blade system
- Read a description of the contents of the logs and access the Customer Product Information (CPI) documents associated with the log.

Logs in ASCII format can be viewed via the GUI.

Both SBG Blade System logs and ASI files can be transferred externally to a remote system via FTP.

SBG Blade System Logs

Logs					ERICSSON
View blade system logs					ERICSSON
Blade system: OMMP 1-17-21					ERICSSON
<hr/>					
Log name	Size	Type	Format	Modified	Description
mpExcessiveTrafficLog	3	Directory	ASCII	2010-08-25 08:18:08	Excessive traffic (MP)
mpH248Log	3	Directory	ASCII	2010-08-25 08:18:08	H 248 Signaling log (MP)
mpMaliciousMSRPLog	3	Directory	ASCII	2010-08-25 08:18:07	Malicious MSRP (MP)
mpMaliciousTrafficLog	3	Directory	ASCII	2010-08-25 08:18:08	Malicious traffic (MP)
sgcHangingResourcesLog	3	Directory	ASCII	2010-08-25 08:18:08	Hanging resources (SGC)
sgcNetworkQosLog	3	Directory	ASCII	2010-08-25 08:18:08	Network QoS (SGC)
sgcSignalingLog	3	Directory	ASCII	2010-08-25 08:18:08	Signaling log (SGC)
sgcUserQosLog	3	Directory	ASCII	2010-08-25 08:18:08	User QoS (SGC)
selLog	0	Directory	ASCII	2010-08-25 08:14:14	SEL log
perfFileLog	81	File	ASCII	2010-08-25 08:17:59	A log of performance file transfer failures

© Ericsson AB 2010

148

SBG 3.1 Operation and Configuration for IMS

ERICSSON

SBG Logs

mpExcessiveTrafficLog

The excessive bandwidth log is used to log information about excessive media received per media stream.

The log contains information per media stream including date and time, source and destination IP address, protocol, number of packets discarded etc.

mpH248Log

The H.248 signalling log includes information about H.248 link status and any H.248 signalling errors detected by the MP blade system during SBG operation. This means, for example, that there will be a log record written to the log each time a H.248 link becomes non-operational or operational.

mpMaliciousMSRPLog

The MSRP malicious traffic log is used by the MP to log information about MSRP chunks that are considered malicious for some of the reasons listed below:

- Missing To-Path header field
- Missing From-Path header field
- Incorrect To-Path header field
- Incorrect From-Path header field
- Header format error
- Header too long

SBG Logs (cont)

mpMaliciousTrafficLog

The malicious traffic log is used by the MP to log information about IP packets that are considered malicious for some of the reasons listed below:

- Packet received with incorrect source IP address or port
- IP options received
- Fragmented IP packet received
- Unsupported protocol received, that is, not UDP, TCP, or ICMP
- Invalid or unsupported Internet Control Message Protocol (ICMP) packet received
- Payload (UDP/TCP) packet received, but no related media stream (pin-hole) exists
- Invalid packet size, for example, wrong IP length field or too short ICMP packet
- Wrong protocol
- Invalid combination of TCP flags received for a TCP stream, that is, both SYN and FIN flags set
- Incompatible IP and UDP length fields (that is, the IP length is not equal to the UDP length plus 20 octets)

sgcHangingResourcesLog

This hanging resources log is used to log events associated with the detection of media inactivity (also called media stop) and signalling inactivity. Media inactivity is detected by the MP and is notified via H.248 to the SGC. signalling inactivity is detected by the SGC.

sgcNetworkQoSLog

The network quality of service log is used to log information regarding the measured quality of service for a specific network in the SBG. The information in the log is collected by the SGC. The SGC will here order the MP to retrieve call counter data for every Nth call and from this data calculate the network quality of service statistics.

sgcSignallingLog

This log is used to log events associated with the SIP or H.323 signalling in the SGC.

sgcUserQoSLog

The user quality of service log is used to log information about the user (SIP users) that have quality of service monitoring activated. Calls to and from a monitored public user identifier will be supervised and statistics about both directions of the media flow will be collected.

perfFileLog

This Performance File Transfer Failures log contains log entries for every transfer error that has occurred between the SBG and the remote ftp client during measurement data file transfer.

(The *sel.log* is a Linux operating system log, not relevant in this context)

SGC Blade System Logs

Logs				
View blade system logs				
Blade system: SGC 1-19-23				
<hr/>				
Log name	Size	Type	Format	Modified
FirewallLog	6	Directory	ASCII	2010-08-25 08:26:59
sellog	3	Directory	ASCII	2010-08-25 08:24:21
perfFileLog	81	File	ASCII	2010-08-25 08:26:58
A log of blocked/unblocked IP-addresses				
SEL log				
A log of performance file transfer failures				

Firewall Log

An event notification is issued when SGC is subject to traffic flooding, or other SIP abuse and an alarm is issued when the amount of data discarded in the MP exceeds configurable thresholds. Rejected SIP and H.323 messages are also logged together with source and destination IP addresses.

If limits are exceeded the source IP address/port can be automatically blocked for a time. The addresses which are blocked are logged in the **Firewall Log**. The structure of the log records is:

Time

Net: the VLAN id

IP-address

Port

Protocol: UDP, TCP or SCTP

Action: *Block* or *Unblock*

Reason: string with reason why IP-address was blocked

Integrated Site Services Logs



MANAGEMENT | **HELP**

- ▶ [Alarm & Event](#)
- ▼ [Integrated Site Services](#)
 - [Administration](#)
 - [Hardware](#)
 - [Logs](#)
 - [Network Configuration](#)
 - [Remote Management](#)
 - [Software](#)
 - [User Interface](#)
- ▶ [Main Switch](#)
- ▶ [Integrated Site Edge Router](#)
- ▶ [MGC 0-11-17](#)
- ▶ [MGW 0-5-8](#)
- ▶ [Session Border Gateway](#)

Integrated Site Services Logs

Logs

[View blade system logs](#)
[Transfer blade system logs](#)
[Transfer additional system information](#)
[ISM audit trail logs](#)

Integrated Site Services Logs

All Blade System logs can be viewed and transferred from the ISM Logs page, as shown above.

In addition, Audit trail logs are available.

These are fully described in the IS Training courses and will not be further described here.

Integrated Site Services Logs

[View blade system logs](#)
[Transfer blade system logs](#)
[Transfer additional system information](#)
[ISM audit trail logs](#)

ISM audit trail logs

[Audit trail logs](#)

Name	Operational state	Log size (kbyte)
► SNMP Agent Log	Up	20 480
► ISM Log	Up	1 024
► Console Log	Up	512
► CMF Log	Up	1 024

[Table as text](#)

[Transfer all logs](#)

Audit Trail Logs

The Audit Trail Logs are not specific for SBG but are part of IS O&M.

The audit trail log files include:

- **SNMP agent log** - SNMP agent activities
 - **ISM log** - Actions performed via the ISM User Interface.
 - **Console log** - Actions performed via a directly connected console.
 - **CMF log** - Actions performed via the Common Management Function (CMF).
 - **Security log** - Successful and unsuccessful user log-in attempts and logout via the ISM-UI.
- This log is only available to users having sufficient security clearance.

Exercise 5



ERICSSON

SBG 3.1 Operation and Configuration for IMS

SBG Performance Management



This section describes how to view SBG performance data, how to create measurement jobs and how to transfer measurement data. For more details, refer to the following documents -

Service Guide 4/154 43-CNA 113 49

Performance Monitoring - Application Blade System – Integrated Site

Interworking Description 1/155 19-CNA 113 49

Performance Monitoring - Application Blade System – Integrated Site

SBG Performance Management

- Counters and Gauges grouped in Managed Object classes
- Used to review the performance of SBG
- View Realtime
- Create Performance Measurement scheduled collection
- Results can be used to:
 - Optimize the overall network performance
 - Verify Quality of Service levels
 - other

SBG Performance Measurement

Performance Measurements are collected to review the performance of an SBG.

Based on the results the operator can make changes to optimize the overall network performance, for example, by adjusting parameter values or reconfiguring the observed system or other systems, or restructuring the network.

Performance Measurements can also be used to verify Quality of Service levels.

The Counter and Gauge attributes are grouped into Managed Object classes.

Viewing immediate Performance Data

Current values of Performance counters and gauges can be viewed in real time by going to the Measurement area in the SBG GUI Menus.

Performance Measurements

Performance measurement jobs can be scheduled to gather statistics periodically and transfer to an external ftp server.

In many places, particularly on screens showing current counter and gauge values, there are links to configure periodic Performance Measurement scheduled jobs.

SBG Performance Monitoring

SBG Performance statistics can be viewed for:

- Equipment
- Media Control
- Media Supervision
- QoS Monitoring
- Session signalling
- System

SBG Performance Monitoring

Performance statistics are viewed in the ISM GUI for the following SBG function areas:

- **Equipment** - IP statistics on interfaces
- **Media Control** - H.248 link statistics
- **Media Supervision** - Network, Streams and MSRP statistics
- **QoS Monitoring** - QoS statistics per Network and per User
- **Session Signalling** - SIP and H.323 signalling statistics
- **System** - Critical resources statistics

Equipment Statistics

- Traffic management statistics
- Ethernet interface statistics
- Bandwidth statistics
- Other statistics

Equipment Statistics

Ethernet Interface Statistics can be seen under *Equipment* → *Ethernet Interfaces* and Open a port (red triangle).

There are four groups of statistics:

Traffic Management

Ethernet Interface

Bandwidth

Other

These are fully described in the *Equipment Service Guide*.

The following pages show example screen captures of the four statistics groups.

SBG - Equipment		ERICSSON	
Ethernet interface		Traffic management statistics	
Subrack:	1	Transmitted EF packets :	881
Slot:	17	Transmitted IC packets :	0
Port:	2	Transmitted AF1 packets :	0
Blade system:	OMMP 1-17-	Transmitted AF2 packets :	0
MAC address:	00:01:EC:B4:3	Transmitted AF3 packets :	0
Administrative state:	unlocked	Transmitted AF4 packets :	0
Operational state:	enabled	Transmitted DF packets :	0
Flow control operational mode:	transmit and receive	Discarded EF packets :	0
Admission control		Discarded IC packets :	0
Lock		Discarded AF1 packets :	0
		Discarded AF2 packets :	0
		Discarded AF3 packets :	0
		Discarded AF4 packets :	0
		Discarded DF packets:	0
		Ethernet interface statistics	
		Performance measurement on Traffic management statistics	
		Transmitted frames:	6455
		Transmitted octets:	444738
		Received valid frames:	1460994
		Received octets:	96991122
		Transmitted broadcast frames:	18
		Received broadcast frames:	2040
		Received MAC control frames:	0
		Transmitted PAUSE frames:	0
		Received multicast frames:	1441669
		Received error-free frames discarded:	0
		Received invalid frames:	1447718
		Error-free frames not transmitted:	0

View Immediate Equipment (Ethernet Interface) Statistics

The example above shows the statistics for the Ethernet Interface on port 2 on the OMMP Blade in slot 17.

This screen is reached from the *SBG* → *Equipment* → *Ethernet Interfaces* link, and by clicking the red triangle next to the required entry.

Performance Measurement Jobs for this specific port can also be created from this screen, by clicking the appropriate link.

Traffic Management Statistics

This group presents statistics about Transmitted/Discarded DiffServ packets for the selected Ethernet Interface :

- Expedited Forwarding (EF)
- Network Control (NC)/Internetwork Control (IC)
- Assured Forwarding 1-4 (AF1-AF4)
- Default Forwarding (DF)

Ethernet Interface Statistics

This group presents statistics about the selected Ethernet Interface Transmitted/Received IP packets.

Performance Measurement Links

There are several links to allow the user to create a measurement job for the statistics shown.

Equipment Statistics 2

Bandwidth statistics	
Performance measurement on Bandwidth statistics	
Receive bandwidth (bit/s):	2080
Transmit bandwidth (bit/s):	0
Other statistics	
Received frames discarded due to FCS error:	0
Received frames discarded due to frame too long:	0
Received frames discarded due to frame too short:	0
Received frames discarded due to wrong MAC address:	1443673
Received frames discarded due to wrong VLAN ID:	0
Received frames discarded due to unknown ethernet protocol:	0
Received frames discarded due to other reasons:	6057
Received frames with a length of 64 octets:	1067982
Received frames with a length of 65-127 octets:	388252
Received frames with a length of 128-255 octets:	713
Received frames with a length of 256-511 octets:	6070
Received frames with a length of 512-1023 octets:	0
Received frames with a length of 1024-1522 octets:	0
Discarded L3 packets:	0

Bandwidth Statistics

This group shows Bandwidth statistics for the selected Ethernet Interface, i.e. the total Receive and Transmit bandwidth in bits per second excluding framing bits but including Frame Check Sequence (FCS) octets.

The bandwidth is the mean value measured over the last 8-second period.

Other Statistics

This group shows various statistics about the numbers of frames discarded for different reasons and counters for different packet lengths.

Performance Measurement Links

There is a link to allow the user to create a measurement job for the statistics shown.

MP Control Links Statistics

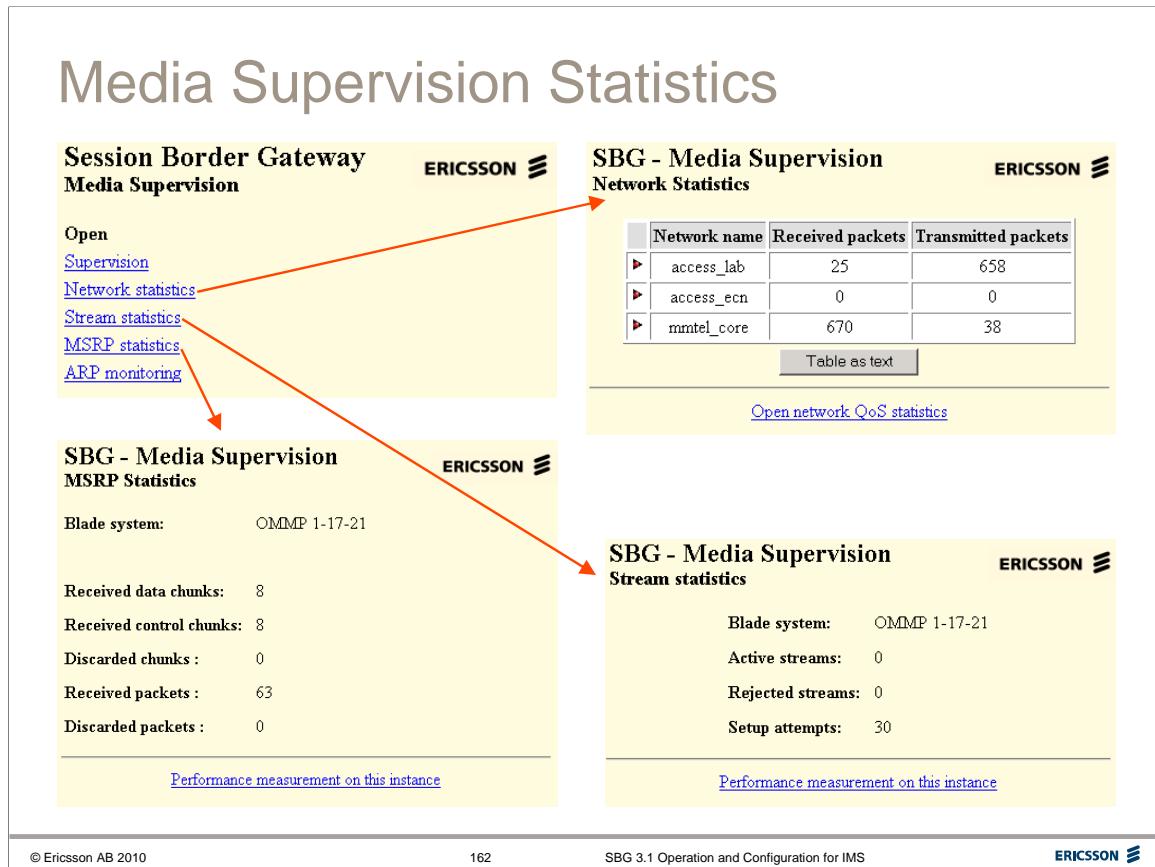
SBG - System	
MP Control link statistics	
Blade system:	SGC 1-19-23
Link ID:	bs_SBG_35/1
Active contexts:	0
Total context setup attempts:	34
Failed context setup attempts:	0
Active transactions:	0
H.248 requests sent:	860
"Invalid ID" replies:	0
"No resource available" replies:	0
"Server error" replies:	0
"Protocol error" replies:	768
Other errors:	1
Abnormally terminated context setup attempts:	0
Hanging terminations released:	0

MP Control Link Statistics

Statistics for the performance of the H248 Media Proxy control links can be seen on this page.

To view, go to:

System → MP Control links → Open a control link (red triangle) → Click “MP control link statistics”



Media Supervision

The **Media Supervision** function area links to three areas of Media Supervision statistics:

Network Statistics (IP)

Stream Statistics (Media)

MSRP Statistics

There are also links to **Supervision** and **ARP Monitoring**. From these two links, monitoring and supervision parameters can be set.

Network statistics

Displays **IP Interface statistics** and **IP Network statistics** for each IP Network.

Stream Statistics

Displays Media Stream statistics for each Media Proxy Blade System.

MSRP Statistics

Displays MSRP statistics for each Media Proxy Blade System.

A message can be delivered in more than one MSRP SEND request. Each of these portions of the complete message is called a *chunk*. MSRP REPORTs report on the status of a previously sent message, or a range of bytes inside a message.

If an MSRP end point receives a request, it may generate an MSRP response, depending on what has been settled for the connection between the end points.

Performance Measurement Links

There are several links to allow the user to create a measurement job for the statistics shown.

Session Border Gateway **ERICSSON**

Media Supervision

- [Open](#)
- [Supervision](#) **Open**
- [Network statistics](#)
- [Stream statistics](#)
- [MSRP statistics](#)
- [ARP monitoring](#)

SBG - Media Supervision Supervision **ERICSSON**

Malicious traffic threshold:

Malicious traffic hysteresis:

Malicious traffic logging: on off

Excessive traffic threshold (kbit/s):

Excessive traffic hysteresis (kbit/s):

Excessive traffic logging: on off

Malicious MSRP logging: on off

Next hop supervision included in blade redundancy: on off

CRC error threshold (%):

CRC error hysteresis (%):

SBG - Media Supervision ARP Monitoring **ERICSSON**

Next hop ARP request threshold:

Fast supervision interval:

Slow supervision interval:

Supervision interval when down:

Address collision supervision interval:

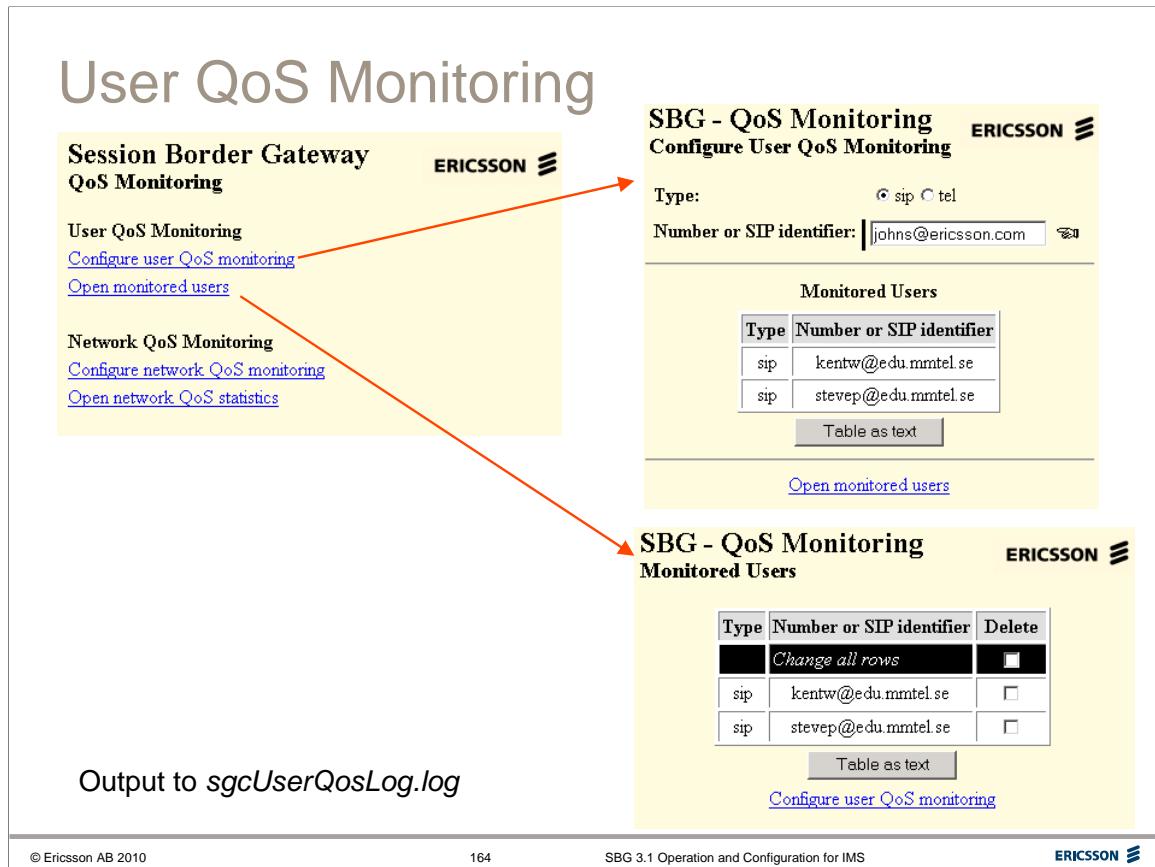
Address collision ARP request threshold:

Media Supervision Settings

Various thresholds can be set, also *Malicious Traffic logging*; *Excessive Traffic logging*; and *Malicious MSRP logging* can be switched on or off.

ARP Monitoring Settings

Various ARP Monitoring parameters can be set.



QoS Monitoring

QoS Monitoring can be performed ***per User or per Network***:

User QoS Monitoring

The operator can monitor all the calls to/from an individual user registered to the A-SBG based on the Public User Identity of the user. The function is not applicable to N-SBG.

If an individual session consists of multiple streams, there will be separate log entries for each stream.

QoS related data for a maximum of 200 Public User Identities can be configured.

Add User to QoS Monitoring

To add a user to QoS Monitoring go to:

QoS Monitoring → Configure user QoS monitoring

select URI type and add the user's sip URI or tel URL.

To view users currently monitored, or to delete a monitored user, go to:

QoS Monitoring → Open monitored users

QoS Logging

The monitoring output is directed to the log file: ***sgcUserQosLog.log***

User QoS Log

A User QoS Log record consists of:

a heading section consisting of:

- a timestamp
- a blade system identifier
- the Public User Identity of the calling user
- the Public User Identity of the called user
- an indicator telling whether it was the Public User Identity of the calling user or the called user that triggered the monitoring
- the media type of the stream

a statistics section, consisting of two network parts (originating and terminating) with:

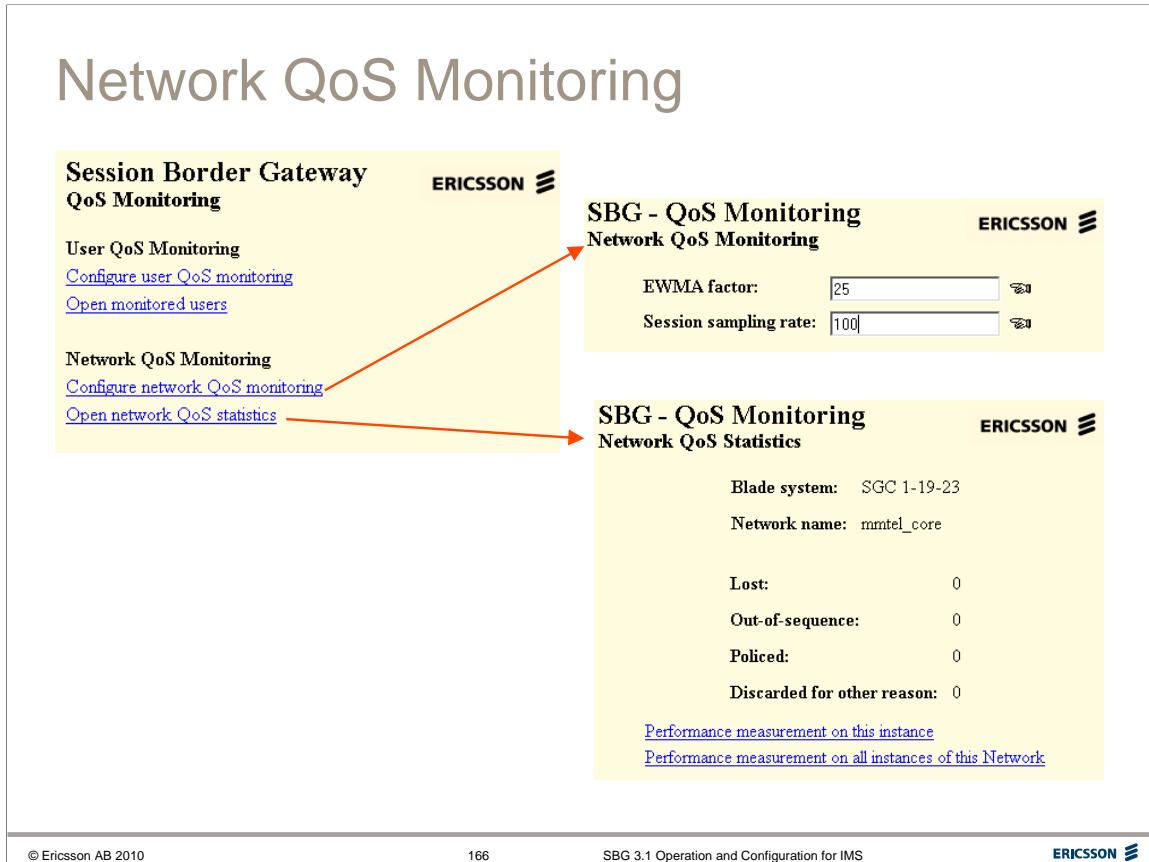
- a network ID
- MP and external BGF statistics (see below)
- User-reported RTCP statistics

MP and external BGF statistics

The following counters are included in the group:

- Packets sent: Number of packets sent to a user.
- Packets received: Number of packets received from a user.
- Octets sent: Number of octets sent to a user.
- Octets received: Number of octets received from a user.
- Discarded packets: Received packets that were discarded due to source filtering, faulty transport protocol, or wrong RTP version.
- Discarded octets: Received octets that were discarded due to source filtering, faulty transport protocol, or wrong RTP version.
- Discarded packets - Policing: Received packets that were discarded due to bandwidth policing (the user is exceeding per-stream bandwidth limits).
- Discarded octets - Policing: Received octets that were discarded due to bandwidth policing (the user is exceeding per-stream bandwidth limits). This is a count on the complete IPv4 packet, including the header.
- Packets out of sequence: Packets that arrived out of sequence. Calculated only for monitored RTP streams and based on received sequence numbers.
- Number of lost packets: Packets that were expected but not received. Calculated only for monitored RTP streams and based on received sequence numbers.

If a counter above is not supported by an MP or external BGF, it will be set to 0.



Network QoS Monitoring

The network QoS monitoring function allows the user to get an overall figure of the QoS of the traffic on each of the networks connected to the SBG.

Network QoS monitoring works by supervising all streams from every N th call in the traffic between the networks to get QoS statistics.

Session sampling rate ('N') is configured in the *Configure network QoS monitoring* screen, as shown above.

A log entry is recorded on the release of a stream. Each session can have one or more streams and a separate log entry is recorded for each stream.

The statistics consist of performance counters and ratio values of certain metrics. The ratio values are calculated using the *current average* method.

In addition, overall floating average estimations of the same metrics as with the current ratio method are calculated based on all streams monitored so far on the network. This is done with a method called EWMA (Exponential Weighted Moving Average).

Each log entry contains the performance counters and current ratio metrics of the monitored stream and also statistics based on EWMA from all monitored streams so far for a particular network.

The *Network QoS Statistics* screen shows current statistics from all the monitored streams per network.

Performance Measurement Links

There are several links to allow the user to create a measurement job for the statistics shown.

Session Signalling Statistics

SBG - Session Signaling
SIP Statistics

Blade system:	SGC 1-19-23
Network name:	access_lab
<hr/>	
SIP session statistics	
Active incoming sessions:	0
Active outgoing sessions:	0
Active originating sessions with local media:	0
Incoming session setup attempts:	24
Incoming rejected sessions:	0
Outgoing session setup attempts:	10
Outgoing rejected sessions:	7
Rejected sessions - no matching codec in answer:	0
Rejected sessions - no matching codec in offer:	0
Rejected sessions - temporary SGC overload:	0
Rejected sessions - user not found :	0
Rejected sessions - user not registered:	876
Rejected sessions - unsuccessful DNS query:	0
Rejected sessions - no BGF resources available:	0
SGC released sessions - media stop:	0
SGC released sessions - session timer expired:	0
BGF reselections :	0
SDP address validation failures:	0

[Performance measurement on this instance](#)
[Performance measurement on all instances of this Network](#)

SBG - Session Signaling
Resource Statistics

Blade system:	SGC 1-19-23
Maximum number of registered users:	120000
Currently registered users:	2
Number of active sessions:	0

[Performance measurement on this instance](#)

© Ericsson AB 2010
ERICSSON

167
SBG 3.1 Operation and Configuration for IMS

Signalling Statistics

SIP Statistics

To view SIP Statistics go to:

Session Signalling → SIP network connections → Open a Blade System (red triangle) → Scroll to bottom and Click “SIP Connection Statistics”

Current statistics values are displayed, as shown above. Measurement Jobs can also be started from this page.

Resource Statistics

Statistics showing the number of Registered Users and the number of Active Sessions can be seen on this page. Go to:

Session Signalling → Resource Statistics

H323 Statistics

H323 Signalling Statistics can also be viewed from:

Session Signalling → H323 network connections

Performance Measurement Links

There are several links to allow the user to create a measurement job for the statistics shown.

System Critical Resources Statistics

SBG - System Critical Resources

ERICSSON 

Blade position:	1-19
Blade system:	SGC 1-19-23
Blade processor load (%):	2
Blade processor memory (Mbytes):	3292
Used blade processor memory (Mbytes):	229
Used blade processor memory (%):	6

[Performance measurement on this instance](#)
[Performance measurement on all SGC blade systems](#)

SBG - System Critical Resources

ERICSSON 

Blade position:	1-17
Blade system:	OMMP 1-17-21
Blade processor load (%):	0
Blade processor memory (Mbytes):	1011
Used blade processor memory (Mbytes):	397
Used blade processor memory (%):	39

[Performance measurement on this instance](#)
[Performance measurement on all MP blade systems](#)

System Critical Resources

To view the current values of Critical Resource usage for each SBG blade, go to:

System → Blade System Administration → Open a Blade System (red triangle) → Open a Blade (red triangle)

The Critical Resources screen is displayed, as shown above for an SGC blade and an OMMP blade.

The statistics shown are:

Blade processor load (%) - The average percentage load during the last minute.

Blade processor memory (Mbytes) - The total processor memory in Mbyte.

Used blade processor memory (Mbytes) - The amount of processor memory in use.

Used blade processor memory (%) - The percentage of processor memory in use.

Performance Measurement Links

There are several links to allow the user to create a measurement job for the statistics shown.

SBG 3.1 Operation and Configuration for IMS

SBG Performance Measurement Jobs

Performance Measurement Job Handling in SBG

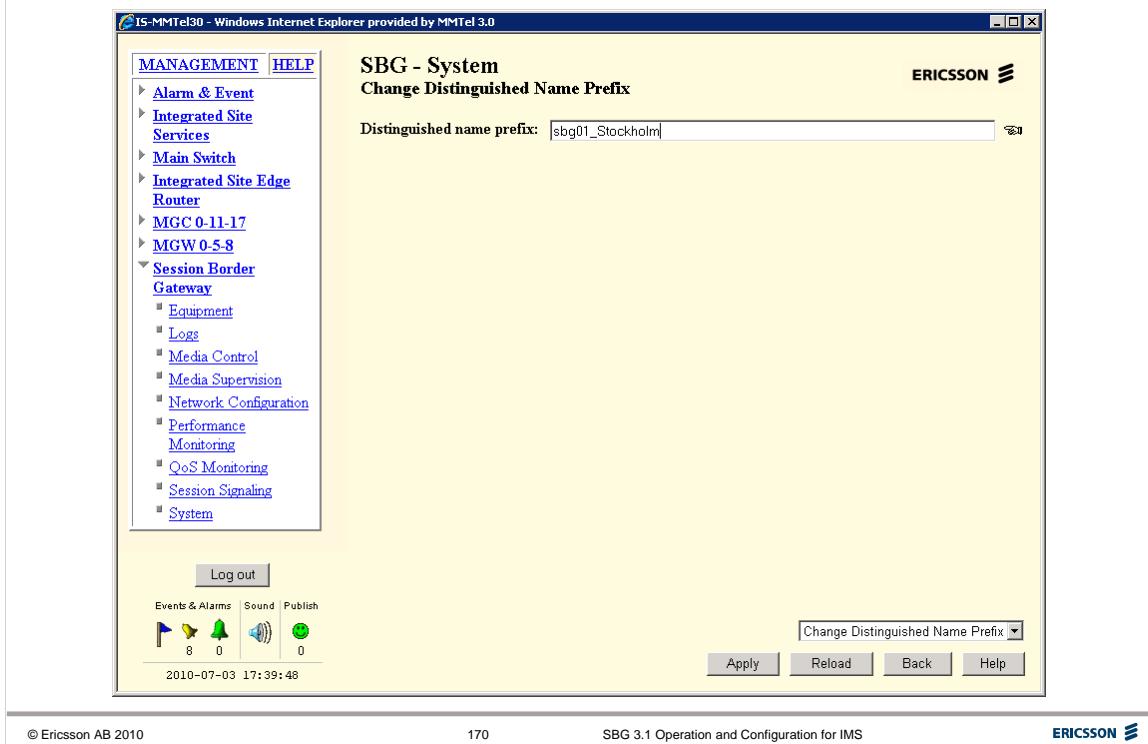
Performance data can also be collected by creating *Measurement Jobs*.

In the previous section, links to Performance Measurements function were seen. These links allow the user to set up measurement jobs on the counters & gauges for the particular area.

Performance Measurement Jobs can be suspended or deleted. A suspended job can be resumed, but a deleted job cannot be recovered.

The Performance Measurement function collects data into files for each measurement job and transfers the collected data by ftp, to for example a network management system.

Distinguished Name Prefix



Distinguished Name Prefix

Before Performance Measurement jobs can be created, the distinguished name prefix must be configured.

Distinguished names are used to identify instances of managed object classes in performance measurement data files.

To configure the distinguished name prefix for the blade system go to:

System → Change distinguished name prefix and enter a suitable name.

In performance data reports, the distinguished name for the CP managed object class may look like this:

DN=mynetwork.operator.com,

SubNetwork=IsNetwork,IsSite=KualaLumpur1,bsId=4,Blade=0-3,Cp=*

Or just simply the node name itself like **sbg01_Stockholm**

The part in bold is the distinguished name prefix.

If the distinguished name prefix is not configured when measurement report data are to be saved, an alarm will be issued, and the data will be saved with no distinguished name prefix. As a consequence, a performance the statistics collection service may misidentify or ignore the data sent.

Creating a Performance Measurement Job

Example

SBG - Equipment
Ethernet interfaces

Subrack	Slot	Port	Blade system	MAC address	Administrative state	Operational state	Flow control operational mode
1	17	0	OMMP 1-17-21	00:01:EC:B4:39:02	-	enabled	transmit enabled
1	17	1	OMMP 1-17-21	00:01:EC:B4:39:03	-	enabled	transmit enabled
1	17	2	OMMP 1-17-21	00:01:EC:B4:39:04	unlocked	enabled	transmit and receive enabled
1	17	3	OMMP 1-17-21	00:01:EC:B4:39:05	unlocked	enabled	transmit and receive enabled
1	21	0	OMMP 1-17-21	00:13:5E:25:A7:FA	-	enabled	transmit enabled
1	21	1	OMMP 1-17-21	00:13:5E:25:A7:FB	-	enabled	transmit enabled
1	21	2	OMMP 1-17-21	00:13:5E:25:A7:FC	unlocked	enabled	transmit and receive enabled
1	21	3	OMMP 1-17-21	00:13:5E:25:A7:FD	unlocked	enabled	transmit and receive enabled

[Table as text](#)

Performance measurement on all MP blade systems

[Traffic management statistics](#)
[Ethernet interface statistics](#)
[Bandwidth statistics](#)

© Ericsson AB 2010

171

SBG 3.1 Operation and Configuration for IMS

ERICSSON

Creating a Performance Measurement Job

Performance Measurement (PM) Jobs are created from the relevant individual function areas described on the previous pages.

The following example shows how to create a measurement job for Ethernet Interfaces performance data.

The process is the same for all other Performance Measurement areas described in the previous pages.

The figure above shows the Ethernet Interfaces view from the **SBG → Equipment → Ethernet Interfaces** link.

At the bottom of the page there are links to start Performance Measurement Jobs

Click a link to open the **Create Measurement Job** page for the measurement statistics MO selected. See the following page.

Similar links are available throughout the SBG Services where statistical values can be collected, allowing the user to set up PM Jobs..

Create Measurement Job

Performance Monitoring

Create Measurement Job

Managed object class:	EthernetInterface	Managed object class:	EthernetInterface
Measurement family:	Ethernet_interface_statistics	Measurement family:	Traffic_management_statistics
Instance:	*,*,*,*	Instance:	9,0,3,2
Administrative state:	On		
Granularity period:	15 minutes		
Reports per file:	4		
Job group id:	SBG_Ethernet_Interface_Stats		
Host:	192.168.3.99		
User:	sbg_expert		
Password:	*****		
Remote directory:	/SBG_PM_jobs		
Priority:	Medium		

Create Measurement Job

Create **Reload** **Back** **Help**

© Ericsson AB 2010 172 SBG 3.1 Operation and Configuration for IMS ERICSSON

Create Measurement Job

When a Performance Measurements link is selected the Create Measurement Job page opens. The **Create Measurement Job** page must be completed with the following parameters:

Administrative state - On or Off.

Granularity period - The period between the initiation of two successive gatherings of measurement data. The period can be set to 5 minutes, 15 minutes, 30 minutes, 1 hour, 12 hours or 24 hours.

Reports per file - The Reports per file attribute makes up a reporting period which is a multiple of the granularity period. If set greater than one, the measurement data is stored until the required number of reports are available and then the measurement data file is created and transferred to the specified host.

e.g. Granularity = 15 mins; Reports per file=4 → File output every hour.

Job group ID - the operator can assign a name to the measurement job. This field is included in the measurement job file output.

FTP parameters – Host address, User, Password and Remote directory

Priority - The Priority attribute is the factor that determines which measurement jobs to suspend if overload conditions occur. The priority can be High, Medium, or Low. Medium is the recommended priority.

NOTE: The **Instance** attribute format is **Blade system number, Subrack, Slot, Port**. In the example above it is set to ***,*,*,*** which means **All Instances**. (The inset shows an example if only one instance is selected – **9,0,3,2**.)

Viewing Measurement Jobs

Performance Monitoring						ERICSSON 
Measurement Jobs						
Job Id	MO Class	Measurement family	Administrative state	Job status	Delete	
<input type="checkbox"/> Change all rows						<input type="checkbox"/>
1	EthernetInterface	Ethernet_interface_statistics	On	Active	<input type="checkbox"/>	
2	EthernetInterface	Bandwidth_statistics	On	Active	<input type="checkbox"/>	

View Measurement Jobs

After creating the job, the operator can view a list of configured performance measurement jobs by selecting *Performance measurement jobs* in the *Performance Monitoring* service of SBG.

The jobs can be modified (FTP Host settings and Priority); and the Administrative State can be set on/off.

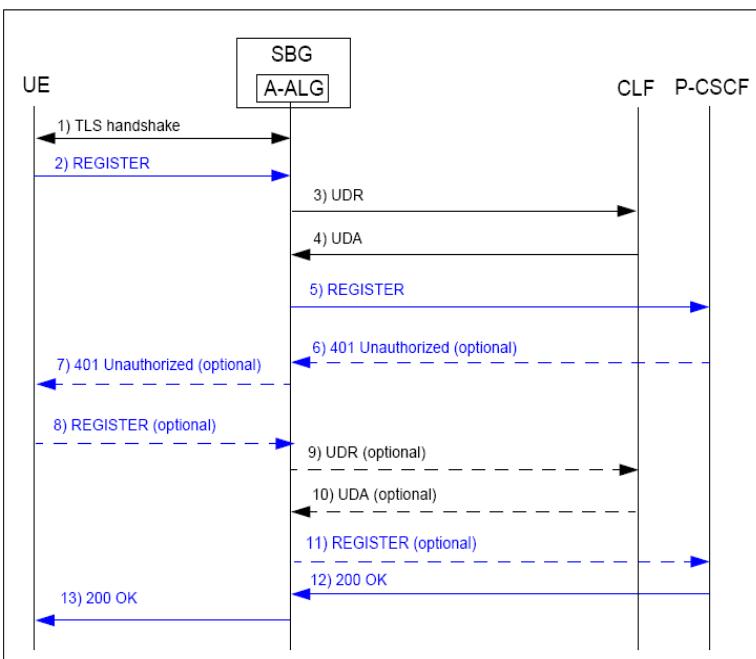
Jobs can also be deleted. It is better to set the Admin state to Off before deleting a job in order not to lose current statistics.

Exercise 6

SBG 3.1 Operation and Configuration for IMS

Signalling Through SBG

Registration of User in A-SBG



Example Use Cases of SBG

This section gives overview examples of signalling sequences involving the SBG. The examples do not cover the complete range of SBG function and are only intended to give a brief high-level figure of the SBG's relationships to other nodes.

Registration of User in A-SBG

DNS queries are not shown in the figures.

The following steps are taken during registration.

1. The user initiates a TLS handshake with the A-ALG. Once the handshake is completed, the A-ALG regards the TLS connection as being in a “suspect” state until successful register authentication of the user is completed.
2. REGISTER request is received from the UE in the access network. At the reception of REGISTER the A-ALG takes a number of actions, including
 - checking that the received registration expiration value complies with the operator-configured value and checking if a NAT is present.
3. A-ALG sends a User-Data-Request (UDR) to CLF to fetch the user's geographical location.

Registration of User in A-SBG (cont)

4. The location information is received by the A-ALG in a User-Data-Answer (UDA) from CLF and is included in further signalling towards the core network.

5. REGISTER request is sent to the P-CSCF in the core network, with modified:

- Contact: header with an expiration value set by the A-ALG
- Path: header pointing at the A-ALG.

The P-CSCF forwards the REGISTER to S-CSCF, via I-CSCF and the user is validated with HSS in the usual way. If digest authentication is required for the REGISTER request, the HSS/S-CSCF rejects the registration by sending 401 Unauthorized back to the P-CSCF, including a challenge for the UE to resolve. (not shown in the diagram). The REGISTER includes authentication parameters from the HSS.

6. P-CSCF proxies the REGISTER to A-ALG.

7. The A-ALG forwards the 401 Unauthorized response backwards to the UE. When receiving a failed registration response from P-CSCF, A-ALG removes the related information from its proxy registrar database as it does not know if UE will authenticate.

8. The user sends a new REGISTER message to the A-ALG. This time it includes a correct response to the challenge that the P-CSCF has sent to it in the 401 response.

9. The A-ALG sends a new request to fetch the user's geographical location to the CLF.

10. The location information is received by the A-ALG from the CLF.

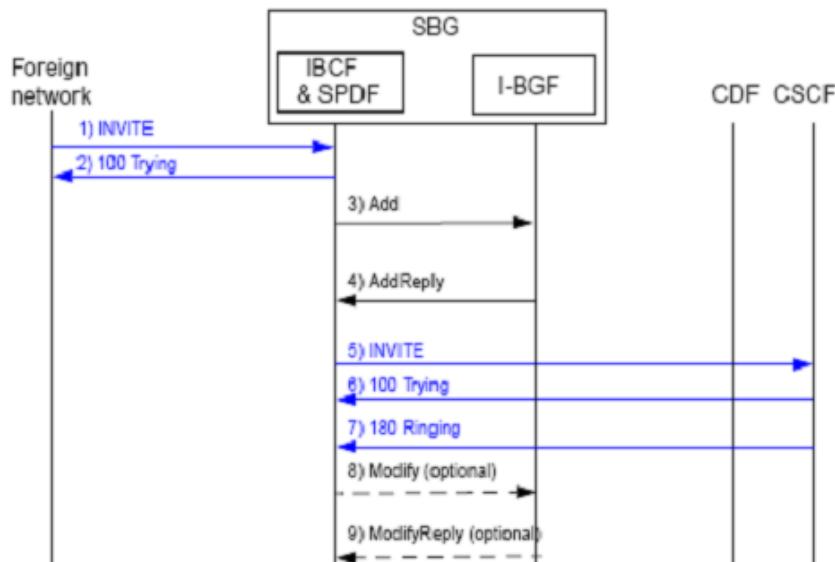
11. The A-ALG forwards the new REGISTER message to the P-CSCF the same way as it forwarded the first REGISTER message.

The S-CSCF verifies that the new REGISTER message contains a correct response to the challenge. It authorizes the registration and sends a 200 OK (REGISTER) back to the P-CSCF.

12. P-CSCF proxies the REGISTER back to A-ALG.

13. The A-ALG stores the successful user registration information to the proxy registrar data base and forwards the 200 OK (REGISTER) to the UE. The expiry timer in the forwarded message is set to indicate how often the A-ALG requires the UE to re-register itself with the A-ALG. On receipt of the 200 OK (REGISTER) response, the A-ALG regards the TLS connection as being "persistent". The TLS connection remains open for the duration of the registration lifetime.

Session Establishment in N-SBG

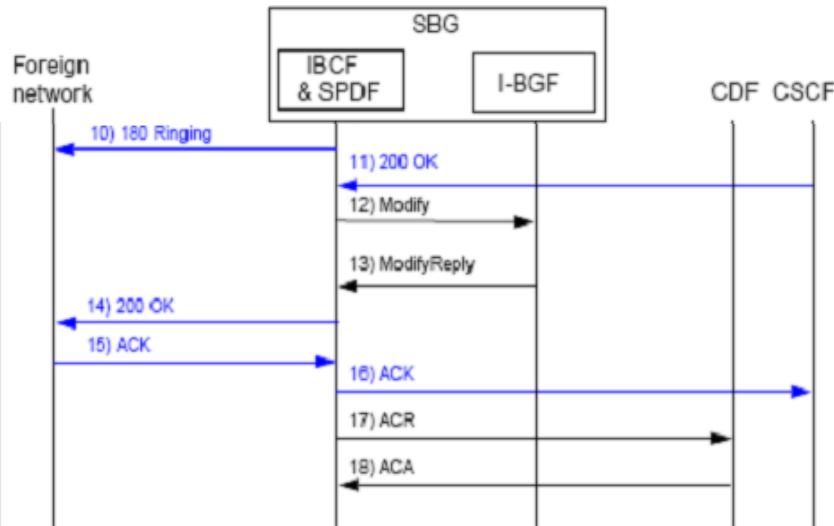


Session Establishment in N-SBG

The following steps are taken during session establishment. This example is for an incoming call from a foreign SIP network.

1. The INVITE request with SDP offer is received from the foreign network. IBCF makes an admission control to check that the configured maximum number of simultaneous SIP sessions per network is not exceeded.
2. 100 Trying is returned to indicate that the INVITE was successfully received.
3. After applying operator-configured policies to the received SDP offer, an H.248 Add request with pinhole criteria, bandwidth request, QoS settings, etc. is sent to the I-BGF in the Media Proxy. I-BGF resources are reserved. The pinhole may be opened in the backward direction, depending on a-line mode attributes in SDP offer and operator configuration of early media.
4. I-BGF sends an H.248 Add reply including allocated media addresses and ports in the I-BGF.
5. The INVITE request including updated SDP offer is sent to the core network.
6. At the reception of 100 Trying the IBCF knows that the next hop has received the INVITE request.
7. 180 Ringing is received from the core network. SDP answer may be included.
8. If SDP answer is received in 180 Ringing, the SPDF applies operator policies and checks that the SDP answer is consistent with the SDP offer. The pinhole criteria and possibly bandwidth request are updated with an H.248 Modify request if the 180 Ringing contained an SDP answer.
9. H.248 Modify reply acknowledges the changes.

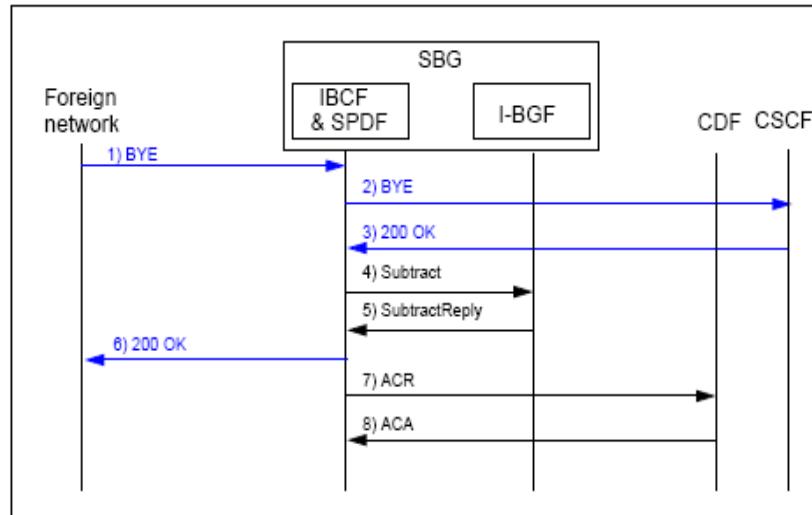
Session Establishment in N-SBG



Session Establishment in N-SBG (cont)

10. 180 Ringing is sent to the foreign network. The modified SDP answer is included if received from core network.
11. 200 OK (INVITE) with SDP answer is received from the core network to indicate that the session has been successfully established.
12. H.248 Modify request is sent to open the media pinhole in both directions (or according to negotiated SDP) and optionally update other pinhole criteria.
13. H.248 Modify reply confirms the updates.
14. 200 OK (INVITE) with modified SDP answer is sent to the foreign network.
15. ACK message received from the foreign network.
16. ACK is sent to the core network. The session setup is now concluded.
17. Diameter Accounting-Request (ACR) is sent to CDF to initiate start of charging.
18. CDF returns Diameter Accounting-Answer (ACA) when charging has been initiated by CDF.

Session Termination in N-SBG

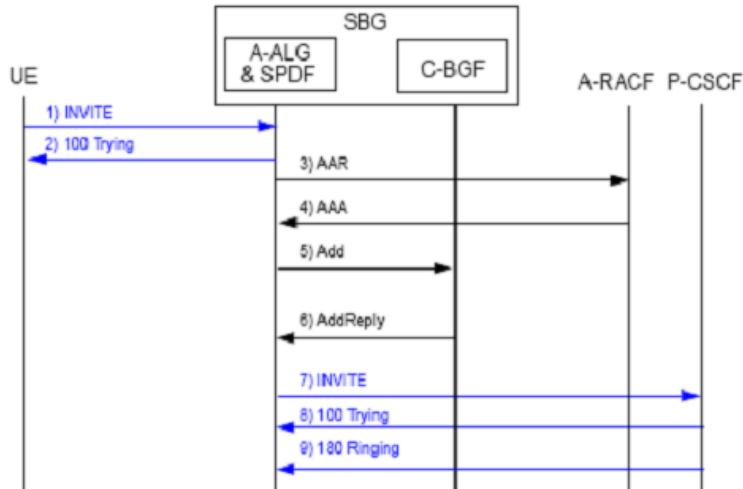


Session Termination in N-SBG

The following steps are taken during session termination.

1. A BYE request is received from the foreign network.
2. A BYE request is sent to the core network.
3. A 200 OK (BYE) message is received from the core network.
4. An H.248 Subtract request is sent to close the media pinhole, release all reserved resources in the I-BGF, and request media plane statistics.
5. An H.248 Subtract reply confirms the release and reports requested statistics.
6. A 200 OK (BYE) message is sent to the foreign network.
7. A Diameter Accounting-Request (ACR) is sent to CDF to stop charging and report charging data, including media plane statistics per operator configuration.
8. CDF returns Diameter Accounting-Answer (ACA) to confirm the reception of ACR.

Session Establishment in A-SBG

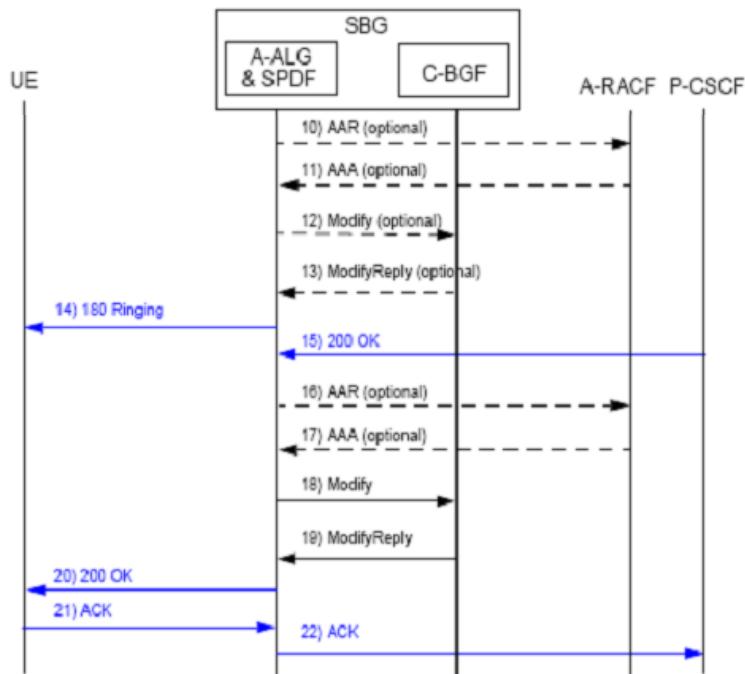


Session Establishment in A-SBG

The following steps are taken during session establishment. The example is for an incoming call from an IMS user in the Access network.

1. An INVITE request with SDP offer is received from the access network. A-ALG performs an admission control to check that the configured maximum number of simultaneous SIP sessions per network is not exceeded. A-ALG also checks that request is received from a registered user.
2. 100 Trying is returned to indicate that the INVITE was successfully received.
3. After applying operator-configured policies to the received SDP offer, an external admission control request is sent from SPDF in a Diameter AA-Request (AAR) command to the A-RACF to reserve bandwidth resources in the access network to the user.
4. The external admission control answer (success) is received by SPDF from the A-RACF, in a Diameter AA-Answer (AAA) command.
5. An H.248 Add request with pinhole criteria, bandwidth request, QoS settings etc. is sent to the C-BGF. C-BGF resources are reserved. The pinhole may be opened in the backward direction, depending on a-line mode attributes in the SDP offer and operator configuration of early media. Latching is also requested if a pinhole is opened for early media and the user is behind a NAT/FW.
6. H.248 Add reply including allocated media addresses and ports in the C-BGF.
7. An INVITE request including updated SDP offer is sent to the called SIP network.
8. At reception of 100 Trying the A-ALG knows that the next hop has received the INVITE request.
9. 180 Ringing is received from the called SIP network. SDP answer may be included.

Session Establishment in A-SBG



10. If SDP answer is received, the SPDF applies operator policies and checks that the SDP answer is consistent with the SDP offer. The SPDF may make an additional external bandwidth request, depending on the previous reservation and the SDP answer (this is typically not needed for VoIP sessions).

11. The A-RACF acknowledges the bandwidth request.

12. The pinhole criteria and possibly bandwidth request are updated with an H.248 Modify request if the 180 Ringing contained an SDP answer. Latching may also be activated.

13. An H.248 Modify reply acknowledges the changes.

14. 180 Ringing is sent to the user. The modified SDP answer is included if received from core network.

15. 200 OK (INVITE) with SDP answer is received from the called network to indicate that the session has been successfully established.

16. The SPDF may update the external bandwidth reservation if needed.

17. Acknowledgment of updated bandwidth reservation.

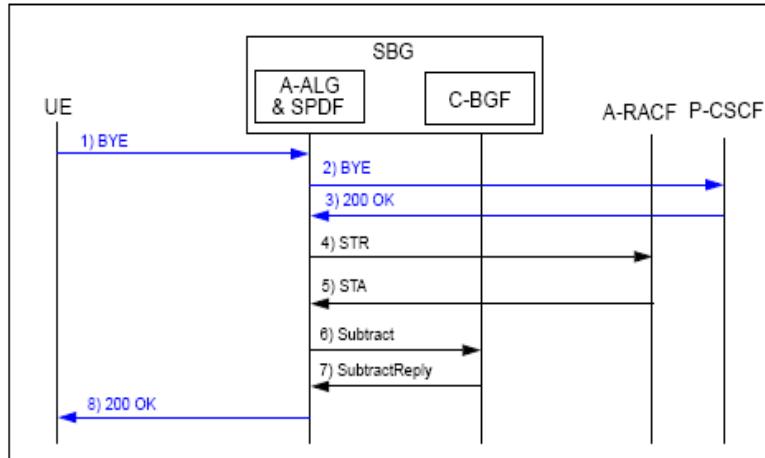
18. An H.248 Modify request is sent to open the media pinhole in both directions (or according to negotiated SDP) and optionally update other pinhole criteria. Latching may also be activated if the user is behind a NAT/FW and latching was not already ordered.

19. An H.248 Modify reply confirms the updates.

20. ACK message received from the user.

21. ACK is sent to the core network. The session setup is now concluded.

Session Termination in A-SBG



Session Termination in A-SBG

The following steps are taken during session establishment.

1. A BYE request is received from the access network.
2. A BYE request is sent to the core network.
3. A 200 OK (BYE) is received from the core network.
4. The SPDF sends a Session-Termination-Request (STR) to the A-RACF to release the reserved access network bandwidth.
5. The A-RACF acknowledges the bandwidth release with a Session-Termination-Answer (STA).
6. An H.248 Subtract request is sent to close the media pinhole, release all reserved resources in the C-BGF, and request media plane statistics.
7. An H.248 Subtract reply confirms the release and reports requested statistics.
8. 200 OK (BYE) message is sent to the UE.

Exercise 7

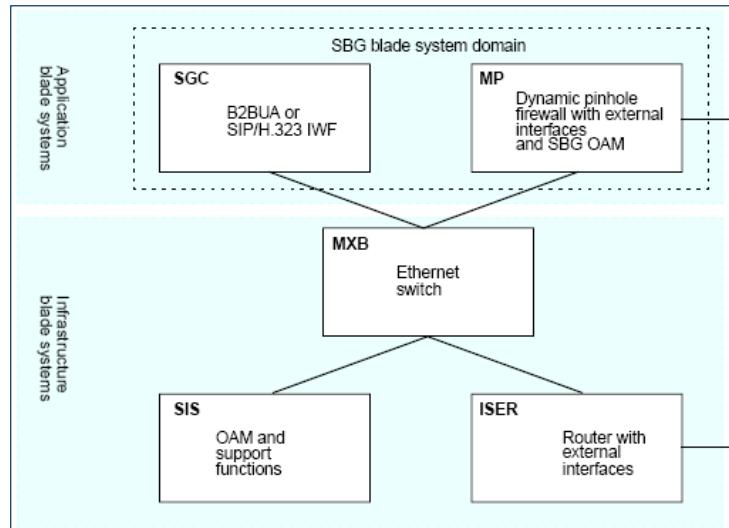
SBG 3.1 Operation and Configuration for IMS

SBG Installation

This section gives a brief overview of the installation of an SBG.

It is for information only, full details are included in the Integrated Site O&C Course.

SBG within IS Infrastructure



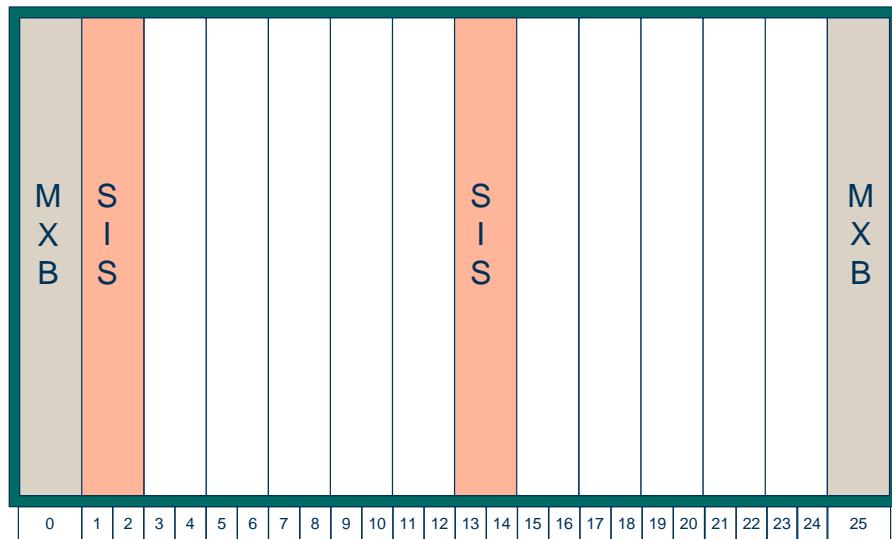
The figure above shows the SBG within the IS framework. SIS, MXB and ISER are part of IS infrastructure and should be handled as a normal IS infrastructure.

To install the SBG, the SGC and MP application blade systems are needed. Initially, the OMMP blade system must be installed, since the SBG O&M must be installed first.

Next, the SGC blade system is installed and then the expansion blade systems. The extension blade systems can be additional SGC blade systems or the MP blade systems.

For the SBG 3.1 installation, it is possible to choose between media using the ISER interface or directly using the MP external interface.

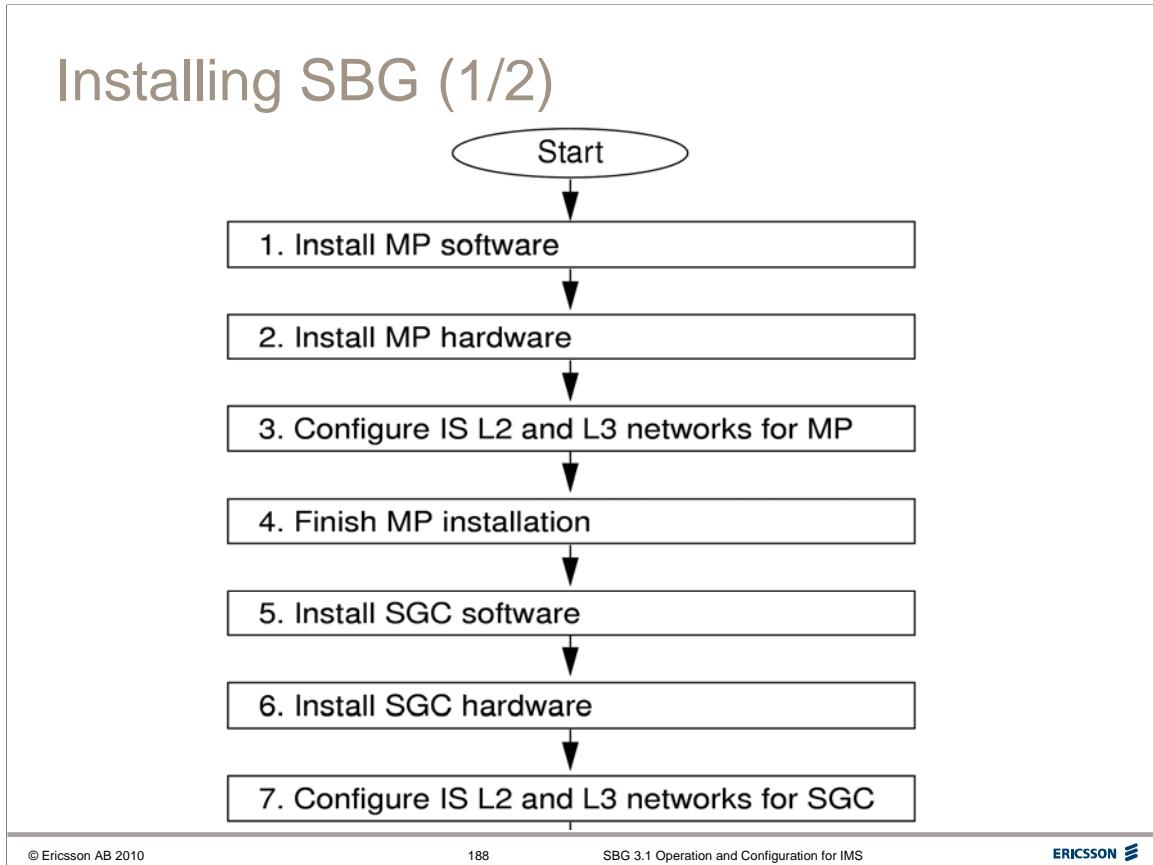
Base IS Infrastructure



The typical installation procedure is described in overview level on the following pages. Before starting with the SBG installation, the base IS should already been installed.

The figure above shows the base IS infrastructure needed before starting with the SBG installation procedure. Therefore, it is assumed that the SIS and MXB are successfully installed prior to start of SBG installation procedure.

Note: the ISER is not included as the IS base infrastructure since it is included in the SBG installation procedure. Also the ISER is not a mandatory blade for the IS.

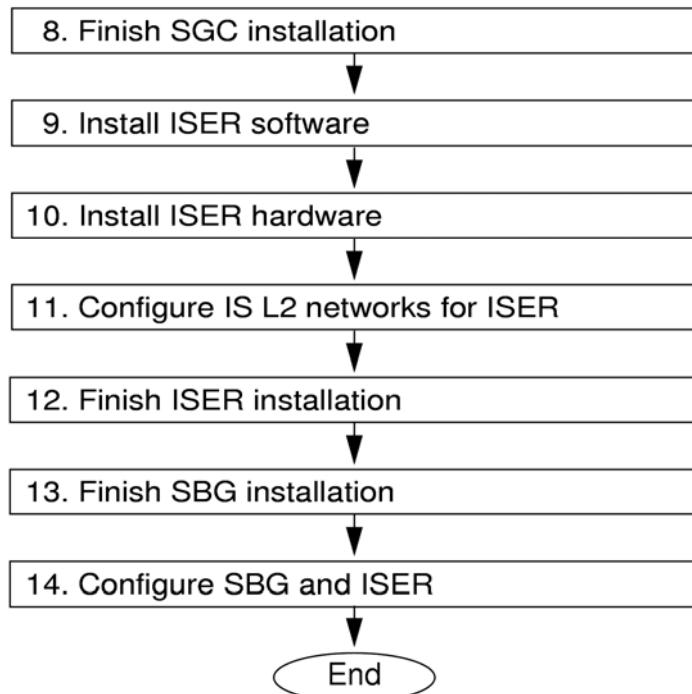


SBG initial installation and configuration

Note: This course describes installation in overview level only since the knowledge of blade system installation should already been acquired in the prerequisite course. The Configuration is also covering the SBG configuration with some configuration guidelines for the ISER. The actual configuration of ISER should also been acquired in the prerequisite course.

1. Install the MP software – downloading MP software from FTP site into IS
2. Install the MP hardware – installing the MP hardware into the designated slots positions.
3. Configure IS layer 2 (VLANs) and layer 3 (IP connectivity) networks for the MP – Configurations of IS VLAN, IP connectivity and traffic classes.
4. Finish MP installation – Unlocking the MP blade system
5. Install the SGC software – downloading SGC software from FTP site into IS
6. Install the SGC hardware – installing the SGC hardware into the designated slots positions
7. Configure IS layer 2 (VLANs) and layer 3 (IP connectivity) networks for the SGC – Configuration of IS VLAN, IP connectivity and traffic classes.

Installing SBG (2/2)

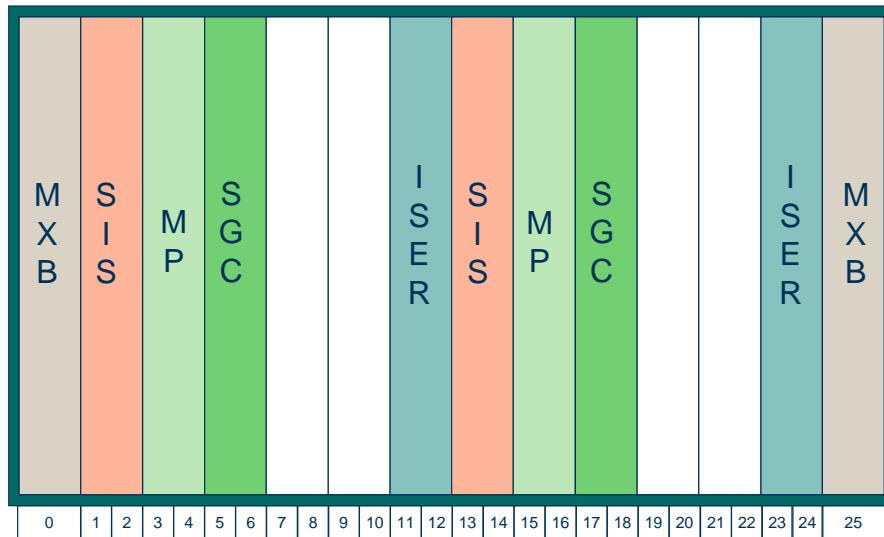


8. Finish SGC installation – Unlocking the SGC blade system
9. Install the ISER software – Downloading the ISER software from the FTP site into the IS
10. Install the ISER hardware – Installing the ISER hardware into the designated slots positions
11. Configure IS layer 2 (VLANs) networks for the ISER – Configure the IS VLAN
12. Finish ISER installation – Unlocking the ISER blade system
13. Finish the SBG installation – Checking the status of the installed MP and SGC blade system and their control link (H.248) status.
14. Configure the SBG and ISER – Configure the SBG and ISER with the related network configuration

At the end of the installation procedure, the SBG should be looking like the figure on the next page.

Note: L2 and L3 configuration is described more in “Configuring the IS Internal Network”

Minimal SBG - 1xMP BS + 1xSGC BS



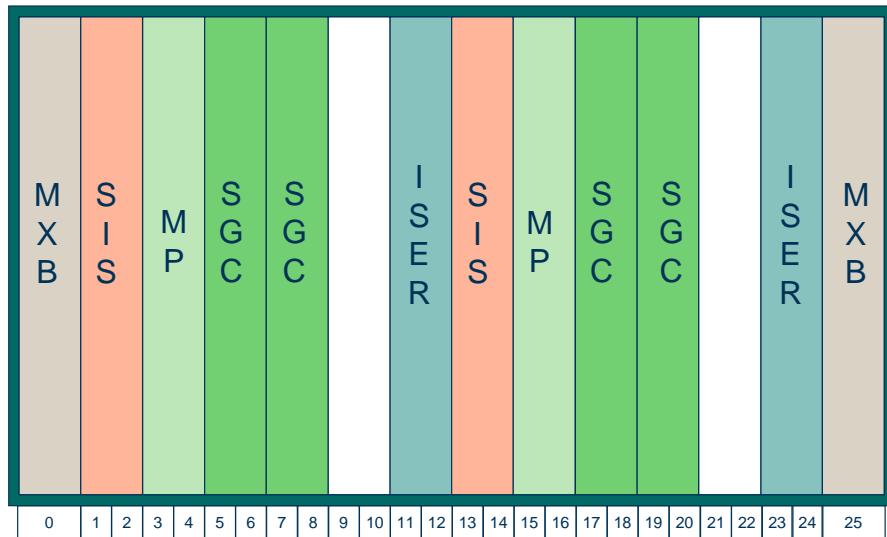
Minimal SBG

This is minimal SBG configuration with only 1 MP blade system and SGC blade system. Note that the SBG implementation always uses 1+1 redundancy for all blade systems. This means that although the actual number of blades is 2 MP blades and 2 SGC blades, the blade systems are 1 SGC blade system and 1 MP blade system.

Note that no specific SBG type is configured yet (i.e.. A-SBG or N-SBG). This is because the Access Session Border Gateway (A-SBG) or Network Session Border Gateway (N-SBG) can be configured by configuring the A-ALG for A-SBG and IBCF for N-SBG during SBG configuration related to network.

There is no specific configuration to the MP blade system during the installation phase.

Extended SBG - 1xMP BS + 2xSGC BS

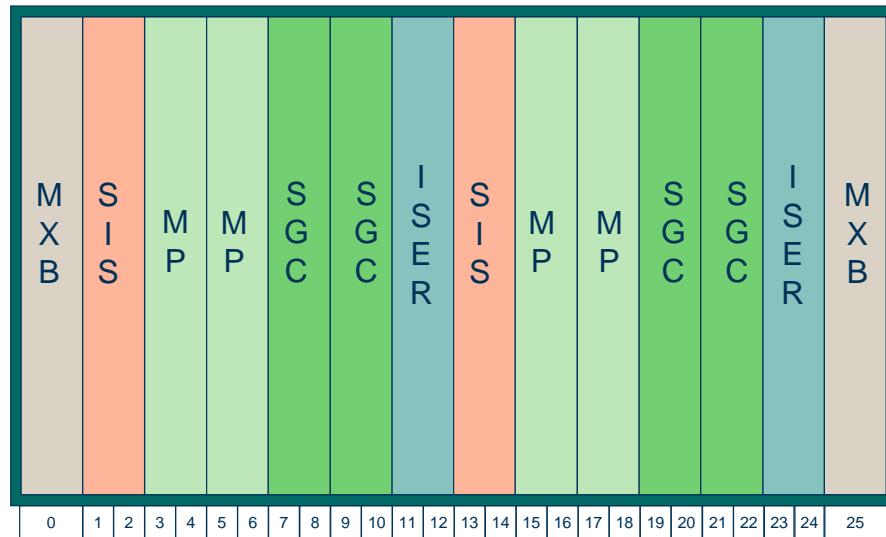


Extended SBG (1 MP + 2 SGC)

The figure above shows the extended SBG with 2 SGC blade system. As described on the previous page, the role of the SBG also depends on the SGC role configured. The figure above can be an A-SBG or N-SBG with 2 SGC blade systems and 1 MP blade system.

This configuration will give the SBG more signalling handling capacity and for the A-SBG more users can be registered to the registrar function of the A-SBG.

SBG with 2 MP + 2 SGC



Extended SBG (2 MP + 2 SGC)

The MP blade system can also be extended. The figure above shows SBG configuration with 2 MP blade systems and 2 SGC blade systems.

The reason for having 2 MP blade systems is when the operator requires more media handling with higher bandwidth streams.

One MP Blade system will be the OMMP BS and handle OAM.

Extended SBG (more than 1 subrack)

The figure above shows an SBG configuration with 2 MP blade systems and 2 SGC blade systems within 1 subrack. SBG 3.1 is based on IS 1.2, having the possibility to extend the IS up to 3 subracks. To have such configuration, the subrack cannot be configured fully as the diagram above since additional blade called Inter-Subrack Link Blade (ISLB) is needed to interconnect the IS backplane to the other subrack.

The extended subracks will only have MXB, MP and SGC blade systems (refer to diagram on page 66).

SBG 3.1 Operation and Configuration for IMS

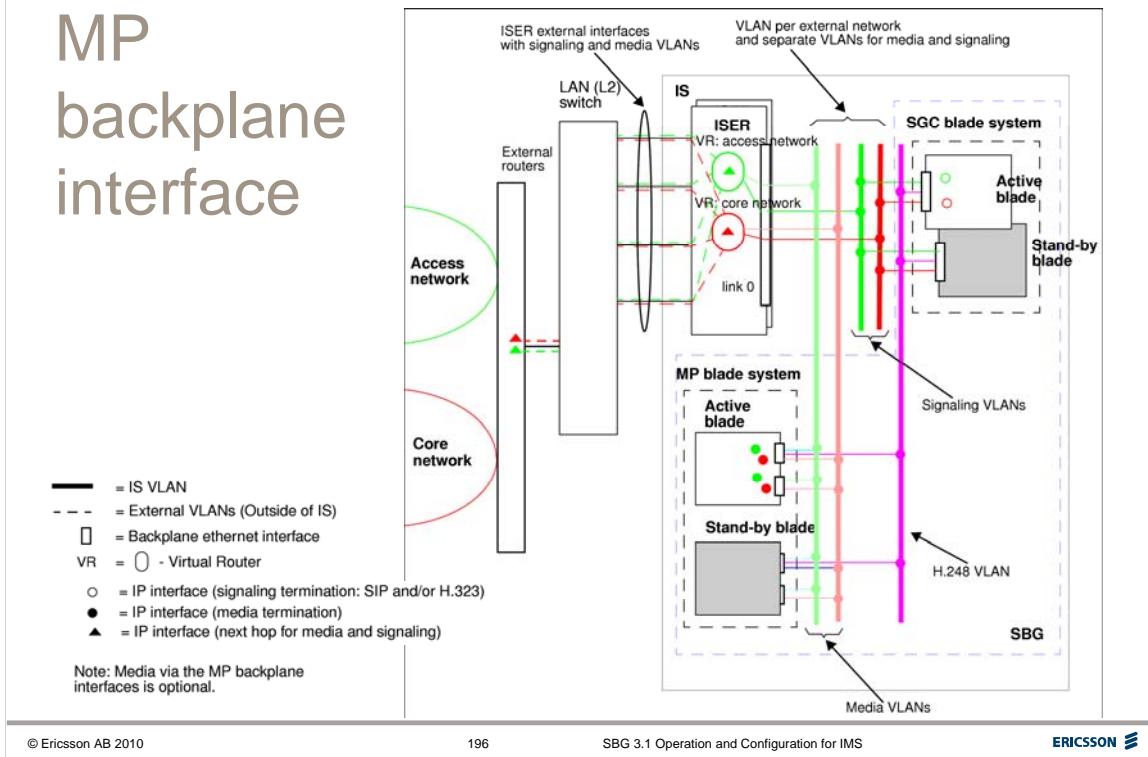
SBG Configuration



SBG 3.1 Operation and Configuration for IMS

VLAN Configuration

VLAN configuration for media via MP backplane interface



© Ericsson AB 2010

196

SBG 3.1 Operation and Configuration for IMS

ERICSSON

VLAN configuration for media via MP backplane interface

The figure above gives an example of the VLAN configuration for an A-SBG with one MP blade system and one SGC blade system. In this example the media is sent and received from/to the MP backplane interfaces via the ISER.

In this configuration the following VLANs are needed within IS:

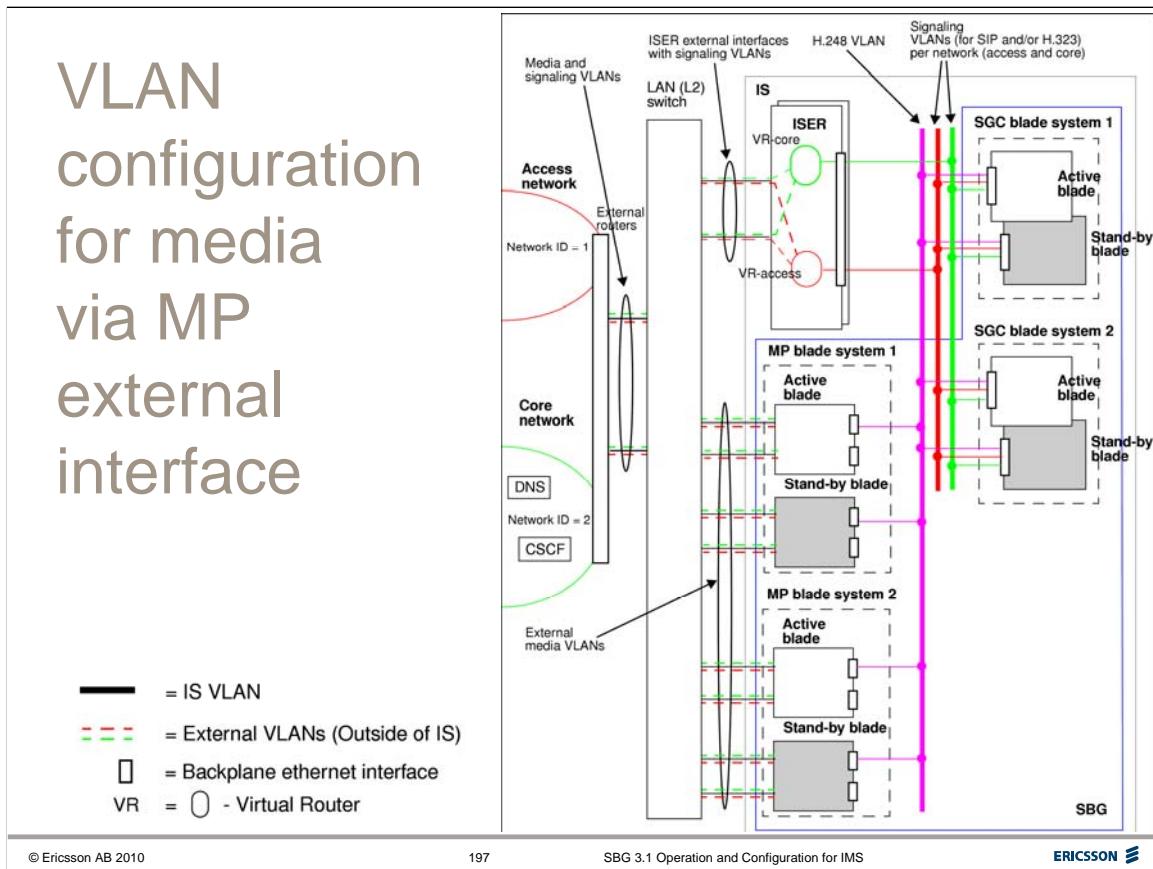
- one or two IS VLANs per network is required for signalling and media. In this example four VLANs are used (two for the access network and two for the core network), which means that signalling and media use separate IS VLANs. Each of the IS VLANs is normally connected to a separate external VLAN via a Virtual Router in the ISER.
- one IS VLAN for the H.248 signalling between the SGC blade system and the MP blade system
- one IS VLAN per SGC blade system for internal communication (not shown).
- one IS VLAN per MP blade system for internal communication (not shown).

In addition, VLANs are also used outside of IS to provide separation of data for the external networks (for example access and core). The Figure above shows that both the ISERs use two VLANs towards an external LAN (L2) switch:

- one or two external VLANs per network

Normally the same external VLAN is used for signalling and media towards a particular network, but separate VLANs for media and signalling may be configured if required.

VLAN configuration for media via MP external interface



VLAN configuration for media via MP external interface

The Figure above shows an example of the VLAN configuration for an A-SBG with two MP blade systems and two SGC blade systems. In this example the media is sent and received from/to the MP external interfaces and so does not have to pass the ISER.

In this configuration the following VLANs are needed within IS:

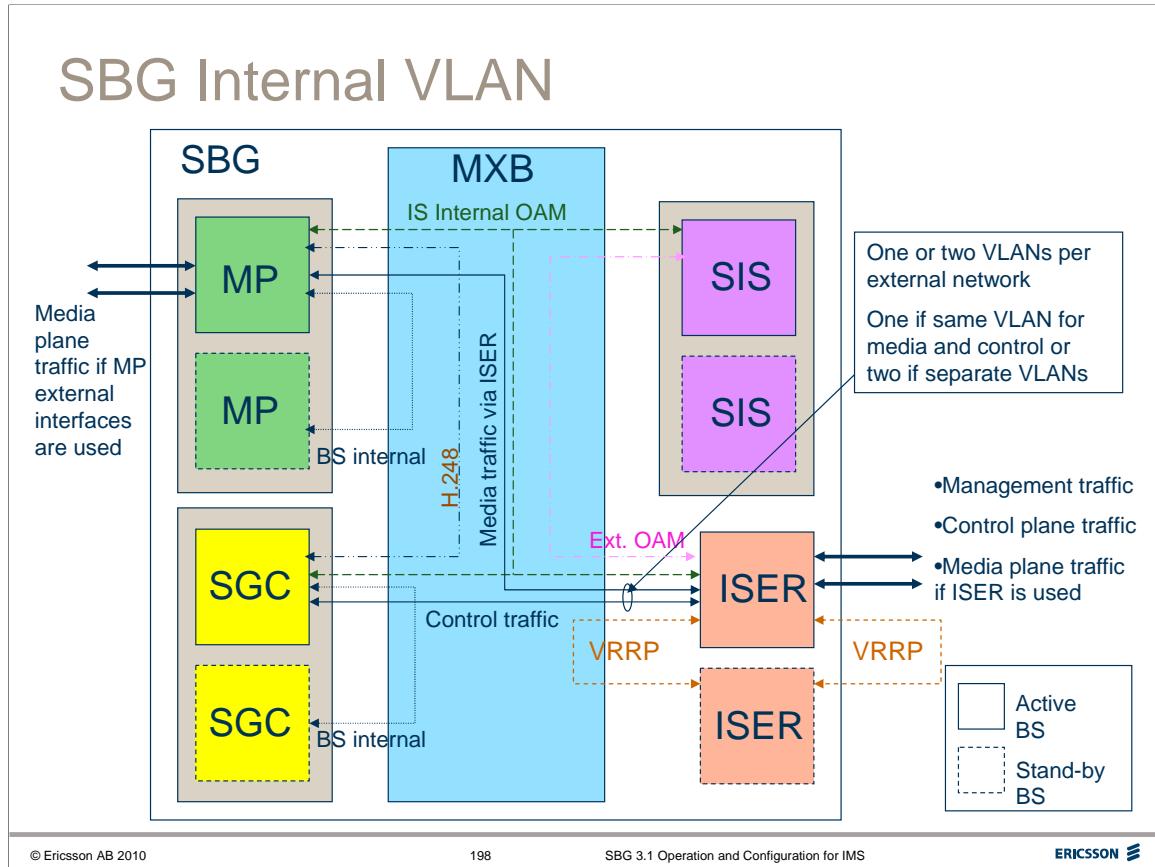
- one IS VLAN per network (in this example, access and core) is required for signalling. That is, in this example two VLANs. Each of the IS VLANs is connected to a separate external VLAN via a Virtual router in the ISER.
- one IS VLAN for the H.248 signalling between the SGC blade systems and the MP blade systems
- one IS VLAN per SGC blade system for internal communication (not shown).
- one IS VLAN per MP blade system for internal communication (not shown).

In addition, VLANs are also used outside of IS to provide separation of data for the external networks (for example access and core). *Figure above* shows that both the ISER and the MP blade system use VLANs for signalling (ISER) and VLANs for media (MP) towards an external LAN (L2) switch:

- one or two external VLANs per network

Normally the same external VLAN is used for signalling and media towards a particular network, but separate VLANs for media and signalling may be configured if required.

Note: In this configuration, signalling to/from different networks must use different VLANs within IS. Outside of IS, signalling to several networks may share VLAN. For media, different VLANs have to be used for different networks.



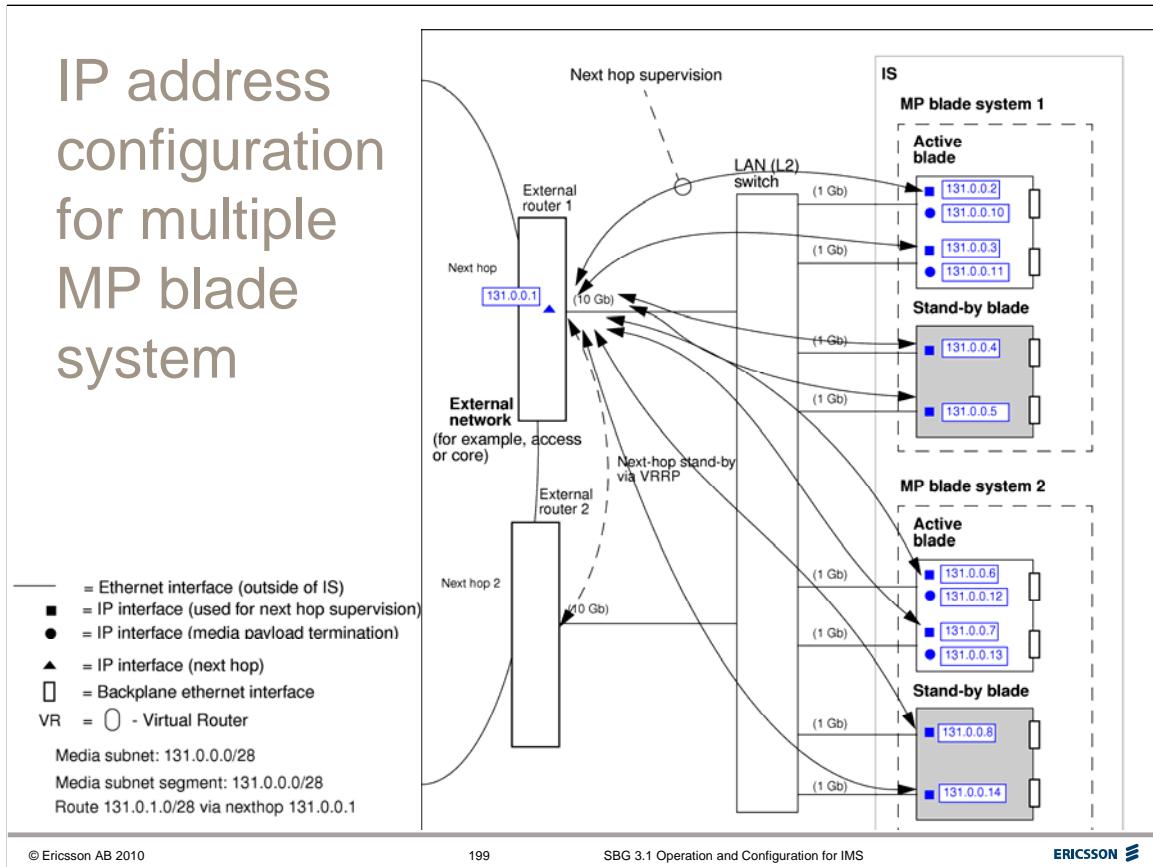
SBG Internal VLAN

The figure above shows in the SBG internal VLANs not shown in the two earlier examples. The internal VLANs are:

- IS Internal OAM
- BS internal for MP
- BS internal for SGC
- External OAM

The figure above also shows the 2 possibilities of the media paths.

- The thick lines/arrows from the MP show media connected via MP external interfaces
- The thick lines/arrows from the ISER show media connected via MP internal interfaces



IP address configuration for multiple MP blade system

When the SBG is extended with another MP, more bandwidth capacity is needed at the external routers. If the configuration with 1 Gb interfaces at the external routers are used, two more 1 Gb interfaces have to be configured at each external router, or, alternatively 10 Gb interfaces can be used at the external routers.

In this example VRRP is assumed at the external routers. Since the routers have 10 Gb interfaces only one subnet and subnet segment is needed for the media transport. In this case the subnet and the subnet segment have the same address and mask 131.0.0.0/28.

One Next hop is needed with one next hop addresses: 131.0.0.1.

As in the earlier examples, one Static Route for media is needed per destination subnet.

The IP interfaces needed are also similar as in the earlier examples; one IP interface for next hop supervision is needed per MP blade and Ethernet interface and one IP interface for media payload termination is needed per MP blade system and Ethernet interface (the payload termination interfaces are moved between the MP blades when the stand-by blade takes over the media traffic).

The subnet address and mask used in the external routers towards the LAN (L2) switch is the same as the subnet address and mask used in the MPs, that is, 131.0.0.0/28.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Network Configuration

For full details of the Network Configuration, refer to the Network Configuration Service Guide, 4/154 43-CNA 113 062

SBG Configuration Options

- A-SBG (A-ALG)
- A-SBG (A-ALG) + P-CSCF
- N-SBG (IBCF)

- **Media Proxy**
 - Internal (Same IS)
 - Internal IP Interfaces (via ISER)
 - External IP Interfaces
 - External

An SBG can be configured for a number of different network scenarios:

SBG Configuration Options

- As an A-SBG connected to one or more access networks and one core network (for example, an IMS core network). Here each access network uses SIP signaling and/or H.323 signaling towards the SBG. The IMS core network uses SIP signaling towards the SBG. The A-SBG can operate either as an A-ALG (Access Application Level Gateway) or as a P-CSCF (Proxy Call Session Control Function).
- As an N-SBG connected to one core network and one or more foreign networks, where each foreign network uses either SIP or H.323 for signaling. The SGC in the N-SBG operates as an IBCF.
- As a combined A-SBG + N SBG

Media Proxy Configuration Options

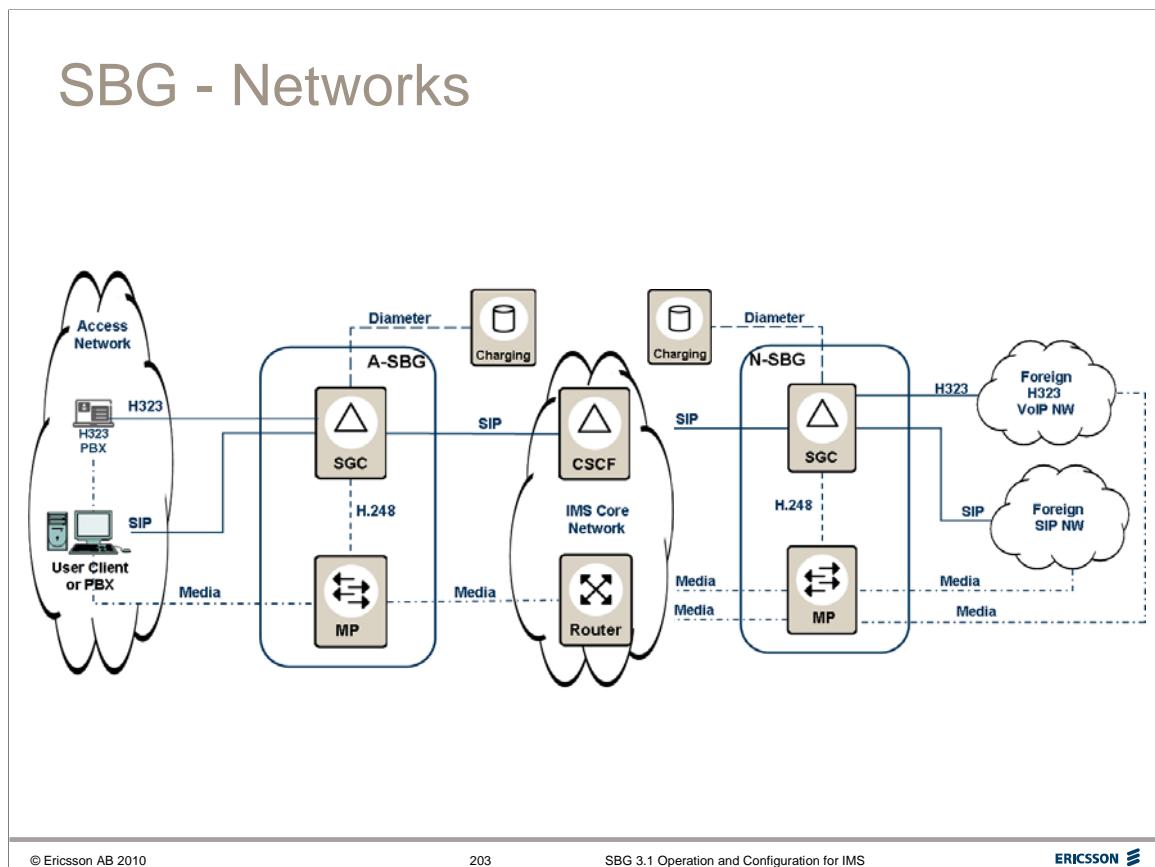
For media, the SBG can be configured to use:

- Internal (same IS) Media Proxies (MPs)
- external Border Gateway Functions (BGFs)
- both external BGFs and internal MPs
- a transcoding function to provide transcoding services (trial only)

Media Options

For MPs there are two possible configurations for Media:

- Media is sent via the MP external interfaces.
- Media is sent via the MP backplane interfaces.



Network Configuration

Configuration of the Networks is performed from

Session Border Gateway → Network Configuration

See the figure above. From here there are links to view/configure

Networks

The Signalling Networks, Media Networks & External BGF Networks are configured here (IP Addresses, Next hops, Supervision settings etc.) for Access, Core and Foreign Networks.

Domains

Configure the domains connected to the SBG

Next Hop Groups

Next Hops for Media can be grouped together to avoid excessive next hop ARP supervision from one MP blade system towards the external routers. Next Hops that are used to reach a specific router Ethernet interface, and that belong to different networks, should be configured to belong to the same **Next Hop Group**.

Next Hop Groups are used when the SBG is connected to more than two networks and when the front (external) interfaces on the MP are used for media transport.

Address to network mapping

The IP **address-to-network mapping** table is used to enable routing of SIP messages from the IMS core network towards a foreign SIP or H.323 network. This table is used when the SBG acts as an N-SBG implementing the IBCF function.

SBG Network Configuration-Networks

SBG - Network Configuration

Networks

	Network name	Network ID	Network type	MPs used for media	BGF status	Codec policy profile	Delete
 Change all rows	Access	2	access	yes	available	0	<input type="checkbox"/>
 Create network	Core	1	core	yes	available	0	<input type="checkbox"/>

[Table as text](#)

[Create network](#)
[Create next hop group](#)
[Open faulty next hops](#)
[Open next hop groups](#)

SBG Network Configuration

For the SBG it is necessary to configure each of the networks that the SBG is connected to (Access, Core and Foreign, as required).

The networks configured here are used by both the SGC blade systems and by the MP blade systems.

In the figure above, one Access Network with network ID 2 and one Core Network with network ID 1 are shown. The network IDs are assigned by the system when creating the network. This identity will be used as a part of the termination identity sent over H.248 from the SGC to the MP at call setup.

A network must be created before it is possible to create any IP Interfaces, Next Hops, Static Routes or Signalling Network Connections, since these Managed Objects are created and maintained per network.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Access Signalling Network

ERICSSON 

For full details of the Network Configuration, refer to the Network Configuration Service Guide, 4/154 43-CNA 113 062

Network Configuration - Access Network 1

SBG - Network Configuration

Network

Network name:	Access
Network ID:	2
Network type:	access
MPs used for media:	<input checked="" type="radio"/> yes <input type="radio"/> no
BGF status:	available
Codec policy profile:	[0]

[Modify network name](#)

Session Gateway Controller

Signaling Network Connections

Blade system	Next hop address	Network type	Policing	RTCP port allocation
▶ SGC 0-5_17	192.168.3.65	access	off	off

[Table as text](#)

© Ericsson AB 2010 208 SBG 3.1 Operation and Configuration for IMS ERICSSON

SBG Signalling Network Connections - Access

In the *Network Configuration* → *Networks* page, select an **Access Network** and the configuration related to Media and Signalling in that network will be displayed, as can be seen above. From this view, the following main attributes can be seen:

Network name & Network Id & Network type

MPs used for media – If ‘yes’ all MPs (internal and external) are used for media, if ‘no’ only external BGFs are used for media.

BGF Status – ‘available’: At least one MP or external BGF is available for media transport. The control links are unlocked and operational.

Codec policy profile - Trial only.

Session Gateway Controller

The defined SGC Signalling Network Connections are shown, with links to Create and Delete signalling network connections.

For existing connections the table shows:

Blade System – Blade System Id

Next hop address - The IP address of the router via which SIP and/or H.323 signalling is sent and received.

Policing - Indicates whether bandwidth policing shall be applied for the media streams for incoming packets from the associated network.

RTCP port allocation - Indicates how RTCP ports will be handled for media streams to and from the associated network.

Network Configuration – Access Network 2

SBG - Network Configuration

Network

ERICSSON

[Create signaling network connection](#)
[Delete signaling network connection](#)

Media Proxy
[Network configuration](#)

Control links

	Blade system	Link ID	Control link available	Operational state
	SGC 0-5_17	bs_SBG_4/1	available	enabled

[Table as text](#)

External BGF
Control links

	Blade system	Link ID	Control link available	Operational state
--	--------------	---------	------------------------	-------------------

[Table as text](#)

[Networks](#)

© Ericsson AB 2010 209 SBG 3.1 Operation and Configuration for IMS ERICSSON

Media Proxy

The table shows:

The **SGC blade system(s)** terminating H248 control links and the link Id.

Control Link Availability (Indicates if links are blocked)

Operational state (Indicates if the control links are available for media stream setup.).

Clicking the **red triangle** next to the Media Proxy Blade System opens the “MP Control Link” page where the status of the H248 links can be viewed, together with details of IP addresses. This is shown in the figure two pages ahead.

Network Configuration – this link opens the **MP Network Configuration** page for configuration of the Media Network – IP Interfaces, Static Routes, Next Hops. This is described in detail in the following pages.

External BGF

If an External BGF is defined, control link details will be seen here.

Clicking the red triangle next to the Session Gateway Controller Blade System opens the “Signalling Network Connection” page where many signalling network parameters can be viewed/set. This is shown on the following page.

Signalling Network – Access Signalling

SBG - Network Configuration
Signaling Network Connection

Network name: Access Network ID: 2 Network type: access Blade system: SGC 0-5_17	Signaling <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"> Next hop address: 192.168.3.65 Subnet address: 192.168.3.64 Subnet mask length: 27 VLAN ID: 1220 Blocking policy: <input type="radio"/> on <input checked="" type="radio"/> off Blocking time (s): <input type="text" value="120"/> Rate limit (pkts/s): <input type="text" value="30"/> Inter-operator identifier: <input type="text"/> </td> <td style="width: 50%;"> Maximum sessions: <input type="text" value="0"/> Trusted for privacy information: <input type="radio"/> False <input checked="" type="radio"/> True Cable or mobile access: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Access network domain name: <input type="text"/> Default location: <input type="text" value="EricssonEducation.net"/> Send default location at emergency: <input checked="" type="radio"/> True <input type="radio"/> False e2 query mode: <input checked="" type="radio"/> Ericsson <input type="radio"/> Standard Phone context: <input type="text"/> Extended SIP-URI number check: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled NASS realm (e2): <input type="text" value="- Not selected -"/> RACS realm (Rq): <input type="text" value="- Not selected -"/> </td> </tr> </table>	Next hop address: 192.168.3.65 Subnet address: 192.168.3.64 Subnet mask length: 27 VLAN ID: 1220 Blocking policy: <input type="radio"/> on <input checked="" type="radio"/> off Blocking time (s): <input type="text" value="120"/> Rate limit (pkts/s): <input type="text" value="30"/> Inter-operator identifier: <input type="text"/>	Maximum sessions: <input type="text" value="0"/> Trusted for privacy information: <input type="radio"/> False <input checked="" type="radio"/> True Cable or mobile access: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Access network domain name: <input type="text"/> Default location: <input type="text" value="EricssonEducation.net"/> Send default location at emergency: <input checked="" type="radio"/> True <input type="radio"/> False e2 query mode: <input checked="" type="radio"/> Ericsson <input type="radio"/> Standard Phone context: <input type="text"/> Extended SIP-URI number check: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled NASS realm (e2): <input type="text" value="- Not selected -"/> RACS realm (Rq): <input type="text" value="- Not selected -"/>
Next hop address: 192.168.3.65 Subnet address: 192.168.3.64 Subnet mask length: 27 VLAN ID: 1220 Blocking policy: <input type="radio"/> on <input checked="" type="radio"/> off Blocking time (s): <input type="text" value="120"/> Rate limit (pkts/s): <input type="text" value="30"/> Inter-operator identifier: <input type="text"/>	Maximum sessions: <input type="text" value="0"/> Trusted for privacy information: <input type="radio"/> False <input checked="" type="radio"/> True Cable or mobile access: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Access network domain name: <input type="text"/> Default location: <input type="text" value="EricssonEducation.net"/> Send default location at emergency: <input checked="" type="radio"/> True <input type="radio"/> False e2 query mode: <input checked="" type="radio"/> Ericsson <input type="radio"/> Standard Phone context: <input type="text"/> Extended SIP-URI number check: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled NASS realm (e2): <input type="text" value="- Not selected -"/> RACS realm (Rq): <input type="text" value="- Not selected -"/>		

© Ericsson AB 2010 210 SBG 3.1 Operation and Configuration for IMS ERICSSON

When opening the signalling network connection, more configuration parameters can be seen.

The main parameters not described in previous page are:

Blocking policy - Indicates whether excessive signalling from a specific user shall be blocked or not. Only applicable for access network type.

Blocking time (s) - Indicates for how long time the signalling from a specific user will be blocked in the event of excessive signalling

Rate limit (pkts/s) - The maximum allowed signalling rate that is allowed from a user or a network node to the SGC. Excessive traffic will be dropped when the rate limit is exceeded. If the Blocking policy is on, signalling traffic may also be blocked for a period of time specified by the Blocking time when the rate limit is exceeded

Inter-operator identifier - The inter-operator identifier (ioi) is used to specify the name of the network operator associated with the signalling network connection of an N-SBG

Maximum sessions - the maximum number of sessions that are allowed to be active for the network connection. Used to limit the number of sessions initiated by INVITE. Setting the attribute to 0 means that no limit will be imposed on the number of sessions.

Trusted for privacy information -Indicates if the network is trusted for receiving privacy protected SIP header information. For SIP, this attribute controls the screening of P-Asserted-Identity (PAI) and History-Info headers when the associated headers are privacy protected. If a header is privacy protected, the header will be forwarded to the network only if the network is trusted for privacy. See reference document for more details.

Cable access and mobile user additions - Specify if cable access and mobile users will be supported for an access network or not. An “a= line” is added to the SDP forwarded to the core with local and remote IP-address on the access side for higher level authorization and policy decisions.

Default location - Specifies the geographical location of the access network

Send default location at emergency - indicates whether the value of the Default location attribute should be included in session signaling (in PANI) for emergency calls when no geographical location information for a user can be obtained from CLF.

e2 query mode - specifies which type of location information the SGC will request from CLF over e2 interface.

Signalling Network - Access Media

SBG - Network Configuration

Signaling Network Connection

Media control

Local media policy:

Policing: on off

RTCP port allocation: on off

RTCP mode:

Media source filtering without NAT: off SDP IP address SDP IP address and port SIP IP address

Media source filtering with NAT: off SIP IP address

Originating network early media support:

Terminating network early media support:

SDP address validation: True False

Always latch: True False

Media stop supervision

Supervision time (s):

On-hold supervision time (s):

Supervision direction:

DiffServ code points

DSCP for audio:

DSCP for video:

DSCP for other:

MEDIA PARAMETERS

Local media policy - Specifies whether local media transport shall be allowed or whether media must pass through the MP (media anchoring) at local calls made within a network. The attribute is only applicable for an access network.

Policing - Indicates whether bandwidth policing shall be applied for the media streams for incoming packets from the associated network. If active the maximum bandwidth used for a media stream will be dictated by the used *payload type*. If policing is applied, any excessive traffic on a media stream will be logged in the excessive media log

RTCP mode - Indicates how RTCP will be handled for media streams to and from the associated network. If RTCP is off, any incoming RTCP packets will be logged in the Malicious media log.

Media source filtering - Specifies whether IP address and port filtering shall be applied for the media received from the associated network

Early media support - Indicates whether the SBG will accept early media from the associated network for originating or terminating media.

SDP address validation - specifies whether the SGC will validate the IP addresses in the SDP against the source IP address of the SIP packet. SDP validation is never applied if the user is behind a NAT. SDP address 0.0.0.0 is always treated as valid.

SBG 3.1 Operation and Configuration for IMS

Core Signalling Network

For full details of the Network Configuration, refer to the Network Configuration Service Guide, 4/154 43-CNA 113 062

Network Configuration – Core Network 1

SBG - Network Configuration ERICSSON

Network

Network name:	Core
Network ID:	1
Network type:	core
MPs used for media:	<input checked="" type="radio"/> yes <input type="radio"/> no
BGF status:	available
Codec policy profile:	<input type="text"/>

[Modify network name](#)

Session Gateway Controller

Signaling Network Connections				
Blade system	Next hop address	Network type	Policing	RTCP port allocation
▶ SGC 0-5_17	192.168.9.121	core	on	on

[Table as text](#)

SBG Signalling Network Connections – Core Network

In the *Network Configuration → Networks* page, select the **Core Network** and the configuration related to Media and Signalling in that network will be displayed, as can be seen above.

From this page, the main network attributes can be seen, as already described for the Access Network view.

Network Configuration – Core Network 2

SBG - Network Configuration Network

ERICSSON 

[Create signaling network connection](#)
[Delete signaling network connection](#)

Media Proxy

[Network configuration](#)

Control links

Blade system	Link ID	Control link available	Operational state
▶ SGC 0-5_17	bs_SBG_4/1	available	enabled

[Table as text](#)

External BGF

Control links

Blade system	Link ID	Control link available	Operational state
--------------	---------	------------------------	-------------------

[Table as text](#)

[Networks](#)

Click ‘Network configuration’ under Media Proxy to view/configure the media network in the core.

Signalling Network – Core Signalling

SBG - Network Configuration
Signaling Network Connection

Network name: Core
Network ID: 1
Network type: core
Blade system: SGC 0-5_17

Signaling

Next hop address: 192.168.9.121
Subnet address: 192.168.9.120
Subnet mask length: 29
VLAN ID: 1200
Blocking policy: on off
Blocking time (s): 120
Rate limit (pkts/s): 8000
Inter-operator identifier:
Maximum sessions: 0

ERICSSON

Trusted for privacy information: True
Cable or mobile access: Enabled Disabled
Access network domain name: EricssonEducation; net
Default location: EricssonEducation; net
Send default location at emergency: True False
e2 query mode: Ericsson Standard
Phone context:
Extended SIP-URI number check: Enabled Disabled

© Ericsson AB 2010 216 SBG 3.1 Operation and Configuration for IMS ERICSSON

Signalling Network Connection – Core Signalling

These parameters are the same as already described for the Access Signalling configuration and will not be described again here.

Signalling Network– Core Media

SBG - Network Configuration
Signaling Network Connection

Media control	
Local media policy:	<input type="button" value="Not allowed"/>
Policing:	<input checked="" type="radio"/> on <input type="radio"/> off
RTCP port allocation:	<input checked="" type="radio"/> on <input type="radio"/> off
RTCP mode:	<input type="button" value="SendReceive"/>
Media source filtering without NAT:	<input type="radio"/> off <input type="radio"/> SDP IP address <input checked="" type="radio"/> SDP IP address and port <input type="radio"/> SIP IP address
Media source filtering with NAT:	<input type="radio"/> off <input checked="" type="radio"/> SIP IP address
Originating network early media support:	<input type="button" value="Bidirectional"/>
Terminating network early media support:	<input type="button" value="Bidirectional"/>
SDP address validation:	<input type="radio"/> True <input checked="" type="radio"/> False
Always latch:	<input type="radio"/> True <input checked="" type="radio"/> False
Media stop supervision Supervision time (s): <input type="text" value="30"/>  On-hold supervision time (s): <input type="text" value="0"/>  Supervision direction: <input type="button" value="off"/>	
DiffServ code points DSCP for audio: <input type="text" value="46"/>  DSCP for video: <input type="text" value="10"/>  DSCP for other: <input type="text" value="18"/> 	

© Ericsson AB 2010 217 SBG 3.1 Operation and Configuration for IMS ERICSSON

Signalling Network Connection – Core Media

These parameters are the same as already described for the Access Media configuration and will not be described again here.

Foreign Networks

Foreign Networks are defined in the same way as Access and Core Networks.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Creating a Network

For full details of the Network Configuration, refer to the Network Configuration Service Guide, 4/154 43-CNA 113 062

SBG Network Configuration-Networks

SBG - Network Configuration

Networks

	Network name	Network ID	Network type	MPs used for media	BGF status	Codec policy profile	Delete
 Change all rows	Access	2	access	yes	available	0	<input type="checkbox"/>
 Create network	Core	1	core	yes	available	0	<input type="checkbox"/>

[Table as text](#)

[Create network](#)
[Create next hop group](#)
[Open faulty next hops](#)
[Open next hop groups](#)

SBG Network Configuration

For the SBG it is necessary to configure the networks that the SBG is connected to (Access, Core and Foreign, as required).

The networks configured here are used by both the SGC blade systems and by the MP blade systems.

In the figure above, one Access Network with network ID 2 and one Core Network with network ID 1 are shown. The network IDs are assigned by the system when creating the network. This identity will be used as a part of the termination identity sent over H.248 from the SGC to the MP at call setup.

A network must be created before it is possible to create any IP Interfaces, Next Hops, Static Routes or Signalling Network Connections, since these Managed Objects are created and maintained per network.

Create Network

SBG - Network Configuration

Create Network

Network name:

Network type: access core foreign

MPs used for media: yes no

Codec policy profile:

Network name	Network ID	Network type	MPs used for media	BGF status	Codec policy profile
Access	2	access	yes	available	0
Core	1	core	yes	available	0

[Table as text](#)

[Create next hop group](#)
[Open faulty next hops](#)
[Open networks](#)
[Open next hop groups](#)

Create a Network

To create a network click **Create Network** in the previous figure; the page shown above opens. Enter the Network name, Network Type and whether the Internal MPs are used for Media. The new Network will appear on the list of networks on the screen shown on the previous page. The Network can now be configured.

Configuring a Network

Once the Network has been created, it can be further configured.

From the main **Network Configuration** → **Networks** page, select the network to be configured. The page shown above opens.

Create Signalling Network Connection

The **Session Gateway Controller Signalling Network Connections** can be configured by selecting the **Create Signalling Network Connection** link.

Media Proxy Network Configuration

The **Media Proxy Network Interfaces** can be configured by selecting the **Network Configuration** link.

Create Signalling Network Connection 1

SBG - Network Configuration
Create Signalling Network Connection

Network name: Foreign_network_1
Network ID: 3
Network type: Foreign
Blade system: SGC 0-5_17

Signaling

Next hop address: 192.168.9.100
Subnet mask length: 24
VLAN ID: 650
Blocking policy: on off
Blocking time (s): 120
Rate limit (pkts/s): 8000
Burst size (pkts): 8000
Differentiate on source port: True False
Inter-operator identifier: eduims.se
Maximum sessions: 0
Trusted for privacy information: True False
Cable or mobile access: Enabled Disabled
Access network domain name:
Default location:
Send default location of emergency: True False
e2 query mode: Ericsson Standard
Phone context:
Extended SIP-URI number check: Enabled Disabled

Create Signalling Network Connection 2

SBG - Network Configuration
Create Signaling Network Connection

Media control

Local media policy: on off

Policing: on off

RTCP port allocation: off SDP IP address SDP IP address and port SIP IP address

RTCP mode: SendReceive Bidirectional

Media source filtering without NAT: off SDP IP address SIP IP address and port SIP IP address

Media source filtering with NAT: off SIP IP address

Originating network early media support: Off Bidirectional

Terminating network early media support: Bidirectional Off

SDP address validation: True False

Always latch: True False

Media stop supervision

Supervision time (s):

On-hold supervision time (s):

Supervision direction: off on off

Client state check: on off

DiffServ code points

DSCP for audio:

DSCP for video:

DSCP for other:

[Create SIP network connection](#)
[Create II 323 network connection](#)
[Delete signalling network connection](#)
[Open network](#)

SBG - Network Configuration
MP Network Configuration

Network name: Foreign_network_1
Network ID: 3
Network type: Foreign

Media

Configuration information: The configuration check has not found any problems.

IP Interfaces

IP interface address	Subrack	Slot	Port	VLAN ID	Subnet mask length	Subnet segment mask length	Usage	Administrative state	Operational state
----------------------	---------	------	------	---------	--------------------	----------------------------	-------	----------------------	-------------------

[Table as text](#)

[Create IP interface](#)
[Delete IP interface](#)

Routes

Remote subnet address	Remote subnet mask length	Type
-----------------------	---------------------------	------

[Table as text](#)

[Create static route](#)
[Delete static route](#)

Next Hops

Next hop address	Next hop address 2	Supervision	Next hop group	Next hop group 2	Administrative state
------------------	--------------------	-------------	----------------	------------------	----------------------

[Table as text](#)

[Create next hop](#)
[Delete next hop](#)

Open networks
Configure bandwidth
Network statistics
Security settings

© Ericsson AB 2010

225

SBG 3.1 Operation and Configuration for IMS

ERICSSON

On the **Create Network** page there is a link to **Network Configuration** under **Media Proxy**. See the figure ‘Create Network’ three pages back.

Select this link and the page shown above opens.

It shows any Media IP Interfaces already defined; Routes for Media traffic, and Next Hops for Media.

From this page the user can create new IP Interfaces for Media; Next Hops for Media and Static Routes. This is described in detail in the section ‘Media proxy Network Configuration’.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Media Proxy Network Configuration

For full details of the Network Configuration, refer to the Network Configuration Service Guide, 4/154 43-CNA 113 062

MP Network Configuration 1

SBG - Network Configuration
MP Network Configuration

Network name: access_lab
Network ID: 1
Network type: access

Media
Configuration information: The Next Hop address 10.200.200.200 is not found in any IP segment.
The Next Hop address 10.100.100.100 is not found in any IP segment.

IP Interfaces

	IP interface address	Subrack	Slot	Port	VLAN ID	Subnet mask length	Subnet segment mask length	Usage	Administrative state	Operational state
▶	10.64.230.7	1	17	2	710	27	27	psyTerm	unlocked	enabled

[Table as text](#)

[Create IP interface](#)
[Delete IP interface](#)

Routes

Select **Network Configuration** → **Networks** and click **Media Proxy Network Configuration** to open the MP Network Configuration page as shown above and on the next figure.

MP Network Configuration

The configuration page is divided into three parts, shown in the figure above and on the following page –

IP Interfaces for Media

There is a table showing configured IP Interfaces for the selected network. The table shows IP Address/netmasks; physical location; VLAN Id; and State.

There are links to Create a new IP Interface or Delete an existing IP Interface.

MP Network Configuration 2

SBG - Network Configuration
MP Network Configuration

Routes

Remote subnet address	Remote subnet mask length	Type
0.0.0.0	0	static
10.64.230.0	27	interface

[Table as text](#)

[Create static route](#)
[Delete static route](#)

Next Hops

Next hop address	Next hop address 2	Supervision	Next hop group	Next hop group 2	Administrative state
10.64.230.1	0.0.0.0	slow	No group defined	No group defined	unlocked
10.100.100.100	0.0.0.0	slow	steves_next_hop_group	No group defined	unlocked
10.200.200.200	0.0.0.0	slow	steves_next_hop_group	No group defined	unlocked

[Table as text](#)

[Create next hop](#)
[Delete next hop](#)

[Open networks](#)
[Configure bandwidth](#)
[Network statistics](#)
[Security settings](#)

Routes

In the *Routes* section, there is a table showing configured Routes. Click the red triangle for more details.

“interface” routes are automatically created by the System when an IP Interface is defined.

“static” routes can be configured by clicking on the “Create static route” link.

Next Hops.

In the Next Hops section, there is a table showing Next Hop IP addresses on external routers. Next Hops can be configured in Next Hop Groups.

The amount of bandwidth that can be reserved for (can be used by) media traffic by a network on the MP interfaces. 2 000 000 kbit/s means that the network may use the full MP interface bandwidth.

At the bottom of the page are links to -

Configure Bandwidth - The amount of bandwidth that can be reserved for/used by media traffic by a network on the MP interfaces.

Network Statistics

To view current statistics values and to configure performance measurements on these counters & gauges.

Security Settings (See next page)

Security Settings

SBG - Network Configuration Security Settings

ERICSSON

Network name:	access_lab
Network ID:	1
ICMP echo :	<input checked="" type="radio"/> false <input type="radio"/> true
ICMP delivery:	<input checked="" type="radio"/> false <input type="radio"/> true
TCP checks:	Level2
IP port range:	1024 to 65535
Minimum number of emergency streams:	2

[Open network](#)
[Network configuration](#)
[Create IP interface](#)
[Create next hop](#)
[Create static route](#)

Security Settings

Security settings can be viewed and some can be configured in this page.

TCP Checks

Configure the strength of TCP security checks in the MP.

IP Port Range

Configure the range of ports available for Media.

Minimum Number of Emergency Streams

Minimum number of streams reserved for emergency calls only.

Media Proxy – IP Interface

SBG - Network Configuration
IP Interface

Network name:	access_lab
Network ID:	1
IP interface address:	10.64.230.7
Subrack:	1
Slot:	17
Port:	2
VLAN ID:	710
Subnet mask length:	27
Subnet segment mask length:	27
Usage:	payload termination
Administrative state:	unlocked
Operational state:	enabled

Lock **Lock gracefully**

SBG - Network Configuration
IP Interface

[Open network](#)
[Network configuration](#)
[Create IP interface](#)
[Create next hop](#)
[Create static route](#)

IP interface statistics

Received packets:	44
Received octets:	5185
Transmitted packets:	931
Transmitted octets:	69227
Malicious packets:	1
Excessive packets:	0
Excessive octets:	0
Discarded packets due to no next hop MAC address:	0
Discarded packets due to other reasons:	59

[Performance measurement on this instance](#)

© Ericsson AB 2010 231 SBG 3.1 Operation and Configuration for IMS ERICSSON

IP Interface – Viewing Configuration

In the **MP Network Configuration** page, select an IP Interface, the page above will be displayed, showing configured data for the interface and statistics.

The configuration data includes –

- The IP Address, VLAN & mask of the interface (used for media streams)
- The subrack; slot, port of the physical link (ports 0 & 1 on the backplane, ports 2 & 3 on the front external ports)
- The State of the interface.

Lock Buttons

Lock Gracefully. Sets the **Administrative state** of the **IP interface** to shutting down (if there are connections) or locked (if there are no connections). New connections on the IP interface will not be allowed but existing connections remain until they are released. As long as connections remain on the IP interface, the **Administrative state** will remain in the shutting down state. When all connections have been released, the **Administrative state** will change to locked.

Lock: Sets the **Administrative state** of the **IP interface** to shutting down (if there are connections) or locked (if there are no connections). When the IP interface is locked, all existing connections on the interface will be released. When all connections have been released, the **Administrative state** will change to locked.

There is also a link to **Create IP interface** where new interfaces can be configured. See the next page.

Create IP Interface

SBG - Network Configuration
Create IP Interface

Network name:	access_lab								
Network ID:	1								
IP interface address:	147.214.0.100								
Subrack:	1								
Slot:	17								
Port:	0 (internal side)								
VLAN ID:	200								
Subnet mask length:	28								
Subnet segment mask length:	29								
Usage:	next hop supervision payload termination next hop interface								
IP interface address	Subrack	Slot	Port	VLAN ID	Subnet mask length	Subnet segment mask length	Usage	Administrative state	Operational state
10.64.230.7	1	17	2	710	27	27	payload	unlocked	enabled

[Table as text](#)

[Open network](#)
[Network configuration](#)
[Create next hop](#)
[Create static route](#)

IP Interface Configuration

There are three types of IP interface usage for the IP interfaces that may be configured for the Media Proxy:

- **Payload Termination:** The interface is used for media (payload) transport.
- **Next Hop Supervision:** The interface is used to supervise a next hop address at the router.
- **Next Hop Interface:** The interface is used to forward media to/from an IP interface at the other side of the MP (usually a non-SBG device such as a MGW in the same IS).

Payload Termination

These IP interfaces are used by the MP as source and destination for media traffic. The payload termination IP interface may be located at the external Ethernet interface or at the backplane Ethernet interface.

The IP interface for payload termination is located at the active MP blade and will be moved automatically to the stand-by MP blade in case of active blade failure.

Next Hop Supervision

This type of IP interface is normally only used when media is sent using the MP *external* Ethernet interfaces. When the operator configures this type of IP interface the operator must configure one interface for each Ethernet interface and MP blade.

That is, four IP interfaces per MP blade system, since there are normally two Ethernet interfaces used for media transport per blade and two MP blades.

One IP interface for **next hop supervision** can be configured per MP blade for each Ethernet interface.

When next hop supervision is used for a network (VLAN), it is essential to configure one next hop supervision IP interface on each MP blade since the number of operational next hop supervision IP interfaces may be used as a basis for switching media connection handling to the other MP blade.

Next Hop Supervision is used to enable the MP to:

- detect faults associated with the L2 network between the external routers and the MP
- detect faults in the external routers, for example, that they are not operational.

Fast or Slow Supervision

In addition to configuring the **IP interfaces** for next hop supervision, it is also necessary to configure whether the **Next hops** should be supervised by *fast* or *slow* next hop supervision.

Two cases must be considered:

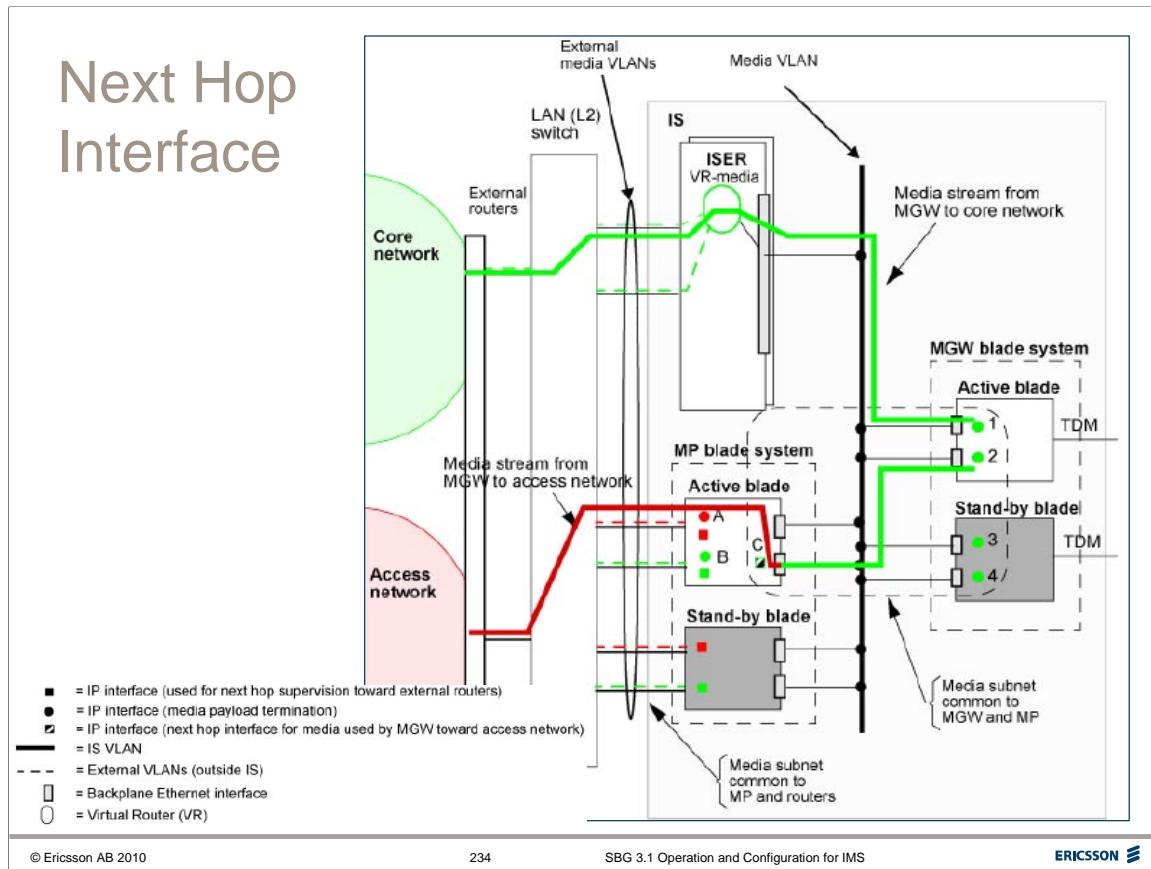
- If there are only two networks configured for the SBG, all the Next hops can be configured to use *fast* ARP supervision. In this case there is no need to configure *next hop groups*.
- If there are more than two networks configured for the SBG, it is recommended to configure one of the networks with **Next hops** to use *fast* next hop supervision and the other networks with **Next hops** to use *slow* next hop supervision. This is to avoid ARP messages being sent to the external routers too frequently.

Next Hop Group

It is also necessary to configure the **Next hops** (used at an individual router interface) for the different networks into a **Next hop group**. That is, the **Next hops** that are used to reach a specific router Ethernet interface, and that belong to different networks, should be configured to belong to the same group. If the MP detects a next hop fault for one of the **Next hops** within a **Next hop group**, all the other next hops in the group will also be considered faulty and will not be used by the MP for media transport. Notice that if separate network for next hop supervision is used the **Next hops** configured for the media networks will not be supervised via periodic ARP supervision, only the **Next hop** configured for the supervision network will be supervised since only this network will have **IP interfaces** of next hop supervision type.

If the active MP blade detects a fault in the next hop supervision towards the router, and if a similar fault is not detected on the stand-by MP blade, the connection handling (the termination of the H.248 protocol) and the media traffic may optionally be moved to the stand-by MP blade, depending on the setting of the *Media Supervision: Next hop supervision included in blade redundancy* attribute

Notice that only the active MP blade sends media traffic over its Ethernet interfaces, although both MP blades will have the next hop supervision activated.



Next Hop Interface

The MP supports dedicated **next hop IP interfaces** on the backplane Ethernet interfaces to enable media transport to and from another *non-SBG blade system* collocated with the SBG in the same IS.

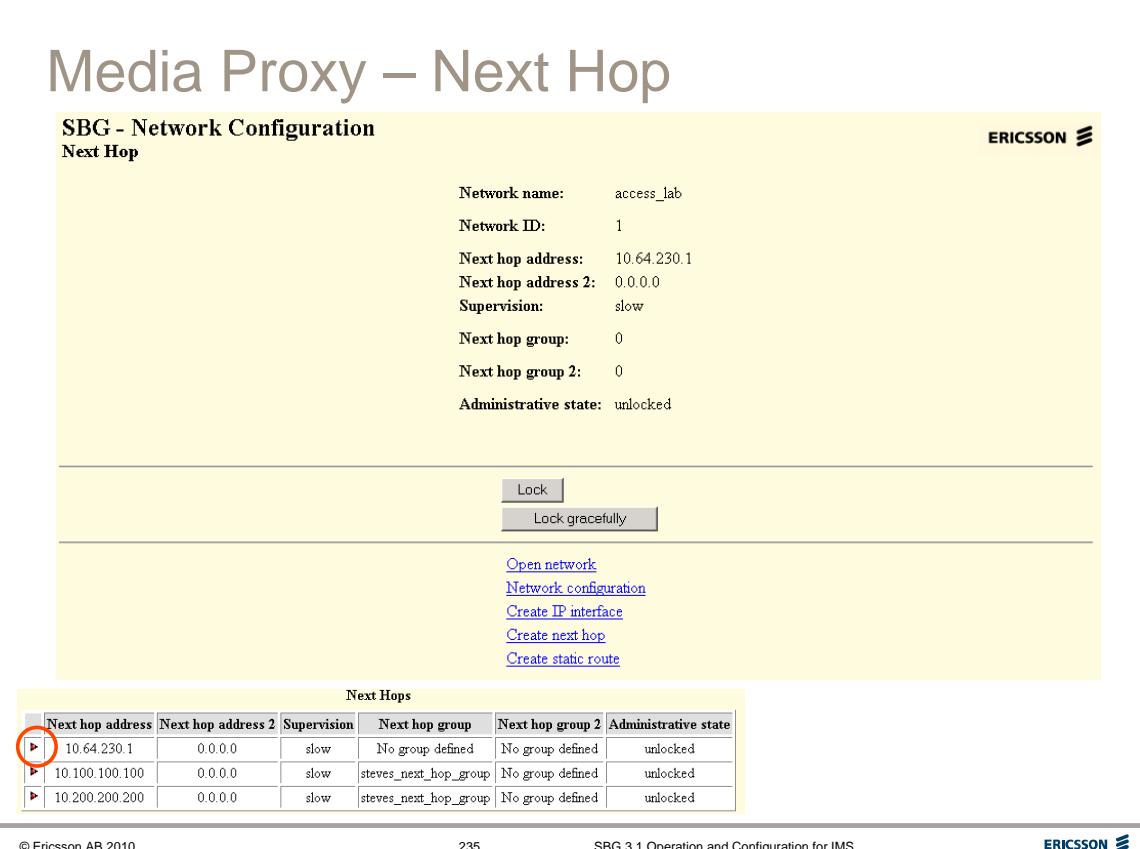
In the example above there is a MGW collocated with the SBG, media transport to and from the access network is required by both the SBG and the MGW. Media traffic going to and from the access network would be media anchored in the MP. So the media passes the MP on its way from the access network to and from the MGW.

When media is not anchored in the MP it is sent directly to and from the MGW via the ISER to the core network.

To avoid using the ISER to forward media between the MP and the MGW, a **next hop interface** on the MP backplane is used.

The **next hop interface** must be configured in the same VLAN and subnet as the payload interface on the MGW. The **MP next hop interface** is used for sessions where media is sent to and from the MGW. The **next hop interface** (C) must be configured for the core network in the MP and on the same logical interface as the IP address B, but on the backplane interface. That is, if B is located on the first *front* interface, C must be located on the first *backplane* interface. The next hop IP interface will automatically be moved to the stand-by MP blade in case of active blade failure and so on.

[In this configuration, an additional **Next hop** and **Static route** is needed in the MGW to enable media to be routed towards the MP. The static route points at the media payload IP interface used on the MP external interfaces (B). The next hop points at the next hop media IP interface on the MP backplane interface (C).]



Media Proxy – Next Hop

SBG - Network Configuration
Next Hop

Network name:	access_lab
Network ID:	1
Next hop address:	10.64.230.1
Next hop address 2:	0.0.0.0
Supervision:	slow
Next hop group:	0
Next hop group 2:	0
Administrative state:	unlocked

[Open network](#)
[Network configuration](#)
[Create IP interface](#)
[Create next hop](#)
[Create static route](#)

Next Hops					
Next hop address	Next hop address 2	Supervision	Next hop group	Next hop group 2	Administrative state
▶ 10.64.230.1	0.0.0.0	slow	No group defined	No group defined	unlocked
▶ 10.100.100.100	0.0.0.0	slow	steves_next_hop_group	No group defined	unlocked
▶ 10.200.200.200	0.0.0.0	slow	steves_next_hop_group	No group defined	unlocked

© Ericsson AB 2010 235 SBG 3.1 Operation and Configuration for IMS ERICSSON

Next Hop

The Next Hops can be viewed on the *Network Configuration* → *MP Network Configuration* page as shown earlier. Clicking the red triangle next to an entry opens the Next Hop details page, an example is shown above.

One or more Next Hops for the media transport must be configured. Each Next hop defines a next hop IP address for media. The next hop is the address in the router via which external media (payload) will be sent and received.

When a Next Hop has been defined, it can be assigned to a Next Hop Route.

Next Hops must be located in the same subnet segment as the associated IP interfaces that will use them.

A Route and a Next Hop are only needed when the destination network (subnet) for media is different to the one the MP media IP interfaces are located in.

Next Hop Group

Next Hops that are used to reach a certain router Ethernet interface and that belong to different networks, are configured to belong to the same Next Hop Group. If the MP detects a next hop fault for one of the Next hops within a Next hop group, all the other next hops within the group will also be considered as faulty and will not be used by the MP for media transport. Next Hop Groups avoid overloading the external routers with ARP messages.

Fault Management

If a failure to contact the next hop address is detected by the ARP monitoring functionality a *nexthopAlarm* will be raised.

Media Next Hop Configuration

SBG - Network Configuration

Create Next Hop

Network name: access_lab

Network ID: 1

Next hop address: 10.10.10.10

Next hop address 2: 10.20.20.20

Supervision: slow

Next hop group: steves_next_hop_group

Next hop group 2: - Not selected -

steves_next_hop_group

Next hop address	Next hop address 2	Supervision	Next hop group	Next hop group 2
10.64.230.1	0.0.0.0	slow	0	0
10.100.100.100	0.0.0.0	slow	1	0
10.200.200.200	0.0.0.0	slow	1	0

Table as text

Open network

Network configuration

Create IP interface

Create static route

Create next hop group

Log out

Events & Alarms Sound Publish

2010-08-04 13:27:39

Create Next Hop

Create Reset Back Help

© Ericsson AB 2010

236

SBG 3.1 Operation and Configuration for IMS

Media Next Hop Configuration

To configure a new Next Hop, click on the *Create Next Hop* link shown on the previous figure.

When creating next hop, the following attributes must be defined:

Next hop address – The IP address at the primary router used to transport the payload (media) to (and from) the external network

Next hop address 2 – The IP address at the secondary router used to transport the payload (media) to (and from) the external network. This second next hop address is optional and is used from the second MP blade when VRRP is not configured in the external routers.

Supervision – The type of ARP supervision used towards the next hop IP addresses. Either slow or fast supervision.

Optionally -

Next hop group – Indicates which next hop group (if any) the next hop at the primary router belongs to.

Next hop group 2 – Indicates which next hop group (if any) the next hop at the secondary router belongs to.

Media Routes

SBG - Network Configuration

Route

Network name:	access_lab
Network ID:	1
Remote subnet address:	0.0.0.0
Remote subnet mask length:	0
Type:	static

Next Hops

Next hop address	Next hop address 2	Supervision	Delete
10.64.230.1	0.0.0.0	slow	<input type="checkbox"/>

[Table as text](#)

[Delete static route](#)

[Add next hop to route](#)
[Open network](#)
[Network configuration](#)
[Create IP interface](#)
[Create next hop](#)
[Create static route](#)

Routes

Remote subnet address	Remote subnet mask length	Type
0.0.0.0	0	static
10.64.230.0	27	interface

[Table as text](#)

[Create static route](#)

© Ericsson AB 2010 237 SBG 3.1 Operation and Configuration for IMS ERICSSON

Media Static Route

The IP media Routes can be viewed from the *Network Configuration* → *MP Network Configuration* page.

The *Interface* route is automatically created when an IP Interface is created.

Static routes are created by the operator.

The Static Route contains information on the next hop addresses that are used to reach a certain destination network (IP subnet), that is, a network (subnet) where the media transport terminates. If Next Hops for media transport have been created, Static Routes must also be configured and the Next Hops associated with the Static Route.

The Route configuration can be viewed by selecting the required entry, as shown above.

Source Filtering

The static routes for media are also used in some special cases to filter out malicious incoming media packets towards the *media pinholes* during initial establishment of a media streams. This is called *source filtering*. e.g. when the users are behind a NAT and the final IP address and port to be used for source filtering are obtained via *latching*. It is recommended to keep the route destination (remote) subnets as small as possible to avoid malicious media being sent towards the *media pinholes* in the MP.

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

Media – Create Static Route

Media Static Route Configuration

Click the **Create Static Route** link in the previous figure. Main attributes are:

Remote subnet address - The IP address of the remote subnet (destination network) for media. The destination network is a subnet containing for example the media IP addresses of the end users or the IP addresses of a remote MGW or SBG.

Remote subnet mask length - The subnet mask length of the remote subnet.

Next hop address - Select a next hop (created earlier) to be associated with the route. This attribute is presented as a selection list with next hop addresses of the defined next hops.

It is not recommended to create a default route (remote subnet address 0.0.0.0 and remote subnet mask length 0) for media since this will, for certain call cases, allow media from all external IP addresses to reach the media pinholes in the MP. This increases the risk for malicious media reaching any open pinholes in the MP, for example during *Latching*.

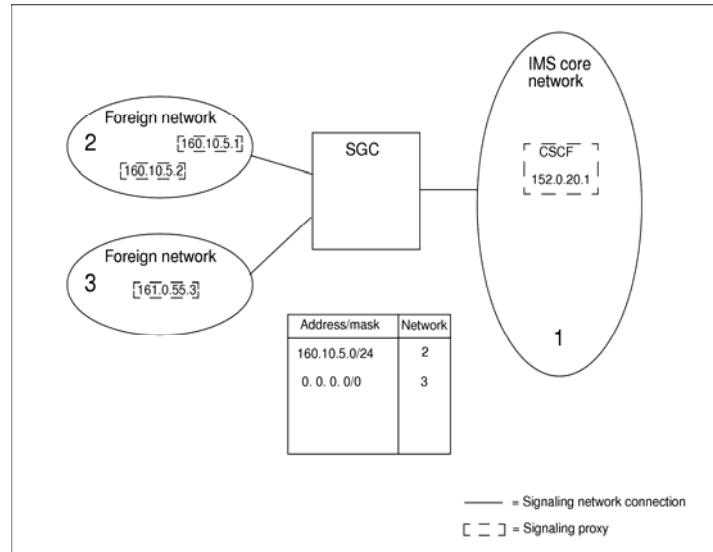
So the example in the figure above is not a recommended configuration. Remote subnet address and remote subnet mask length should be configured correctly, according to the actual network setup.

SBG 3.1 Operation and Configuration for IMS

Address to Network Mapping

For full details of the Network Configuration, refer to the Network Configuration Service Guide, 4/154 43-CNA 113 062

Address-to-network Mapping Overview



Address-to-network Mapping

The IP address-to-network Mapping service is used to enable routing of SIP messages from the IMS Core Network towards a Foreign SIP or H323 Network. i.e. when the SBG acts as an N-SBG implementing the IBCF function.

The SGC determines the IP address of the signalling proxy in the foreign network, either

- a) using a Route or the Request-URI included in the SIP message, or
- b) using the optional outgoing proxy configuration of the core network (configured under **Session Signalling** → **SIP Network Connection** → **Open** the core network).

Using this IP address as input to the **Address-to-network** table, the SGC decides to which Foreign Network the signalling should be forwarded.

In the figure, if the SGC receives a signalling message to be forwarded to IP address 160.10.5.1 in a foreign network, it selects the network by a lookup in the *address-to-network* table and matches the IP address to the record 160.10.5.0/24, which points to foreign network 2.

For the direction from the foreign networks towards the core, the SGC does not use the Address-to-network table for signalling routing (signalling messages are always routed towards the core network from a foreign network), which means that the core network addresses should not be configured in the table.

Address-to-Network Mapping Configuration

Blade system	Subnet address	Subnet mask length	Foreign network name	Delete
SGC_7_19	10.100.6.0	24	Foreign1	<input type="checkbox"/>
SGC_7_19	10.100.7.0	24	Foreign2	<input type="checkbox"/>

In order to use the Address-to-network table, it is required that the foreign networks use different **non-overlapping IP address ranges** for signalling, since the SGC uses the IP address of the signalling proxy in the foreign network as the base for signalling routing.

The user can also configure a default route for signalling (0.0.0.0/0 in the figure above), which means that all IP addresses that do not match any specific IP address and mask will point to the network that is associated with the default route.

When the SGC uses the **address-to-network** table a longest match of the destination IP address will always be performed. This means, for example, if partly overlapping IP address ranges are defined in the table and points to different networks (for example, 123.24.33.128/24 → network A and 123.24.33.192/26 → network B) and the SGC should send signalling towards an address it will always select the network for which the address matches best.

Example

Address 123.24.33.193 matches both the definitions 123.24.33.128/24 and 123.24.33.192/26 but matches best to the 123.24.33.192/26 address, which means that network B will be selected.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Session Signalling Configuration

For full details of the Session Signalling service, refer to the Session Signalling Service Guide, 1/154 43-CNA 113 062

The screenshot shows a web-based configuration interface for the Session Border Gateway. The title 'Session Signalling' is at the top. The left sidebar has a 'MANAGEMENT' menu with several options, and the 'Session Signalling' option is currently selected. The main content area lists various configuration items under 'Session Signalling'.

- Create**
 - [SIP network connection](#)
 - [H.323 network connection](#)
 - [Trunk contexts](#)
 - [IP-PBX](#)
 - [Emergency number](#)
 - [Blacklist profile](#)
 - [Blacklist header](#)
 - [SMM filters](#)
- Open**
 - [SIP network connections](#)
 - [H.323 network connections](#)
 - [SIP registrars](#)
 - [Registrar contact bindings](#)
 - [SIP throttling definitions](#)
 - [Trunk contexts](#)
 - [IP-PBXes](#)
 - [Emergency numbers](#)
 - [Emergency settings and counters](#)
 - [Signaling parameters](#)
 - [Resource statistics](#)
 - [DNS configuration](#)
 - [Blacklist profiles](#)
 - [Blacklist headers](#)
 - [User agent whitelists](#)
 - [SMM rule sets](#)
 - [SMM filters](#)

At the bottom left is a 'Log out' button. The footer contains the text '© Ericsson AB 2010', '244', 'SBG 3.1 Operation and Configuration for IMS', and the 'ERICSSON' logo.

Session Signalling

The main Session Signalling page has links to the following configuration areas:

SIP network connections

H.323 network connections

SIP registrars

Registrar contact bindings

SIP throttling definitions

Trunk contexts

IP-PBXes

Emergency numbers

Emergency settings and counters

Signaling parameters

Resource statistics

DNS configuration

Blacklists

User Agent white lists

SMM rule sets

SMM filters

Session signalling service

SIP network connections & H.323 network connections: Configuration of SIP and H.323 signalling parameters for the networks connected to the SBG.

SIP registrars: Configure SIP Registrars settings - max registered users; timer settings. And view statistics.

Registrar contact bindings: View details of Registered IMPUs (IMS Public Identities) – IP Address/Port; user client and so on.

SIP throttling definitions: support for configuration of SIP message rate limiting (throttling) toward the core network

Trunk contexts & IP-PBXs: Configure Trunk Context and IP-PBX data for access networks to enable IP-PBX session set-up.

Emergency numbers & Emergency settings and counters: Configure Emergency Numbers and associated settings for Emergency Call Handling.

Signaling parameters: Certain Signalling parameters can be configured such as maximum SIP message size, user identification (3GPP or 3261); and attributes for the geographical redundancy function.

Resource statistics – number of registered users and maximum number allowed.

DNS configuration: DNS configuration of the core network DNS used by SGC.

Blacklists: Support for configuration of **blacklists** for SIP signalling, that is, support for specifying not allowed SIP methods, headers, and so on.

User Agent white lists: Support for configuration of **whitelists** - define a list of SIP user agents that are allowed to register with the A-SBG from an access network. It is possible to define one whitelist per network. The user agent whitelist is activated when the User agent restriction attribute is set to true in the associated SIP network connection for an access network.

SIP Message Manipulation (SMM) rule sets and **SMM filters** can be viewed & administered

These **Session Signalling** areas will be described on the following pages.

Performance Measurements

For many of the services described above, there are links to view statistics and create Performance Measurement jobs.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

SIP Network Connections

For full details of the Session Signalling service, refer to the Session Signalling Service Guide, 1/154 43-CNA 113 062

SIP Network Connections

SBG - Session Signaling
ERICSSON

SIP Network Connections

Blade system	Network name	Network role	IP address	Administrative state	Delete
Change all rows					
▶ SGC 1-19-23	access_lab	A-ALG	10.64.230.52	unlocked	<input type="checkbox"/>
▶ SGC 1-19-23	access_ecn	A-ALG	134.138.58.20	unlocked	<input type="checkbox"/>
▶ SGC 1-19-23	mmtel_core	A-ALG	10.64.229.132	unlocked	<input type="checkbox"/>

[Table as text](#)

Blade system	Network name	Network role	IP address	Administrative state	Delete
Change all rows					
▶ SGC 0-5_17	Core	P-CSCF	192.168.9.124	unlocked	<input type="checkbox"/>
▶ SGC 0-5_17	Core	IBCF	192.168.9.125	unlocked	<input type="checkbox"/>
▶ SGC 0-5_17	Access	P-CSCF	192.168.3.68	unlocked	<input type="checkbox"/>

[Table as text](#)

[Create SIP network connection](#)
[Open SIP registrars](#)

© Ericsson AB 2010
248
SBG 3.1 Operation and Configuration for IMS
ERICSSON

SIP Network Connections

SIP network connections must be configured for both Access and Core networks:

IP address – The local IP address of the SGC used for the associated SIP network connection. It is the SIP contact address in the network.

Administrative state – Determines whether the SIP network connection in question is enabled or disabled for traffic. The value can be changed with the buttons Lock forcefully, Lock gracefully and Unlock. The possible values are:

- *shuttingDown*: No new sessions and registrations are allowed, but already established sessions are preserved. Re-registrations are not allowed.
- *locked*: No new sessions and registrations are allowed. Already established sessions are released.
- *unlocked*: New sessions and registrations are allowed.

Network Role

The role for which the SIP network connection is used: A-ALG or P-CSCF for an A-SBG or IBCF for an N-SBG.

Note that the roles in related networks must match e.g. the Access Network and Core Network must both have the role A-ALG (or P-CSCF).

Two examples are shown above.

The top example shows an A-SBG with two access networks and one core network.

The bottom example shows a combined P-CSCF and N-SBG. The N-SBG in the example must have a Foreign Network created with the role IBCF.

SIP Network Connection – Access Network 1

SBG - Session Signaling SIP Network Connection		ERICSSON
Blade system:	SGC 1-19-23	
Network name:	access_lab	
Network role:	A-ALG	
Administrative state:	unlocked	
IP address:	10.64.230.52	
UDP port:	5060	
TCP port:	5060	
SCTP port:	0	
Use TLS:	false	
Blacklist profile:	Access network	
Incoming SMM filter:	No filtering	
Outgoing SMM filter:	No filtering	
Received route trusted:	<input type="radio"/> true <input checked="" type="radio"/> false	
FQDN in via header:	<input type="radio"/> true <input checked="" type="radio"/> false	
User agent restriction:	<input type="radio"/> enabled <input checked="" type="radio"/> disabled	
Outgoing UDP fragmentation:	<input checked="" type="radio"/> Never <input type="radio"/> Standard <input type="radio"/> Always	
Session setup time (s):	60	

To view the settings for a particular network, click the red triangle next to the network entry on the table shown on the previous figure.

The **SIP Network Connection** page appears.

Many of the parameters are self-explanatory, some are described on the following pages.

For full details of all parameters, refer to the reference document.

Signalling Network Connection

A signalling network connection which is identified by the name of the SGC blade system with the name of the network.

Network role

The role for which the SIP network connection is used. Either A-ALG or P-CSCF for an A-SBG or IBCF for an N-SBG.

Blacklist profile:

The SBG can be configured to filter certain SIP headers before proxying SIP messages. The definitions are known as Blacklist profiles.

The operator can configure which SIP headers are to be removed by the SGC. The configuration is defined per combination of SIP method, network and direction. Separate configurations for requests and responses for each method can be defined.

SMM Filters (SIP Message Manipulation):

The SMM function enables the definition of rewriting rules for SIP messages.

Received route trusted:

Specifies if the SGC trusts Route headers in the received SIP messages from the associated network.

true: the SCC trusts Route headers received in incoming SIP messages and will use the headers for SIP routing if present. The SGC will also forward the Route headers in the outgoing SIP messages, if the Route header is not blacklisted.

false: the SCC does not trust Route headers received in incoming SIP messages. The headers will be removed and not forwarded into the other network.

User agent restrictions:

Specifies if the SGC trusts Route headers in the received SIP messages from the associated network. i.e. specifies if Whitelists are to be used.

Use TLS

Indicates if TLS is to be used in the associated network.

FQDN in via header

The attribute indicates whether a Fully Qualified Domain Name (FQDN) or an IP address will be used as the SGC address in the Via header in outgoing SIP requests.

Outgoing UDP fragmentation

It is possible to configure per network the method of handling fragmentation of too large outgoing SIP messages over UDP. It is possible to select 3 different methods:

Never

Try to use TCP (if configured), reject request if not successful

Standard

Try to use TCP (if configured) and use UDP fragmentation if not successful.

Always

Use UDP fragmentation directly, without trying TCP (even if configured SCTP will not be used as fallback protocol from UDP for large SIP messages).

SIP Network Connection – Access Network 2

SBG - Session Signaling

SIP Network Connection

Session setup time (s):	<input type="text" value="60"/>	<input checked="" type="radio"/> enabled <input type="radio"/> disabled
Session expiry supervision:	<input checked="" type="radio"/> enabled <input type="radio"/> disabled	
Minimum session expiry time (s):	<input type="text" value="900"/>	
Maximum session expiry time (s):	<input type="text" value="3600"/>	
Default session expiry time (s):	<input type="text" value="1800"/>	
Maximum non supervised session duration (min):	<input type="text" value="0"/>	
Maximum time before SIP retransmission (ms):	<input type="text" value="500"/>	
Maximum SIP retransmit interval (ms):	<input type="text" value="4000"/>	
Maximum message life time (ms):	<input type="text" value="5000"/>	
Proxy invite transaction timeout (s):	<input type="text" value="180"/>	
Inactivity timer (s):	<input type="text" value="7200"/>	
Registration timer (s):	<input type="text" value="30"/>	
Maximum number of incoming SCTP streams:	20	
Maximum number of outgoing SCTP streams:	20	
SCTP heartbeat timer:	60	

Various signalling parameters can be viewed and changed on this part of the **SIP Network Connection** page.

Session setup time

This timer supervises a session setup and indicates the maximum time in seconds allowed from the moment the SGC sends an INVITE until a Final Response has been received for the INVITE. When the timer expires the SGC will release the associated session

Session Expiry Supervision

The SGC supports the session expiry timer (RFC 4028). This is enabled by the *Session expiry supervision option*. Min, Default, and Max SE values can be configured. If the SGC detects an expired session, it sends a SIP BYE in both directions and releases the reserved resources.

Emergency calls are not affected by session timer expiration.

Default session expiry time (Default SE)

Defines the default session expiry timer to be used when no Session-Expires value is provided in the request.

When two networks are involved in the session the larger of the two configured values is used.

Maximum session expiry time - The maximum value in seconds for a session interval in SIP session supervision.

If the incoming request indicates a higher value for the Session-Expires, the value is reduced to equal this configured value.

If the Min-SE header is greater than the configured Maximum session expiry time, the Session-Expires value will be set to the Min-SE value in the outgoing request.

Minimum session expiry time - The minimum value in seconds for a session interval in SIP session supervision.

If the incoming request indicates a lower value for the Session-Expires, the request is rejected by the SGC with cause *422 Session Timer Too Small*.

When two networks are involved in the session the larger of the two configured Minimum session expiry time values is used.

Maximum non-supervised session duration - If the session timer supervision is disabled in the SGC, or if the UEs of a session do not support the use of the session timer, the operator can configure the SGC to supervise sessions via the "Maximum non supervised session duration" attribute.

Maximum time before SIP retransmission - The value in milliseconds for the SIP T1 timer as defined in RFC 3261.

Maximum SIP retransmit interval - The value in milliseconds for the SIP T2 timer as defined in RFC 3261, for the associated SIP network connection.

Maximum message lifetime - The value in milliseconds for the SIP T4 timer as defined in RFC 3261.

Proxy invite transaction timeout - The value in seconds for the SIP Timer C as defined in RFC 3261.

Inactivity timer - The amount of time in seconds after which a registered SIP UE on a TCP connection in the A-ALG or any TCP connection used for SIP in the IBCF with no activity can be closed. The timer is started each time a new SIP message is received for the connection.

For an access network in the A-ALG, in hosted NAT traversal cases, this timer is not applied. This allows SIP UEs to keep their TCP connections open as long as the UEs are registered in the A-ALG.

Registration timer - The timer provides a security mechanism against attempts by unauthorized users to keep the TCP sockets open by sending SIP messages.

The timer for observing the socket state is started when the TCP connection of the user is established and stopped when the user has successfully registered.

This timer is applicable only for an access network in the A-ALG, since proxy registrar is an A-ALG-specific function. For other types of networks, the timer is always disabled.

SIP Network Connection – Access Network 3

**SBG - Session Signaling
SIP Network Connection**

Outgoing proxy

Proxy domain name:

Proxy IP address:

Default transport protocol: SCTP UDP TCP

Proxy UDP port:

Proxy TCP port:

Proxy SCTP port:

Outgoing topology hiding

Via: on off

Contact: on off

Record route: on off

Path: on off

Service route: on off

[Open signaling network connection](#)
[Create SIP network connection](#)
[SIP connection statistics](#)
[SIP Registrar](#)

© Ericsson AB 2010

253

SBG 3.1 Operation and Configuration for IMS

ERICSSON

Outgoing Proxy (Optional)

The outgoing proxy specifies the default destination IP address and port(s) (or a FQDN domain name) when sending SIP messages from the Access or Foreign Network to the Core Network where the SIP signaling proxy is located.

For the P-CSCF-role a separate E-CSCF can be configured .

Outgoing Topology Hiding

The indicated SIP routing headers can be switched off to hide the topology from an Access or Foreign Network.

Lock Gracefully

No new sessions or registrations are allowed on the network connection. Existing sessions will remain until released. Re-registrations for users with active sessions are allowed while the network connection is in the shuttingDown state. Clients without active sessions will be deregistered.

Lock Forcefully

No new sessions, registrations, or re-registrations are allowed on the network connection. Existing sessions are released by the SGC. When the SGC has released all sessions an *sgcSipNetConnLockedEvent* is issued.

There are also links at the bottom, to **SIP Connection Statistics** for Statistics & Performance Measurements; and to **SIP Registrars** (described later)

SIP Network Connection – Core Network 1

SBG - Session Signaling
SIP Network Connection

Blade system:	SGC 1-19-23
Network name:	mantel_core
Network role:	A-ALG
Administrative state:	unlocked
IP address:	10.64.229.132
UDP port:	5060
TCP port:	5060
SCTP port:	0
Use TLS:	false
Blacklist profile:	Core network
Incoming SMM filter:	No filtering
Outgoing SMM filter:	No filtering
Received route trusted:	<input type="radio"/> true <input checked="" type="radio"/> false
FQDN in via header:	<input type="radio"/> true <input checked="" type="radio"/> false
User agent restriction:	<input type="radio"/> enabled <input checked="" type="radio"/> disabled
Outgoing UDP fragmentation:	<input checked="" type="radio"/> Never <input type="radio"/> Standard <input type="radio"/> Always
Session setup time (s):	60

SIP Network Connection – Core

As well as defining at least one Access Network, a Core Network is needed facing towards the IMS Core Nodes.

The same explanations apply when configuring a SIP network connection for the Core network as in the previous examples, which showed the Access network for A-SBG.

The main parameters to note are:

Network role

This must also be A-SBG or P-CSCF to match the Access Network role.

IP Address

This will be a Private IP Address for signalling to/from the IMS core.

SIP Network Connection – Core Network 2

SBG - Session Signaling
SIP Network Connection

Session expiry supervision:	<input checked="" type="radio"/> enabled <input type="radio"/> disabled
Minimum session expiry time (s):	900
Maximum session expiry time (s):	3600
Default session expiry time (s):	1800
Maximum non supervised session duration (min):	0
Maximum time before SIP retransmission (ms):	500
Maximum SIP retransmit interval (ms):	4000
Maximum message life time (ms):	5000
Proxy invite transaction timeout (s):	180
Inactivity timer (s):	7200
Registration timer (s):	30
Maximum number of incoming SCTP streams:	20
Maximum number of outgoing SCTP streams:	20
SCTP heartbeat timer:	60

SIP Network Connection – Core Network 3

SBG - Session Signaling
SIP Network Connection

Outgoing proxy

Proxy domain name:

Proxy IP address: . . .

Default transport protocol: SCTP UDP TCP

Proxy UDP port:

Proxy TCP port:

Proxy SCTP port:

Outgoing topology hiding

Via: on off

Contact: on off

Record route: on off

Path: on off

Service route: on off

[Open signaling network connection](#)
[Create SIP network connection](#)
[SIP connection statistics](#)
[SIP Registrar](#)

SIP Network Connection – Foreign Network 1

SBG - Session Signaling SIP Network Connection

ERICSSON

Blade system:	SGC_7_19
Network:	Foreign1
Network role:	IBCF
Administrative state:	unlocked
IP address:	192.168.92.140
UDP port:	5060
TCP port:	5060

SBG - Session Signaling SIP Network Connection

ERICSSON

Blade system:	SGC_7_19
Network name:	Core
Network role:	IBCF
Administrative state:	unlocked
IP address:	192.168.9.125
UDP port:	5060
TCP port:	5060

SIP Network Connection – Foreign

The same explanations apply when configuring SIP network connection for the Foreign Network as in the previous descriptions for Access & Core Network.

Network Role

The most important thing to note is the *Network role*.

When defining the N-SBG type of connectivity, SBG uses the IBCF functionality. So the Foreign Network and Core Network must be configured with the IBCF role, as shown above.

IP Address for Foreign Network

The IP Address for the Foreign Network must be in the range defined in *Address to Network Mapping* described earlier.

SIP Network Connection – Foreign Network 2

SBG - Session Signaling
SIP Network Connection

Outgoing proxy in core network

Proxy domain name:

Proxy IP address:

Default transport protocol: UDP TCP

Proxy UDP port:

Proxy TCP port:

Outgoing topology hiding

Via: on off

Contact: on off

Record route: on off

Path: on off

Service route: on off

© Ericsson AB 2010 258 SBG 3.1 Operation and Configuration for IMS ERICSSON

SIP Network Connection – Foreign

The same parameters apply when configuring SIP network connection for the Foreign network as described for the Access network.

Outgoing Proxy

The Outgoing Proxy configuration should be pointing to the **I-CSCF** of the **Core Network**.

Topology Hiding

Normally, the **topology hiding** should be set to “on” as the Foreign Network is normally treated as **untrusted**.

Trusted Network

If the foreign network is a trusted network, e.g. same operator, then the topology hiding can be set to “OFF”.

SBG 3.1 Operation and Configuration for IMS

Creating SIP Network Connections

For full details of the Session Signalling service, refer to the Session Signalling Service Guide, 1/154 43-CNA 113 062

Create a SIP Network Connection 1

SBG - Session Signaling
Create SIP Network Connection

Signaling network connection (Blade system/Network name): SGC1-19-23/access_lab
SGC1-19-23/access_ecn
SGC1-19-23/mmTel_core

Network role: IBCF

IP address: 192.168.1.96

UDP port: 5060

TCP port: 0

SCTP port: 0

Use TLS: true false

Blacklist profile: Access network

Incoming SMM filter: No filtering

Outgoing SMM filter: No filtering

Received route trusted: true false

FQDN in via header: true false

User agent restriction: enabled disabled

Outgoing UDP fragmentation: Never Standard Always

Session setup time (s): 60

Session expiry supervision: enabled disabled

Minimum session expiry time (s): 900

Maximum session expiry time (s): 3600

Default session expiry time (s): 1800

Maximum non supervised session duration (min): 0

Maximum time before SIP retransmission (ms): 500

Maximum SIP retransmit interval (ms): 4000

© Ericsson AB 2010 260 SBG 3.1 Operation and Configuration for IMS ERICSSON

SIP Network Connection

When the SGC acts as a combined A-ALG (or P-CSCF) and IBCF the operator must configure two SIP network connections for the core network.

The reason for this is that the two network roles (IBCF and A-ALG) require different DNS configuration views.

This is enabled by the SGC using the local IP addresses for SIP when requesting DNS information.

The IP address of the A-ALG SIP Network Connection will be used when sending DNS requests for A-ALG session setups, and the IP address of the IBCF SIP Network Connection will be used for IBCF session setups.

Create a SIP Network Connection 2

SBG - Session Signaling
Create SIP Network Connection

Maximum message life time (ms):	<input type="text" value="5000"/>
Proxy invite transaction timeout (s):	<input type="text" value="180"/>
Inactivity timer (s):	<input type="text" value="7200"/>
Registration timer (s):	<input type="text" value="30"/>
Maximum number of incoming SCTP streams:	<input type="text" value="20"/>
Maximum number of outgoing SCTP streams:	<input type="text" value="20"/>
SCTP heartbeat timer (s):	<input type="text" value="60"/>

Outgoing proxy

Proxy domain name:	<input type="text" value="edu.mmtel.net"/>
Proxy IP address:	<input type="text" value="0.0.0.0"/>
Default transport protocol:	<input type="radio"/> SCTP <input checked="" type="radio"/> UDP <input type="radio"/> TCP
Proxy UDP port:	<input type="text" value="5060"/>
Proxy TCP port:	<input type="text" value="5060"/>
Proxy SCTP port:	<input type="text" value="0"/>

Outgoing topology hiding

Via:	<input checked="" type="radio"/> on <input type="radio"/> off
Contact:	<input checked="" type="radio"/> on <input type="radio"/> off
Record route:	<input checked="" type="radio"/> on <input type="radio"/> off
Path:	<input checked="" type="radio"/> on <input type="radio"/> off
Service route:	<input checked="" type="radio"/> on <input type="radio"/> off

[Open SIP network connections](#)

© Ericsson AB 2010 261 SBG 3.1 Operation and Configuration for IMS ERICSSON

Outgoing Proxy

The outgoing proxy specifies the default destination IP address and port(s) (or a FQDN domain name) when sending SIP messages from the Access or Foreign Network to the Core Network where the SIP signaling proxy is located.

Outgoing Topology Hiding

Defined whether certain headers are sent to the network. Setting to ‘on’ for a network means the header **will not be sent to that network**.

Normally set to ‘off’ for Core Networks, as these routing headers are safe in the IMS Core.

Normally set to ‘on’ for Access and Foreign Networks to prevent topology details being sent to ‘untrusted’ users & networks.

For P-CSCF Networks, the Topology Hiding is automatically set to ‘off’ for the Core Network and ‘on’ for Access Networks and cannot be changed.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

Signalling Parameters

The SIP Signalling Networks have now been defined, certain SGC-wide Signalling Parameters can be configured.

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154 43-CNA 113 062

Signalling Parameters

SBG - Session Signaling
Signaling Parameters

Proxy failover delay (s):

Proxy fallback delay (s):

Proxy polling interval (s):

Proxy polling method: REGISTER OPTIONS

I/S-CSCF location: colocated separated

Blade system	Fallback Mode
▶ SGC 0-5_17	Automatic

[Table as text](#)

Forced SIP-URI escaping: Reject Escape

User identification method: 3GPP RFC 3261

Blade system	Host and domain name	Maximum size of SIP messages (bytes)
▶ SGC 0-5_17	eelis01.edu.ims.se	3 000

[Table as text](#)

Proxy failover delay

The proxy failover delay defines the time that a signaling proxy must be down (as seen from the SGC) before the SGC stops using it and declares it as unreachable.

When the SGC stops using the proxy the SGC will send an *sgcDestUnreachEvent* indicating that the proxy is down.

Proxy fallback delay

The proxy fallback delay defines the time that the signaling proxy must be up (assuming that the SGC has detected it to be unreachable) before the SGC starts using it again.

When the SGC starts to use the primary proxy again, the SGC will send an *sgcDestReachEvent* indicating that the primary proxy is up.

Proxy polling interval

The proxy polling interval defines the time between sending polling signaling messages toward a signaling proxy that the SGC has detected as unreachable.

Polling is used by the SGC to be able to detect that a proxy is available for use again.

Setting the interval to zero disables the polling.

Proxy polling method

This attribute defines which SIP message method to use for polling signaling proxies that have been detected as unreachable, REGISTER or OPTIONS.

I/S-CSCF Location

This attribute specifies how geographical redundancy is handled by the SGC when it acts as a P-CSCF. The attribute is not valid when the SGC acts as an A-ALG or IBCF.

It affects the failover/fallback mechanism and the way the SGC views the I/S-CSCF nodes in the core network in terms of availability.

- **colocated**: The I- and S-CSCF nodes are expected to be jointly available/unavailable. If one is down, the other is also down.
- **separated**: The I- and S-CSCF nodes are expected to be available/unavailable independently of each other.

Forced SIP URI Escaping

In the SBG 3.1 it is possible to configure how illegal characters in a SIP URI should be handled. When illegal characters are detected in a SIP URI, the message can be rejected or the characters are *escaped** using hex encoding and forwarded to the core.

**escaped* – the character is sent in the form “%hexvalue”.

User identification method

The P-CSCF will assert that a P-Preferred-Identity header received from a user matches a registered IMPU of the user.

If the assertion of the P-Preferred-Identity is successful the identity will be inserted in the P-Asserted-Identity header to the S-CSCF in the core network.

If the P-Preferred-Identity does not match a registered user IMPU or no P-Preferred-Identity was included, the **User identification method** attribute will be used as follows:

User identification method - 3GPP

The **default IMPU** of the user will be forwarded as the user's P-Asserted-Identity. The default IMPU is either the first IMPU received in the P-Associated-URI, if received in the REGISTER response, or the To header used at registration by the user.

User identification method - RFC3261

P-CSCF will use the **From** header to assert the user identity. If the assertion of the From header is successful the identity will be forwarded as a P-Asserted-Identity header to the S-CSCF in the core network. If the From header does not match a registered user IMPU the request will be rejected.

SBG - Session Signaling
Proxy Fallback

Fallback Mode: Manual Automatic

Initiate Manual Fallback

SBG - Session Signaling
Signaling Parameters

Blade system: SGC 0-5_17

Blade system	Host and domain name	Maximum size of SIP messages (bytes)
SGC 0-5_17	ee1is01.edu.ims.se	3 000

© Ericsson AB 2010

266

SBG 3.1 Operation and Configuration for IMS

ERICSSON

Proxy Fallback (for Geographical redundancy)

Fallback Mode

When the SGC detects that a signaling proxy is down, it may either use an automatic fallback mechanism to initiate a fallback to the primary proxy which is done instantaneously when the primary node becomes available, or rely on the operator to manually initiate a fallback after proxy recovery.

If the SGC is configured as a P-CSCF, and the *I/S-CSCF location attribute* is set to *separated*, then this attribute is valid for S-CSCF fallback only.

For I-CSCF nodes the fallback will always be performed automatically by the SGC.

For the A-SBG after the manual fall back all sessions that have been established using a secondary proxy, except emergency call, are released by the SGC as they reregister. This means that when the users reregister they migrate back to the primary proxy.

For the IBCF, sessions established via a secondary proxy will not be released on manual fallback. New session setups (or other initial or standalone SIP requests) will use the primary proxy but the remaining sessions will remain at the secondary proxy until released.

Signalling Parameters

Defines the **Host and Domain name** (the SBG FQDN) and the **Maximum Size of SIP Messages**.

SBG 3.1 Operation and Configuration for IMS

SIP Registrars

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154
43-CNA 113 062

**SBG - Session Signaling
SIP Registrars**

Session Gateway Controller Blade Systems

Blade system	Maximum number of registered users	Registered users
SGC 1-19-23	120 000	2

Access Network Connections

Blade system	Network name
SGC 1-19-23	access_lab
SGC 1-19-23	access_ecn

**SBG - Session Signaling
Open SIP registrar**

Blade system: SGC 1-19-23
Registered users: 2
Maximum number of registered users: 120000

**SBG - Session Signaling
Open SIP registrar**

Blade system: SGC 1-19-23
Network name: access_lab
Quarantine timer (s): 1800
Default contact expiry duration (s): 90
Default core expiry duration (s): 1900
Maximum contact expiry duration (s): 36000
Minimum contact expiry duration (s): 40
Accepted registrations: 4412
Rejected registrations: 732
Registered users: 2

[Performance measurement on this instance](#)
[Performance measurement on all instances of the SBG](#)

© Ericsson AB 2010

268

SBG 3.1 Operation and Configuration for IMS

ERICSSON

SIP REGISTRARS

The **SIP registrars** configuration section allows the operator to define the behaviour of user registration handling per access network connection when users register with the core network.

SIP registrar attributes can be configured only for **Access Signaling Network Connections**.

Session Signalling → SIP Registrars displays a survey of the SIP Registrar networks, as shown above.

Session Gateway Controller Blade Systems

Selecting one of the **Session Gateway Controller Blade Systems** opens a page where:

The Maximum Number of Registered Users can be viewed/configured

The current number of registered users is displayed.

Access Network Connections Blade Systems

Selecting one of the **Access Network Connections Blade Systems** opens a page where the following parameters can be viewed/set:

Quarantine timer

The length in seconds of the quarantine period of the associated access network. If the IP filtering mechanism in the SGC detects an IP packet flood from a certain IP address and port, the mechanism first triggers an *sgcBlockingIPTrafficEvent* notification. In addition, if there is a registered user in the A-SBG that has used this IP address and port combination, an *sgcRegUserInQuarantineEvent* notification is issued.

All Public User Identities that have been registered from that IP address with explicit or implicit registration are then deregistered and put into quarantine. During this quarantine period, no registrations with these Public User Identities are allowed from any IP address and port combination.

Default contact expiry duration

The default value in seconds used for the registration Expires timer at the access network side, if a SIP UE has not set an Expires value in the REGISTER request sent to the A-SBG.

In this case, when calculating the Expires value to return to the SIP user (in the 200 OK to REGISTER), this default value is used if it is lower than the Expires time negotiated for the core network side. Otherwise, if the Default contact expiry duration is greater than the Expires value negotiated for the core network side, the core network Expires timer will be used in the 200 Ok response (to REGISTER) sent to the SIP UE.

Default core expiry duration

The default Expires value in seconds that the A-SBG assigns to Expires for a contact in a REGISTER request forwarded from the access network to the core network during SIP user or IP-PBX registration. The core network will return the Expires value to be used for the core network side in the 200 OK response to the REGISTER message.

Maximum contact expiry duration

The maximum value in seconds that the A-SBG accepts as an *Expires* value for a contact at the access network side.

Minimum contact expiry duration

The minimum value in seconds that the A-SBG accepts for an *Expires* value for a contact on the access network side.

If the SIP UE presents a lower Expires value in the REGISTER request, the A-SBG will reject the request with error response 423 – *Interval Too Brief*.

The screenshot displays the SBG - Session Signaling interface. The top left window is titled 'SBG - Session Signaling' and 'Registrar Contact Bindings'. It contains two buttons: 'Display contact bindings' and 'Export registrar database'. The top right window is titled 'SBG - Session Signaling' and 'Display Contact Search'. It has a search bar with 'New IMPU search: stevep@edu.ims.se' and a 'Table as text' button. Below these are two tables. The first table is titled 'IMPU lookups' and shows two entries: 'sip:4687131007@edu.ims.se' (Time stamp: 2010-07-01 11:36:57, Search status: Ready) and 'sip:4687131001@edu.ims.se' (Time stamp: 2010-07-01 11:35:36, Search status: Ready). The second table is titled 'Display Contact Bindings' and shows a single entry: 'Access Contact' (sip:4687131007@147.214.150.29:5060;transport=udp) and 'Core Contact' (sip:4687131007@147.214.150.29:5060;transport=udp;EnBindingId=420). Both tables have a 'Table as text' button at the bottom.

Display Contact Bindings

This function makes it possible to query SIP registry data for all contacts registered for a certain specified IMS public user identity (IMPU).

When a query is made, it is possible to display the contacts registered to a specific IMPU. It is also possible to view the details of any contact by opening a link to a 'Contact details' page.

The SBG can store up to ten IMPU queries.

Export Registrar Database

This function allows the user to transfer the SIP registrar database, with all contacts registered in the SBG, as a set of files (one file per SGC) to an external host using FTP.

SBG 3.1 Operation and Configuration for IMS

IP-PBX

IP-PBX Support

The A-SBG (A-ALG/P-CSCF) is the PNI connection point between the IMS core network and IP-PBXs. Three main types of IP-PBXs are supported by the SBG:

IP-PBX sending REGISTER. Used with the BroadSoft Business Trunking (BT) solution. Referred to as *BroadSoft Business Trunking REG IP-PBX*.

IP-PBX relying on Registration Surrogate in the A-ALG. Used with the BroadSoft BT solution. Referred to as *BroadSoft Business Trunking non-REG IP-PBX*.

IP-PBX not using REGISTER. Used with the Ericsson BT solution. Referred to as *Ericsson Business Trunking IPPBX*.

In general, the SBG treats the IP-PBXs like ordinary UEs, but as described below, there are a number of differences in registration and handling of certain SIP headers.

A-SBG recognizes traffic going to/from IP-PBX and applies special handling to messages. It limits the number of simultaneous sessions for each IP-PBX by configuration.

Common Functions

The access network, IP address, and geographical location of each IP-PBX is configured in the A-SBG. The geographical location information is inserted in the PANI header.

Each IP-PBX is configured as trusted or untrusted which determines how the A-SBG handles the P-Asserted-Identity and History-Info headers toward the IP-PBX.

The A-SBG also provides session admission control per IP-PBX.

BroadSoft Business Trunking REGISTERING IP-PBX

The BroadSoft BT REG IP-PBX is a SIP PBX and sends single REGISTERs for the entire PBX to the A-SBG, which forwards it according to the same principles as for normal users.

The A-SBG supports that a BroadSoft BT REG IP-PBX is placed behind a NAT/FW.

The A-SBG has support to modify the Request-URI of terminating SIP requests, i.e. if the request URI is a SIP URI; the user part is replaced with the phone number in the To-header field.

BroadSoft Business Trunking Non-REGISTERING IP-PBX

The BroadSoft BT non-REG IP-PBX can be either a SIP or H.323 PBX and the SBG performs SIP-H.323 interworking if needed.

This IP-PBX does not issue REGISTER requests but is dependent on some other node to do that. The A-SBG therefore contains a Registration Surrogate function which initiates single REGISTERs for the entire PBX to the IMS core network and ensures that the PBX stays registered. The ASBG includes the Trunk Group parameter in REGISTER requests to the IMS core network, so that other nodes can identify the IP-PBX.

The A-SBG supports that a BroadSoft BT non-REG IP-PBX is placed behind a NAT/FW.

For a SIP based BroadSoft BT non-REG IP-PBX, the A-SBG undertakes the same modification of terminating Request-URI as for a BroadSoft BT REG IP-PBX. For H.323 based IP-PBX, the A-SBG performs normal mapping, H.323 to SIP mapping.

Ericsson IP-PBX

The Ericsson IP-PBX can be either a SIP or H.323 PBX and the SBG performs SIP-H.323 interworking if needed.

The Ericsson IP-PBX does not issue REGISTER requests and does not need any other node to do so for it.

For signaling originating from the Ericsson IP-PBX, the A-SBG adds the Trunk Context and Trunk Group parameters before sending the messages to the IMS core network, so that other nodes can identify the PBX.

The ASBG can also modify the Request-URI before forwarding the message to the core network. Depending on the configuration of the Public Service Identity (PSI) parameters in the SGC, the A-SBG modifies the host part, replaces the host part, or replaces both the host and user parts of the Request-URI.

For signaling destined for an Ericsson IP-PBX, the A-SBG uses the Trunk Context and Trunk Group parameters in the Request-URI received from the IMS core to look up which PBX to forward the message to.

Create IP-PBX 1

SBG - Session Signaling
Create IP-PBX

Common Parameters

Signaling network connection (Blade system/Network name):

Type of PBX: Ericsson Broadsoft Broadsoft RS

IP address:

UDP port:

TCP port:

Trunk group:

Trusted for privacy information: true false

Signaling protocol: SIP H.323

SIP default transport protocol: UDP TCP

Default location:

Maximum sessions:

© Ericsson AB 2010 273 SBG 3.1 Operation and Configuration for IMS ERICSSON

Create IP-PBX 2

SBG - Session Signaling
Create IP-PBX

Ericsson PBX Parameters

PSI user part:
PSI prefix part:
PSI host part:
PSI host part:

Broadsoft PBX Parameters

Proxy domain name:
Proxy IP address: 192 . 168 . 7 . 97
Default transport protocol: SCTP UDP TCP
Proxy UDP port: 5060
Proxy TCP port: 5060
Proxy SCTP port: 0
NAT: True False
Request-URI: jee1pcscf01.edu.ims.se
Core contact expiry duration: 1900

[Open IP-PBXs](#)

IP-PBXs

SBG - Network Configuration IP-PBXs

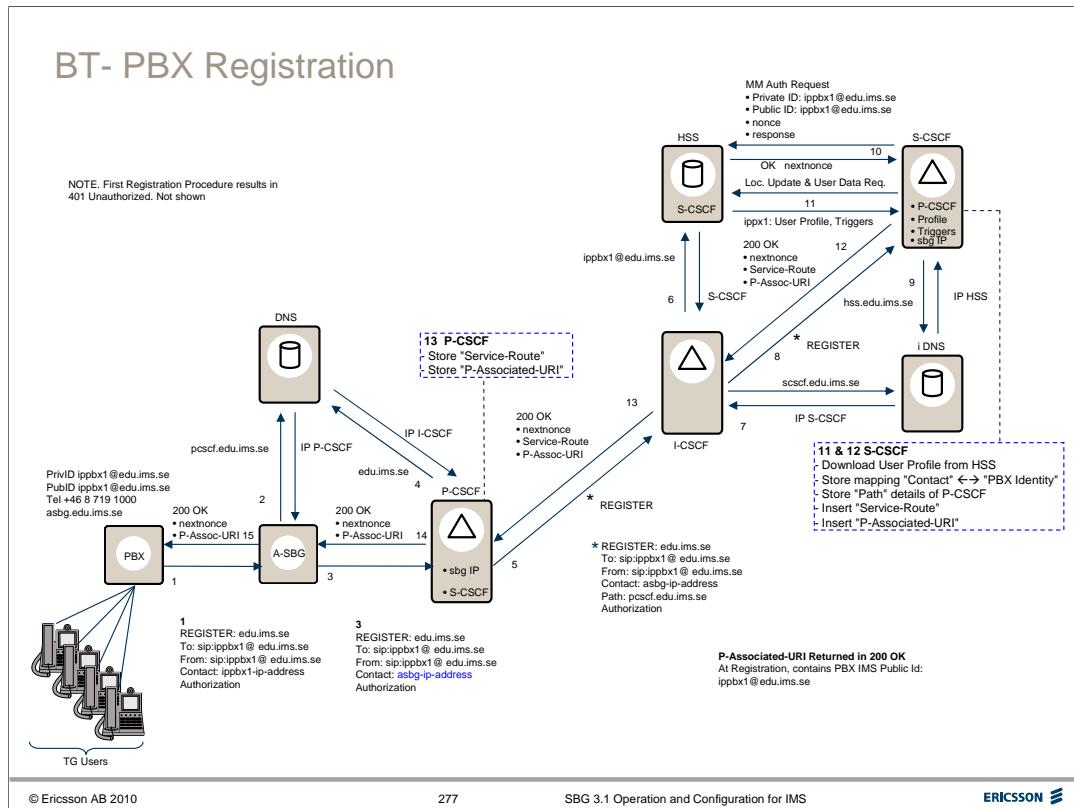
ERICSSON

Blade system	Network name	Type of PBX	IP address	Trunk group	Trusted for privacy information	Signaling protocol	Delete
▶ SGC 0-5_17	Access	Broadsoft RS	147.214.150.29	sip:tgr2@edu.ims.se	false	SIP	<input type="checkbox"/>

[Table as text](#)[Create IP-PBX](#)

SBG as Registration Surrogate

```
⊕ Internet Protocol, Src: ee1is01asgc01 (192.168.9.124), Dst: ee1pcscf01 (192.168.7.97)
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊕ Session Initiation Protocol
  ⊕ Request-Line: REGISTER sip:ee1pcscf01.edu.ims.se SIP/2.0
  ⊕ Message Header
    Max-Forwards: 70
    ⊕ Via: SIP/2.0/UDP 192.168.9.124:5060;branch=z9hg4bkg3zqkv7in7glm1uc13peevibss12yfp75
    ⊕ To: <sip:tgr2@edu.ims.se>
    ⊕ From: <sip:tgr2@edu.ims.se>;tag=svpzhzq6z2ggz84fd8i1l268f3z5smri
      Call-ID: h7hg7f3iv4yv83qm2353e9tsikmoov15
    ⊕ CSeq: 319080 REGISTER
    ⊕ Contact: <sip:2263@192.168.9.124:5060;transport=udp;EriBindingId=2263>;expires=1900
      Route: <sip:192.168.7.97:5060;transport=udp;lr>
      P-Access-Network-Info: Education;network-provided
      P-Visited-Network-ID: ee1is01.edu.ims.se
      Path: <sip:192.168.9.124;transport=udp;lr>
    Content-Length: 0
```



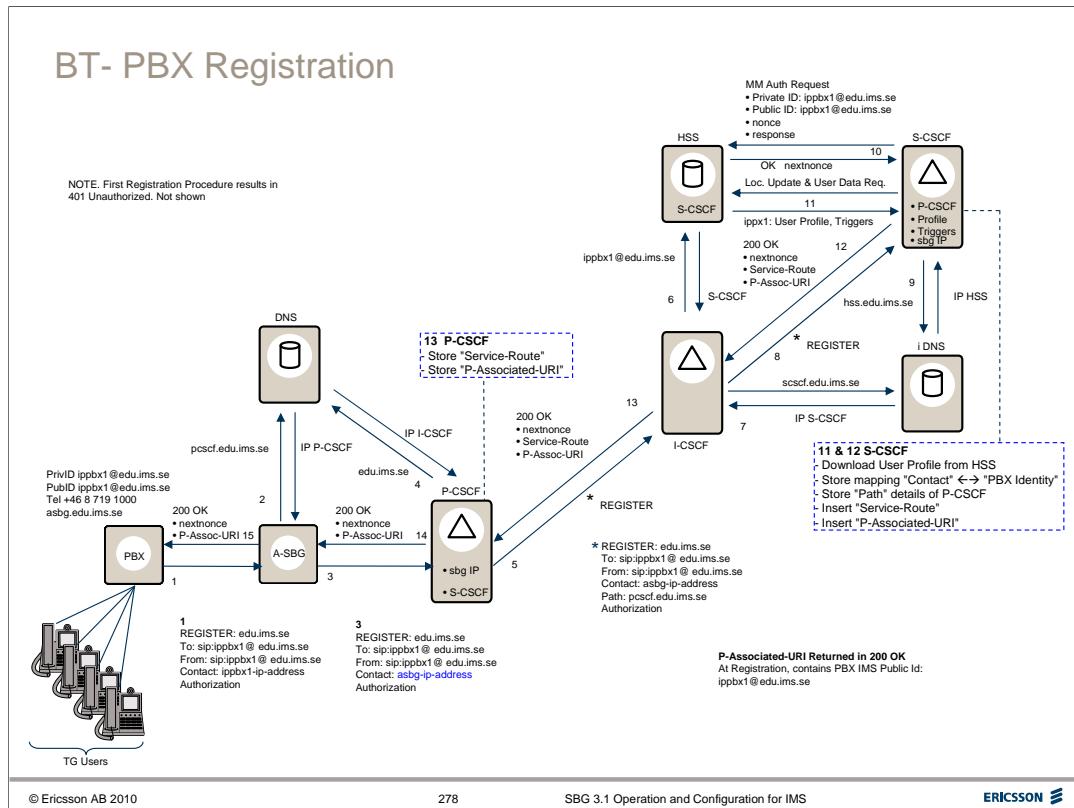
REGISTERING the IP-PBX

From IMS, the IP-PBX is seen as a single SIP UA addressed with a single Public Identity **representing the PABX as a whole**. The IP PBX Registers by sending a REGISTER with the IP-PBX IMS Public User identity (IMPU). The end users behind the IP PBX are not registered in IMS. The IP-PBX IMS Private User identity (IMPI) is configured in the IP-PBX SIP client.

IP-PBX IMPU is provisioned in HSS, ENUM and CS-AS. End users behind the IP PBX are not provisioned in HSS.

The SIP interface present in the IP PBX is able to answer HTTP-Digest challenges. SIP and Non-SIP terminals can be connected behind the IP PBX.

In the case of a SIP terminal connected to the IP PBX, a unique SIP client in IP PBX represents the SIP terminals and is able to answer HTTP-Digest challenges on behalf of the SIP terminals. IP PBX acts as a B2BUA.



REGISTRATION FLOW

(Numbers refer to the signal numbers in the figure above, not all signals are described)

The first Registration Flow resulting in 401 Unauthorized is not shown.

1. IP-PBX Sends Register to A-SBG. The From, To & Contact fields all contain the Public ID of the IP-PBX. The Request header contains the domain.

3. A-SBG replaces the Contact field with its own ID.

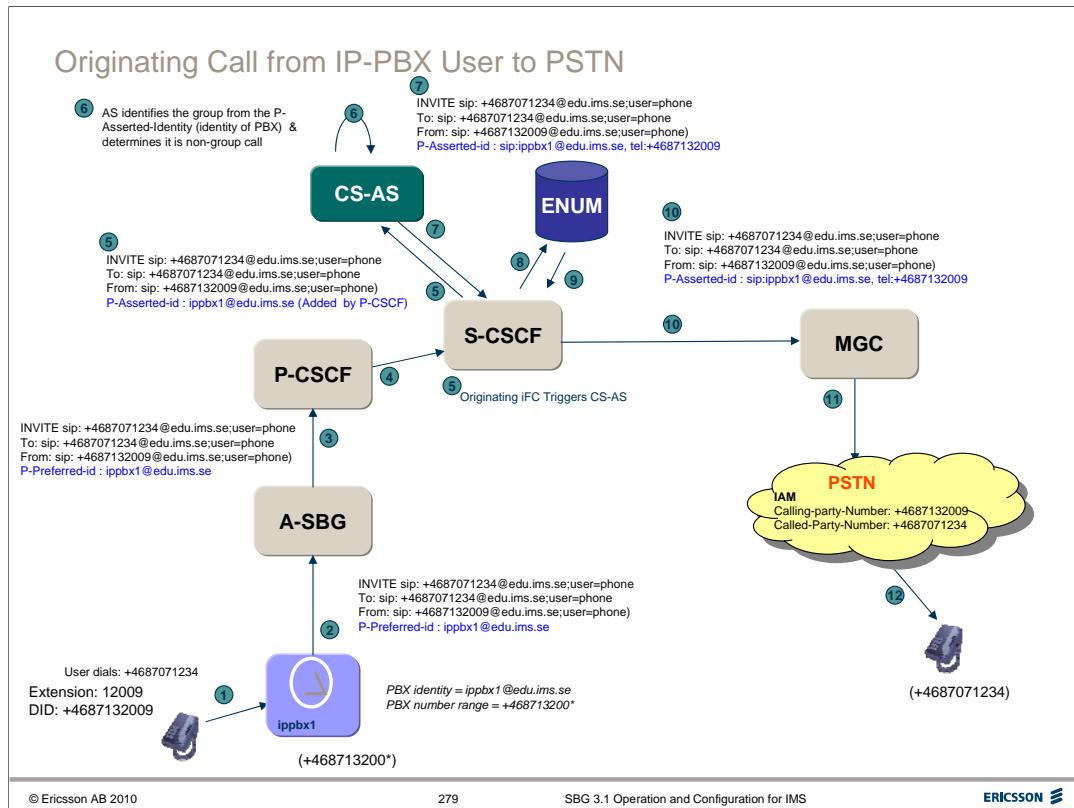
5. P-CSCF Adds its FQDN in the Path header.

6. I-CSCF queries HSS for the Public ID of the IP-PBX. This is defined in HSS, which Returns a 'success' message and directs the I-CSCF to an appropriate S-CSCF.

10 & 11 S-CSCF Sends HSS the Public ID of the PBX and the Authentication vectors. HSS authenticates the PBX and the PBX Profile & Triggers are downloaded to S-CSCF. The PBX is marked as Registered in HSS & S-CSCF.

12 S-CSCF Returns 200 OK, adding the P-Associated-URI field with the Sip: URI and Tel: URI of the PBX.

PBX Users can now make and receive calls.



ORIGINATING CALL FLOW Example

(Numbers refer to the signals in the figure above)

2 & 3 The PBX inserts the PBX Public-ID in the P-Preferred-Id field (or SBG if the PBX cannot provide the header). The From header contains the ID of the PBX User.

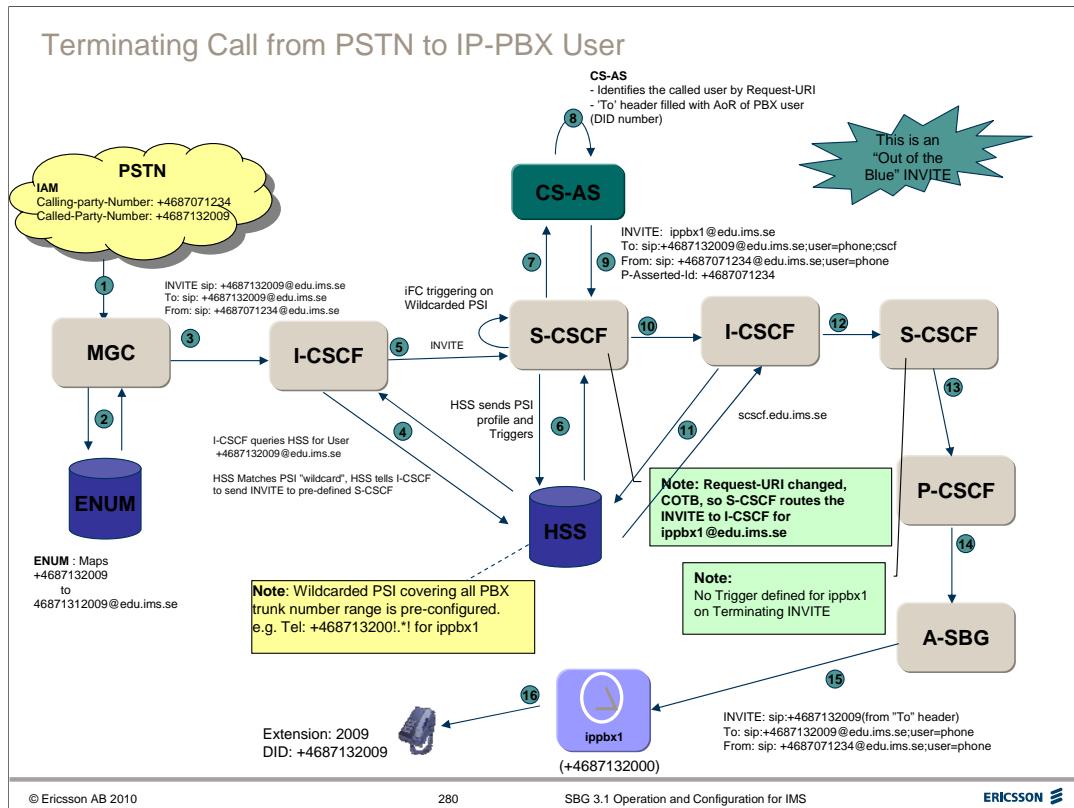
4. P-CSCF The UserID in the P-Preferred-Id (or From field if there is no P-Preferred-Id) is compared with all registered users in the P-CSCF. This identifies the service route and the correct implicit registration set.

If a match is found then the P-CSCF populates the P-Asserted-Identity header with the P-Preferred-ID (assuming `CscfServedUserIdentitySelection`, is set to `PPreferredId`).

If there is no match at all on any registered public ID then the P-CSCF returns 403 Calling User Not Registered.

5. The S-CSCF Checks the Originating Triggers for the UserID in the P-Asserted-Id (i.e. the PBX) and proxies the INVITE to the PBX's CS-AS.

6. The CS-AS identifies the Trunk Group from the P-Asserted-Id; AS checks the To header and determines the called user is not in the same Group; it applies any originating services for the Trunk User in the From header and sends a new INVITE to the S-CSCF and the call proceeds in the normal way for IMS Routing.

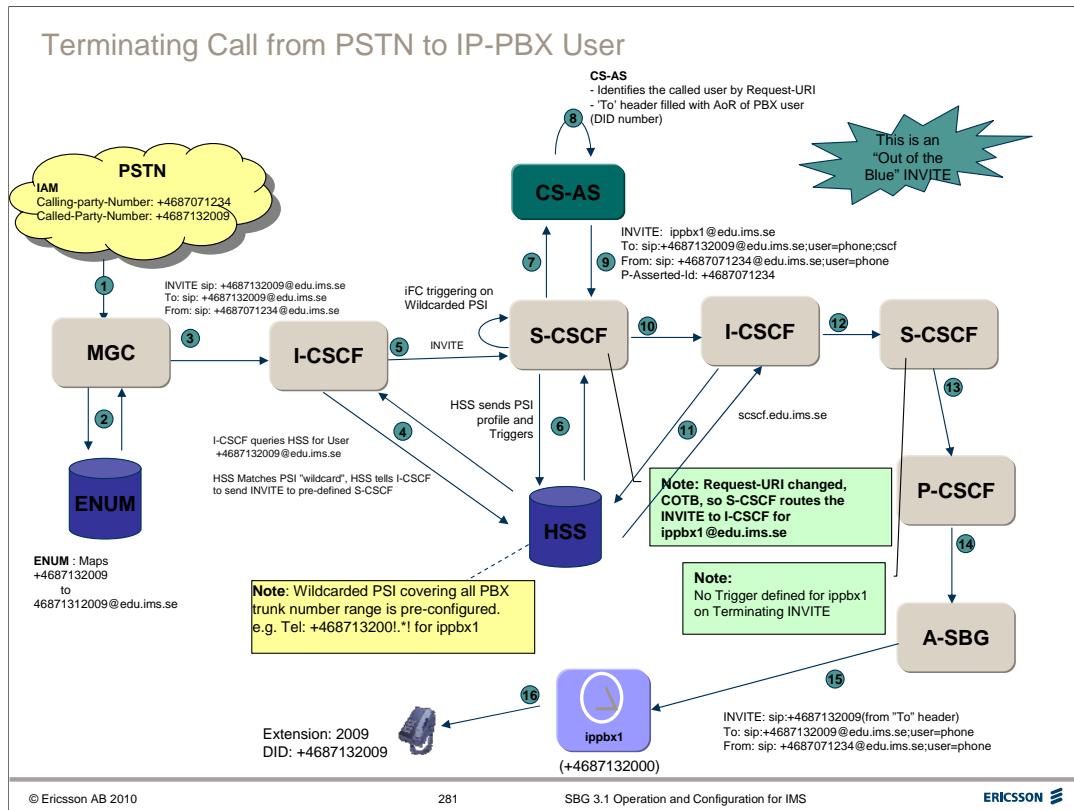


TERMINATING CALL FLOW Example. MGC using ENUM

(Numbers refer to the signals in the figure above)

Incoming calls to PBX users make use of the wildcarded PSI defined in HSS to route the INVITE. The figure above shows a call from a PSTN user to a PBX user.

1. The MGC receives the IAM from PSTN containing the PBX user's telephone number (+4687132009).
 2. MGC performs ENUM lookup of the PBX user's number and is given the user's Public SIP:URI (All PBX users must be configured in ENUM).
 3. MGC queries DNS for the user's domain 'edu.ims.se' and is given the I-CSCF for the domain. MGC then sends the SIP INVITE to I-CSCF. The Request URI and To field contain the PBX user's Public ID.
 4. I-CSCF queries HSS to check if the PBX user in the Request URI is registered, and to which S-CSCF to send the INVITE. HSS matches the user's ID to the wildcard PSI and replies that there is a match but the user is not registered. So the I-CSCF proxies the INVITE to the default S-CSCF defined in its configuration.
 - 5, 6 & 7. S-CSCF receives the terminating INVITE and sees that it does not have the called user registered. It queries HSS which matches the user ID to the wildcarded PSI entry. It downloads the PSI profile and its triggers to S-CSCF. S-CSCF then sends the INVITE to the CS-AS defined in the Terminating Unregistered INVITE trigger.



8 & 9. CS-AS identifies the Group to which the called user belongs and notes that the user is a Trunk Group member. The CS-AS applies any Terminating Services for the called user, if any are active, inserts the PBX ID in the Request URI and sends a new INVITE back to S-CSCF. This is treated as a Call out of the Blue, so S-CSCF needs to find the S-CSCF on which the PBX pilot ID is registered.

10. S-CSCF queries DNS for the I-CSCF serving the PBX's domain and sends the INVITE to I-CSCF. (Note this is probably the same I-CSCF in steps 4,5 & 6).

11. I-CSCF queries HSS with the PBX Public ID. HSS sees that the PBX is registered and returns the relevant S-CSCF details.

12 & 13. S-CSCF finds the PBX is registered and has no Triggers (to avoid triggering the CS-AS twice for the same call), so proxies the INVITE on to the PBX's P-CSCF (Stored from the 'Path' header during Registration). Before sending the INVITE, the S-CSCF replaces the domain in the Request URI with the IP address of A-SBG, also obtained during Registration).

14 The P-CSCF proxies the INVITE on to the A-SBG

15 A-SBG replaces the Request URI with the called user's URI from the 'To' header and forwards the INVITE to the PBX.

16. The PBX sends the INVITE to the user's SIP client, with appropriate manipulation (PBX is a B2BUA).



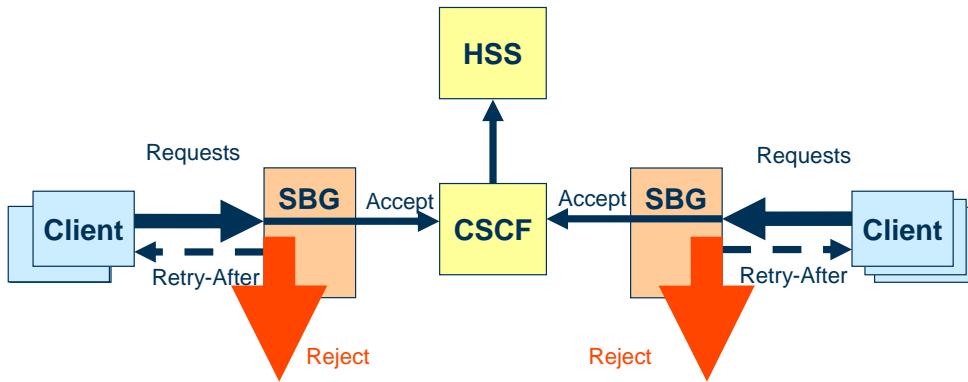
ERICSSON

SBG 3.1 Operation and Configuration for IMS

SIP Message Throttling

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154
43-CNA 113 062

SBG Request message throttling



Core Network Protection Including Retry-After

The throttling mechanism in the SGC limits the rate of SIP messages to protect the core network from overload, for example, if many users try to register simultaneously. The function is based on a transaction window, containing the number of outstanding SIP transactions towards the core network.

Once a SIP request has been handled in the SGC, (Final Response received, or transaction timeout), the next SIP request can take its place in the transaction window. The faster the core network can process the transactions, the shorter time each transaction will stay in the window, and the faster a new SIP transaction can be placed in the transaction window.

There is a mechanism to prioritize which transaction requests are to be sent to the core network if the transaction window becomes full. The following priorities are used:

1. Emergency calls (Highest priority)
2. Release requests
3. Subsequent requests within a dialog
4. Subsequent REGISTER requests, i.e. REGISTER requests with an authentication header (only relevant for the A-SBG)
5. Initial (non-REGISTER) requests
6. Initial REGISTER requests, without an authentication header (Lowest priority)

If the transaction window becomes full, the SGC does not forward new SIP messages to the core network but rejects them with a SIP final response *503 Service Unavailable* which includes a **Retry-After** header.

SBG Signalling Overload protection

The SBG implements a load control mechanism to protect the SBG from becoming overloaded by signalling requests. The SGC blade system performs the load control by measuring the processing time of the signalling messages and the usage of the system resources. Messages are prioritized, and at high load messages with the lowest priority are rejected. Initial requests are rejected first. When rejecting SIP messages due to overload, the SGC sends a SIP final response 503 Service Unavailable which includes the Retry-After header. The Retry-After is set to a random value between the configured minimum and maximum times in order to smooth out the load caused by repeated attempts. This function is particularly useful in REGISTER avalanche scenarios where a lot of REGISTER messages are sent to the SBG.

SIP and H.323 messages for setting up new emergency sessions are prioritized, so that they are accepted also during overload. At extreme load, if the SGC socket buffers for SIP and H.323 become full, the SGC will drop excessive messages silently.

BGF Overload Protection

For robustness, the SBG also has an internal window mechanism to protect the BGF from being overloaded by H.248 requests from the SGC or SGCs. Using the same mechanism, the SGC is protected from being subject to overload from the BGFs.

In the event of processor and memory overload the SGC starts to reject gradually, as follows:

Step 1:

SGC accepts REGISTER and INVITE request normally, but other requests are accepted only if those are connected to existing sessions.

The requests that are not accepted are rejected with SIP response 503, Service Unavailable.

Ongoing sessions are served normally. In practice, this means that the non session related SIP requests, like MESSAGE, NOTIFY, SUBSCRIBE, REFER, etc. are the first ones affected when those requests are not sent in an INVITE dialog.

Step 2:

SGC rejects REGISTER and INVITE requests.

New SIP sessions and user registrations are thus not accepted. If memory shortage exists but there is available processor power re-REGISTER will be processed.

Step 3:

Any received requests or responses are rejected including for ongoing sessions.

Step 4:

SGC temporarily stops reading the sockets for SIP communication.

SGC uses the SIP 503 Service Unavailable final response to reject the SIP requests in points 1, 2, and 3 above.

A Retry-After header is included.

SIP Request Throttling - Configuration

SBG - Network Configuration
SIP Request Throttling Definitions

Blade system	Network name	Network role	Window size	Retry-after low limit	Retry-after high limit
SGC 1-19-23	mmtel_core	A-ALG	0	10	60

[Table as text](#)

ERICSSON

SBG - Session Signaling
SIP Request Throttling Definition

Blade system: SGC 1-19-23
Network name: mmTEL_core
Network role: A-ALG
Window size:
Retry-after low limit:
Retry-after high limit:
Ongoing SIP requests: 0
Rejected SIP requests: 0

ERICSSON

© Ericsson AB 2010

286

SBG 3.1 Operation and Configuration for IMS

ERICSSON

SIP Message Throttling Configuration

Window size

The maximum number of open SIP transactions for the associated **Signaling network connection**. Setting the **Window size** to 0 disables the throttling function.

Retry-after low limit - Defines a lower limit, in seconds, to be used when randomizing a value for Retry-After SIP header.

Retry-after high limit - Defines an upper limit, in seconds, to be used when randomizing a value to the Retry-After SIP header.

The *Retry-After* value is selected between the *Retry-after low limit* and the *Retry-after high limit* and is included in the *500 Internal Service Error* response to a request that was rejected by the SGC due to one of the following situations:

- message throttling
- SGC overload.

Statistics

Ongoing SIP requests

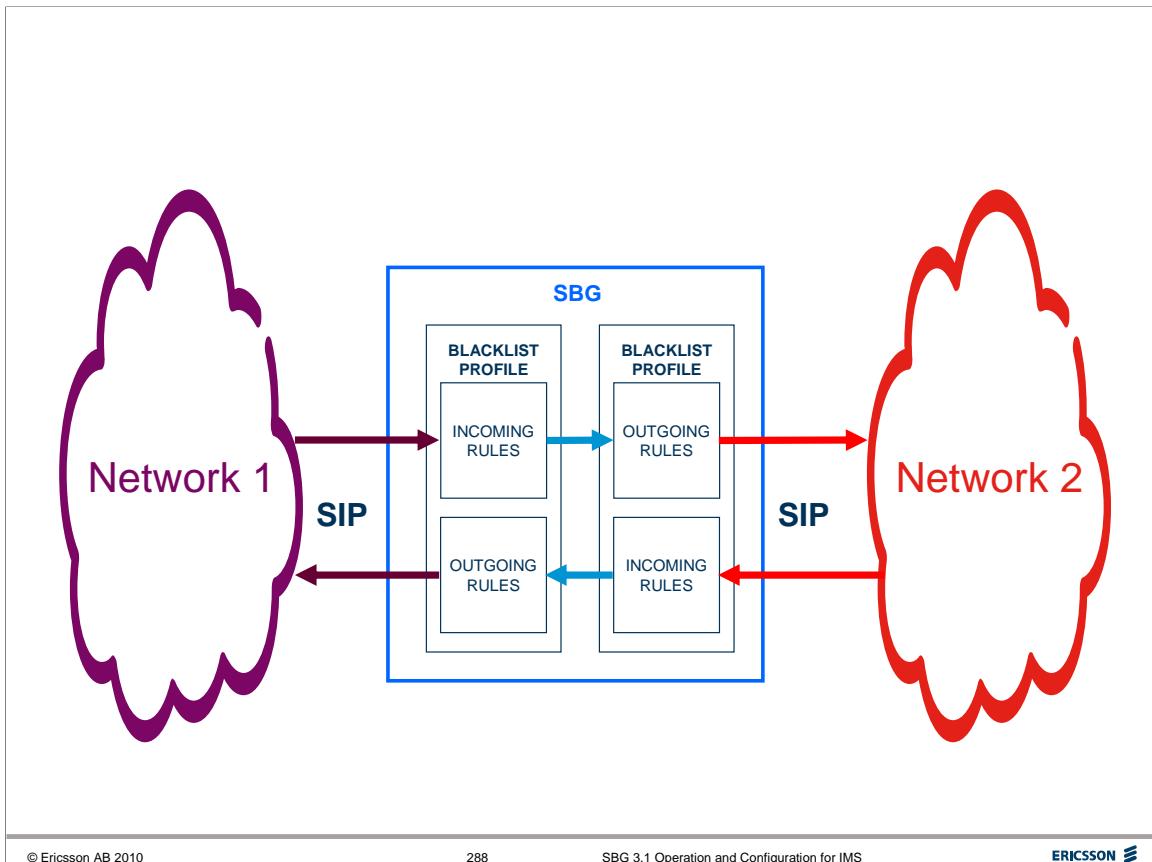
Shows the current number of ongoing SIP requests on the associated **Signaling network connection** for which no provisional or final responses have been received yet (that is, unfinished SIP transactions).

Rejected SIP requests

Shows the total number of rejected SIP requests due to the throttling function on the associated **Signaling network connection**.

SBG 3.1 Operation and Configuration for IMS

Blacklists



SIP HEADER BLACKLISTS

Using the SBG SIP header blacklist feature, the operator can configure for certain SIP headers to be removed by the SGC. The configuration is performed for a combination of SIP method or response, network and direction. Separate configurations for requests and responses of each method are also supported.

This means each SIP message will be filtered through two Blacklist Profiles, incoming and outgoing, as shown in the Figure above.

Blacklists are created in three stages –

1. Any SIP Headers to be specified in a Blacklist must be defined.
2. A Blacklist Profile is created and assigned a name.
3. Rules are then added to the Blacklist Profile, identifying the Method and/or response; the direction and the name of the SIP header to be removed. A Blacklist Profile can include several rules.

A Blacklist Profile can then be assigned to a Network

Create a Blacklist Header

SBG - Session Signaling
Create Blacklist Headers

Header name:

Blacklist header	Delete
*	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
P-Access-Network-Info	<input type="checkbox"/>
Diversion	<input type="checkbox"/>
History-Info	<input type="checkbox"/>
P-Charging-Function-Addresses	<input type="checkbox"/>
P-Visited-Network-ID	<input type="checkbox"/>
P-Charging-Vector	<input type="checkbox"/>
P-Associated-URI	<input type="checkbox"/>
P-Called-Party-ID	<input type="checkbox"/>
P-User-Database	<input type="checkbox"/>
P-Asserted-Identity	<input type="checkbox"/>
Priority	<input type="checkbox"/>
Security-Client	<input type="checkbox"/>
P-Media-Authorization	<input type="checkbox"/>
P-Early-Media	<input type="checkbox"/>

[Table as text](#)

Create Blacklist Headers

To define a new SIP Header for use in Blacklists, go to **Session Signalling → Create Blacklist Headers** and add the header string.

See the figure above.

The '*' entry means “all SIP headers”.

Create a Blacklist Profile

SBG - Session Signaling
Create Blacklist Profiles

Blacklist profile name:

Blacklist profile name	Delete
<i>Change all rows</i>	<input checked="" type="checkbox"/>
▶ No filtering	<input type="checkbox"/>
▶ Core network	<input type="checkbox"/>
▶ Foreign network	<input type="checkbox"/>
▶ Access network	<input type="checkbox"/>

[Table as text](#)

[Create and List Blacklist headers](#)

Create a Blacklist Profile

To create a new Blacklist Profile, go to **Session Signalling → Create Blacklist Profile** and enter a name for the Profile, as shown above.

Create Blacklist Rule

SBG - Network Configuration
Create Blacklist Rule

ERICSSON

Blacklist profile name:	Steves
Blacklist profile ID:	4
Method:	INVITE
Direction:	<input type="radio"/> In <input checked="" type="radio"/> Out
Message type:	<input checked="" type="radio"/> Request <input type="radio"/> Response <input type="radio"/> Both
Blacklist header:	* P-Preferred-Identity P-Access-Network-Info Diversion History-Info

© Ericsson AB 2010

291

SBG 3.1 Operation and Configuration for IMS

ERICSSON

Create Blacklist Rules

To add rules to the new Blacklist Profile, go to **Session Signalling → Open Blacklist Profiles** select the Profile from the list and click the **Create Blacklist Rule** link. The screen shown above opens.

Multiple rules can be added to a Blacklist Profile.

The following parameters are configured for the rule –

Method

The SIP Method for which the rule applies is entered or a '*' if the rule applies for all Methods.

Direction

In or Out.

Message Type

Select Request, Response or Both (i.e. Request & Response).

If for example Method is set to 'INVITE' and Response is selected, then the rule applies to all Responses to an INVITE.

Blacklist Header

Select the Header for the rule from the pull-down list. '*' indicates all headers are blacklisted and will be removed.

Example Backlist Profile - Core

SBG - Session Signaling
Blacklist Profiles

Blacklist profile ID: 1
Blacklist profile name: Core network

Blacklist rules				
Method	Direction	Message type	Blacklist header	Delete
<i>Change all rows</i>				
*	in	Both	P-Preferred-Identity	<input type="checkbox"/>
*	in	Both	P-Access-Network-Info	<input type="checkbox"/>
*	in	Both	P-Media-Authorization	<input type="checkbox"/>
*	in	Both	P-Early-Media	<input type="checkbox"/>

[Table as text](#)
[Create Blacklist Rule](#)

© Ericsson AB 2010 292 SBG 3.1 Operation and Configuration for IMS ERICSSON

Example Backlist Profile - Access

SBG - Session Signaling Blacklist Profiles

ERICSSON

Blacklist profile ID: 3
Blacklist profile name: Access network

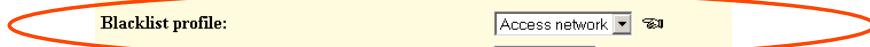
Blacklist rules				
Method	Direction	Message type	Blacklist header	Delete
<i>Change all rows</i>				
*	in	Both	P-Access-Network-Info	<input type="checkbox"/>
*	in	Both	Diversion	<input type="checkbox"/>
*	in	Both	P-Charging-Function-Addresses	<input type="checkbox"/>
*	in	Both	P-Visited-Network-ID	<input type="checkbox"/>
*	in	Both	P-Charging-Vector	<input type="checkbox"/>
*	in	Both	P-Associated-URI	<input type="checkbox"/>
*	in	Both	P-Called-Party-ID	<input type="checkbox"/>
*	in	Both	P-User-Database	<input type="checkbox"/>
*	in	Both	Priority	<input type="checkbox"/>
*	in	Both	P-Media-Authorization	<input type="checkbox"/>
*	in	Both	P-Early-Media	<input type="checkbox"/>
*	out	Both	Diversion	<input type="checkbox"/>
*	out	Both	P-Charging-Function-Addresses	<input type="checkbox"/>
*	out	Both	P-Visited-Network-ID	<input type="checkbox"/>
*	out	Both	P-Charging-Vector	<input type="checkbox"/>
*	out	Both	P-Called-Party-ID	<input type="checkbox"/>

[Table as text](#)[Create Blacklist Rule](#)

Blacklist Usage

**SBG - Session Signaling
SIP Network Connection**

Blade system:	SGC 1-19-23
Network name:	access_lab
Network role:	A-ALG
Administrative state:	unlocked
IP address:	10.64.230.52
UDP port:	5060
TCP port:	5060
SCTP port:	0
Use TLS:	false
Blacklist profile:	<input type="button" value="Access network"/>
Incoming SMM filter:	<input type="button" value="No filtering"/>
Outgoing SMM filter:	<input type="button" value="No filtering"/>
Received route trusted:	<input type="radio"/> true <input checked="" type="radio"/> false
FQDN in via header:	<input type="radio"/> true <input checked="" type="radio"/> false
User agent restriction:	<input type="radio"/> enabled <input checked="" type="radio"/> disabled
Outgoing UDP fragmentation:	<input checked="" type="radio"/> Never <input type="radio"/> Standard <input type="radio"/> Always
Session setup time (s):	<input type="text" value="60"/>



The **Blacklist Profile** can be assigned to a SIP Network Connection, as shown above.

SBG 3.1 Operation and Configuration for IMS

User Agent Whitelist

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154
43-CNA 113 062

SBG - Session Signaling
SIP Network Connection

Blade system: SOC
Network name: Access
Network role: A-ALG
Administrative state: unlocked
IP address: 192.168.3.68
UDP port: 5060
TCP port: 5060
SCTP port: 0
Use TLS: false
Blacklist profile: No Mailing
Received route trusted: true false
FQDN in via header: true false
User agent restriction: enabled disabled
Outgoing UDP fragmentation: Never Standard Always

SBG - Session Signaling
User Agent Whitelist

User agent	Priority	Delete
Movial	1 000	<input type="button" value="Delete"/>

© Ericsson AB 2010 296 SBG 3.1 Operation and Configuration for IMS

User agent whitelist

It is possible to configure a list of user agent types that are allowed to register, per access network.

Wildcards ('*') are allowed at the start or end of the User Agent field.

If the User-Agent header in the REGISTER request is configured in the whitelist, the registration attempt is accepted.

If the User-Agent header in the REGISTER request is not configured in the whitelist, the registration attempt is rejected with 403.

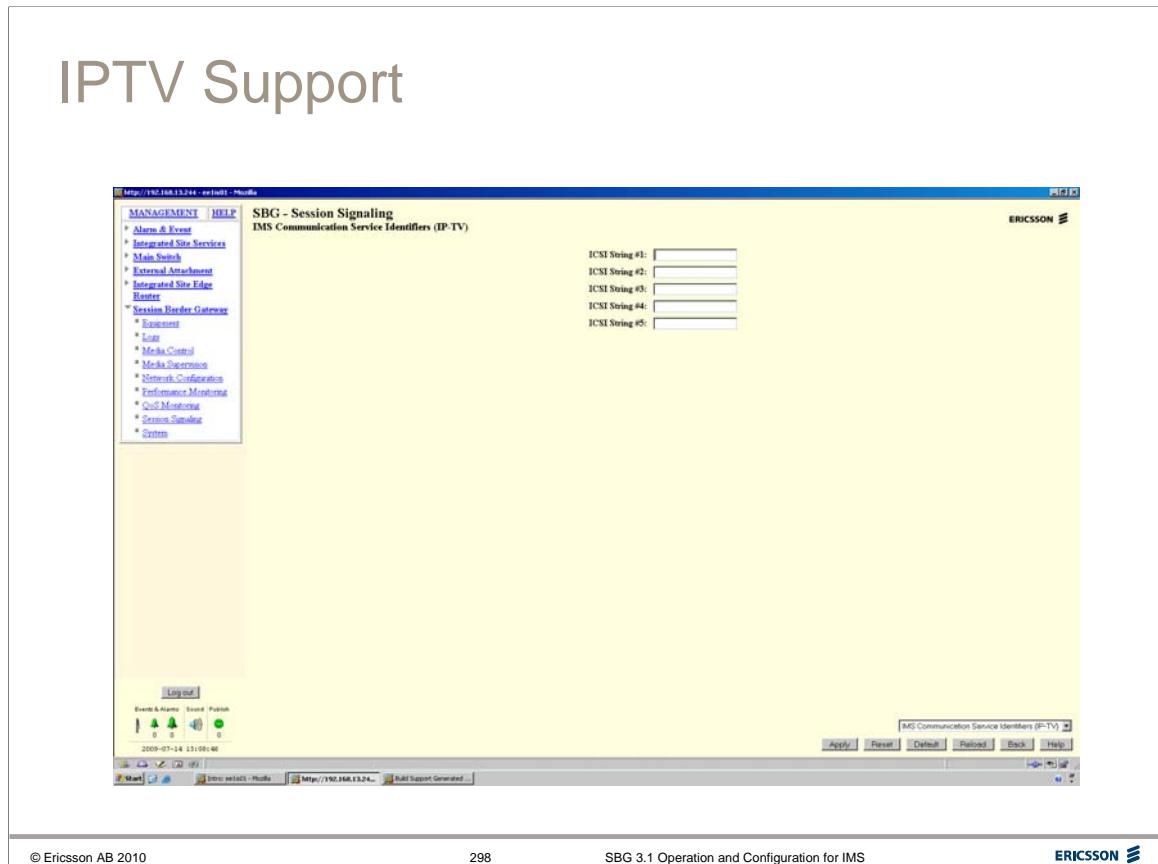
The user agent whitelist is activated when the operator sets the "User agent restriction" attribute to true in the associated SIP network connection for an access network.

In the above example, only Registrations with the User Agent field containing exactly the string "Movial" would be allowed. It might be better to use "*Movial*" instead.

SBG 3.1 Operation and Configuration for IMS

IPTV Support

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154
43-CNA 113 062



IPTV Support

To avoid anchoring certain types of IPTV traffic in the BGF the A-ALG and the PCSCF will determine if a SIP session is an IPTV session. The classification is performed only to ensure correct handling of IPTV streams in the SPDF.

The IPTV session classification in A-SBG is performed when the initial SIP INVITE request is received. If the request contains the ***Accept-Contact*** SIP header and includes the ***g.3gpp.app_ref*** or the ***g.3gpp.icsi_ref*** feature tag, the feature tag value is compared to the list of configured IMS Communication Service Identifiers ***ICSI String#1 - ICSI String #5***.

It is possible to define five different values of the IPTV feature tags.

The feature tags are defined as ICSI String#1 - ICSI String #5. The setting is valid for the whole SBG.

SBG 3.1 Operation and Configuration for IMS

Emergency Calls

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154
43-CNA 113 062

Emergency Settings and Counters

SBG - Session Signaling
Emergency Settings and Counters

Non-registered users allowed: true false

Emergency location settings

Blade system	Network name	Network type	IP version	Default location	Send default location at emergency
▶ SGC 1-19-23	access_lab	access	IPv4	stockholm; network-provided	true
▶ SGC 1-19-23	access_ecn	access	IPv4	london; network-provided	true
▶ SGC 1-19-23	mmtel_core	core	IPv4		true

[Table as text](#)

E-CSCF Address

E-CSCF domain name:

E-CSCF IP address: [...](#)

Default transport protocol: UDP TCP

E-CSCF UDP port: [...](#)

E-CSCF TCP port: [...](#)

Emergency Calls Counters

Blade system	Network name	Total number of Emergency Calls setup	Number of failed Emergency Calls
▶ SGC 1-19-23	access_lab	0	1
▶ SGC 1-19-23	access_ecn	0	0
▶ SGC 1-19-23	mmtel_core	15	10

[Table as text](#)

© Ericsson AB 2010 300 SBG 3.1 Operation and Configuration for IMS

Emergency Settings and Counters

Emergency Call handling is configured at **Session Signalling** → **Emergency Settings and Counters** see the figure above. The settings are:

Non-registered users allowed

Defines if Emergency calls from non-registered users are allowed.

Emergency Location Settings

The default geographic location name and activation are configured for each network. If location information could not be retrieved from CLF, this location will be used.

E-CSCF Address

In P-CSCF role, emergency calls will be routed to an E-CSCF if configured (or as a normal call if no E-CSCF is configured).

In A-ALG, Emergency calls will be routed to P-CSCF as for normal calls.

In N-SBG, Emergency calls are routed as normal sessions. The calls will be given priority if the associated destination URI has been configured as an emergency number.

Emergency Calls Counters

There are counters for the number of emergency calls set up and failed for each network.

SBG - Session Signaling
Emergency Numbers

Description	Type	Number or SIP identifier	Delete
SOS	sip	+112	<input type="checkbox"/>
SOS	sip	112@edu.mmtel.net	<input type="checkbox"/>
SOS	tel	112	<input type="checkbox"/>
SOS	tel	+112	<input type="checkbox"/>

[Table as text](#)

[Create emergency numbers](#)

SBG - Session Signaling
Create Emergency Numbers

Description: [Change](#)

Type: sip tel

Number or SIP identifier: [Change](#)

Emergency numbers			
Description	Type	Number or SIP identifier	Delete
SOS	sip	+112	<input type="checkbox"/>
SOS	sip	112@edu.mmtel.net	<input type="checkbox"/>
SOS	tel	112	<input type="checkbox"/>
SOS	tel	+112	<input type="checkbox"/>

[Table as text](#)

[Open emergency numbers](#)

© Ericsson AB 2010

301

SBG 3.1 Operation and Configuration for IMS

ERICSSON

Emergency numbers

In the **Session Signalling** → **Emergency Numbers** page, the telephone numbers or SIP:URIs that should be treated as Emergency Numbers are viewed/defined. Calls to these destinations will be prioritized in the SBG.

Emergency Numbers must be defined in the same format as that received from the incoming signaling system.

The **Emergency Numbers** can be a tel:URL or SIP:URI.

For emergency number comparison, the incoming URI is normalized to a string as follows:

For a SIP URI, only the user and host parts are considered (including the @ character if present). The port, if received after the host part, is removed.

For a TEL URI only the number (global or local) is considered.

The resulting URI string is then compared to the Emergency Number definitions.

If the URI matches any of the emergency number definitions of the corresponding URI scheme (SIP or TEL), then the call will be treated as an emergency call.

Note that no other configured SIP Message Manipulation (SMM) functions are executed before the Emergency Number check is performed.

As an option, the *Identifier* field can also be in the form of a *regular expression* which may cover a wider range of identifiers. These should be used very carefully as regular expressions can be complicated.



ERICSSON

SBG 3.1 Operation and Configuration for IMS

DNS Configuration

For full details of the Session Signalling, refer to the Session Signalling Service Guide, 1/154
43-CNA 113 062

DNS Configuration

SBG - Session Signaling
DNS Configuration

Blade system: SGC

Primary DNS address: 192.168.7.3

Secondary DNS address: 192.168.7.3

[DNS query testing](#)

SBG - Session Signaling
DNS Query Testing

Query: edu.ims.se

Record: NAPTR

Query role: A-ALG

Last change: 2008-10-21 7:27:14

Result

100 50 s SIP+D2T_sip._tcp.edu.ims.se
100 40 s SIP+D2U_sip._udp.edu.ims.se

Table as text

DNS Configuration

The DNS servers in the Core IMS network must be configured in SBG.

The SGC will query these DNS servers for Naming Authority Pointer (NAPTR), service (SRV), and address (A) records for the IP Address & Port for servers in the IMS core network (CSCFs) or an N-SBG or I-CSCF in the foreign network.

Select the **Session Signalling → DNS configuration** to display and modify the DNS settings of the SBG.

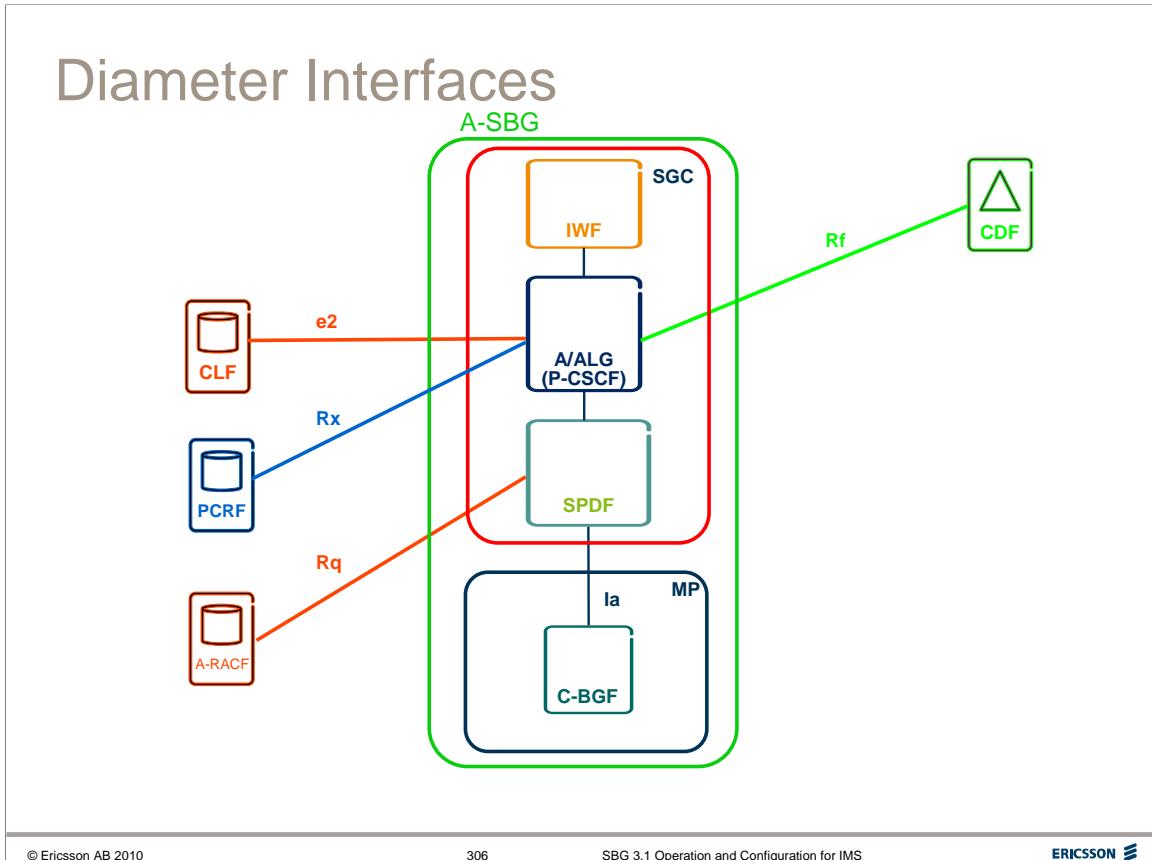
There are IP Addresses for two core (internal) DNS servers. See the figure above.

From this page there is a link, **DNS query testing**, to test the DNS connectivity and lookup results.

NAPTR, SRV and A records queries are supported.

SBG 3.1 Operation and Configuration for IMS

Diameter interfaces



DIAMETER INTERFACES

There are several Diameter Interfaces used in SBG. All are optional, depending on the services required.

Charging (Rf)

The SGC supports Diameter-based off-line charging. The SBG uses the Rf interface to report the accounting records.

Geographical Location (e2)

An A-SBG can request geographical location information for all registered clients. This information is available in the Connectivity Session Location and Repository Function (CLF) via the e2 Diameter interface.

Admission Control (Rq)

The A-SBG supports the Rq interface. The Rq interface is defined between the A-SBG and the Access Resource and Admission Control Function (A-RACF).

The Rq interface is used for the SGC to reserve media resources in the access network. The SGC can request resources, modify reserved resources during a session, and release resources at session initiation, modification and termination.

Policy control (Rx)

The A-SBG supports the Rx interface which is defined between the A-SBG and the Policy and Charging Rule Function (PCRF). The Rx interface is used for the SGC to perform authorization of the IP flows and QoS resources in the access network. The SGC can request authorization of resources, modify already authorized resources during a session and release the authorized resources.

Diameter Configuration

Session Border Gateway System

ERICSSON 

Create

[Charging IP address](#)

[Diameter realm](#)

Open

[Blade system administration](#)

[Change distinguished name prefix](#)

[Diameter realms](#)

[MP control links](#)

[Transfer configuration file](#)

[Load configuration file](#)

[Import TLS certificate](#)

[Import SIP rule sets](#)

[Export SIP rule sets](#)

Diameter Realm

A Diameter network of servers hosting the same Diameter service is identified by a 'Realm' which has the format of an FQDN.

Realms are used by Diameter proxies to route requests to the destination network.

A Diameter Realm must be configured before Diameter Instances can be configured.

Diameter Instance

A **Diameter Instance** is a server implementing a Diameter service (charging, geographical location etc.)

Create Diameter Realm

Diameter realm	Application
charging.edu.mmtel.se	Charging (Rf)
clf.edu.mmtel.se	Geographical location (e2)
aracf.edu.mmtel.se	Admission control (Rq)

Diameter Realm

To configure a Diameter Realm, go to **System → Create Diameter Realm**, the page shown in the figure above will be displayed.

Enter the FQDN **Diameter Realm** and select the **Diameter Application** for the Realm from the pull-down list of available Applications.

Charging Diameter Realms

A maximum of ten Charging Diameter Realms are supported per SGC blade system.

Charging Realms are not configured per network, these are signalled in SIP.

Configure Rf or CLF Diameter Realm

SBG - System
Diameter Realm

Diameter realm: charging.edu.mmtel.se

Application: Charging (Rf)

Reconnect timer (s):

Watchdog timer (s):

Max reconnect retries:

Diameter instances

[Blade system](#) [Peer IP address](#) [Peer port](#) [Peer protocol](#)

[Table as text](#)

[Create diameter instance](#)

Click the red triangle next to an Rf Realm or CLF Realm to display more settings, as shown above.

The changeable parameters are:

Reconnect timer

Range: 0..4294967

Defines the Reconnection Timer (frequency of retries) in seconds for a Diameter Peer connection.

Max reconnect retries

Range: 1..10

Defines the number of repeat attempts which the SGC will make to try to re-establish a Diameter Peer connection.

When the number of repeat attempts is reached, the connection peer is considered to be down.

Watchdog timer

Range: 6..294967

Defines the frequency of Diameter Watchdog requests, the Watchdog Timer for monitoring of inactive Diameter Peer Connections.

Configure Rq Diameter Realm

SBG - System
Diameter Realm

Diameter realm:	aracf.edu.mmtel.se
Application:	Admission control (Rq)
Reconnect timer (s):	<input type="text" value="30"/>
Watchdog timer (s):	<input type="text" value="30"/>
Max reconnect retries:	<input type="text" value="3"/>
Authorization lifetime (s):	<input type="text" value="1500"/>
Single phase reservation:	<input type="radio"/> true <input checked="" type="radio"/> false
Globally unique address in STR:	<input type="radio"/> true <input checked="" type="radio"/> false
Flow description support:	<input checked="" type="radio"/> true <input type="radio"/> false
Filters in flow description:	<input checked="" type="radio"/> signaling address <input type="radio"/> media address
Emergency calls	
Resource authorization:	<input type="text" value="Only QoS"/>
Continue on authorization reject:	<input type="radio"/> true <input checked="" type="radio"/> false

© Ericsson AB 2010 310 SBG 3.1 Operation and Configuration for IMS ERICSSON

Rq Diameter Realm

Clicking the red triangle next to an Rq Realm displays more settings, as shown above.

There are more parameters than for Rf & CLF, the additional parameters are A-RACF-specific and are described on the following page.

See also the ***System Service Guide 3/154 43-CNA 113 062***.

Authorization lifetime

This determines the value in seconds of the Authorization-Lifetime AVP in the initial AA-Request.

Single phase reservation

This determines if single phase reservation is to be used.

SPDF performs only ReserveAndCommit operations for resource authorization, that is, the reserved resources are available for usage as soon as they are reserved..

Globally unique address in STR

This determines if Globally-Unique-Address AVP is to be used in Session-Termination-Request (STR).

Flow description support

This determines if Media-Sub-Component AVP is to be used.

When the Media-Sub-Component AVP is used each media stream will have its own flow description, for example, bandwidth usage and so on.

Filters in flow description

This determines if signaling addresses or media addresses is to be used in AA-Requests in the Flow-Description AVPs.

Continue on A-RACF connectivity loss

Range: No, Only emergency calls or Yes

Determines whether the SGC will proceed with a call if no A-RACF is available due to connectivity loss.

Continue on A-RACF profile reject

Determines whether to proceed if A-RACF rejects the call due to QoS profile failure (Experimental-Result-Code 4045) or Access profile failure (Experimental-Result-Code 4046).

Additionally, for emergency calls, the following parameters can be specified for Rq:

Resource authorization type

Range: No, Only QoS, Only Best Effort, Best Effort at QoS reject

The attribute specifies the type of resource authorization, for example bandwidth reservation, that shall be performed by the SGC toward A-RACF for emergency calls:

Continue on authorization reject

This attribute determines if an emergency call setup will proceed even at resource reservation reject from the A-RACF server.

Create Diameter Instance

**SBG - System
Diameter Instance**

Blade system: 

Diameter realm: charging.edu.mmtel.se

Application: Charging (Rf)

Peer IP address:  

Peer protocol: TCP SCTP

Local port: 

Peer port: 

Create Diameter Instance

When a Diameter Realms has been defined, Diameter Instances (Servers) can be configured by selecting **System → Open Diameter Realm → Create Diameter Instance** for the particular Realm required.

The page shown above is displayed.

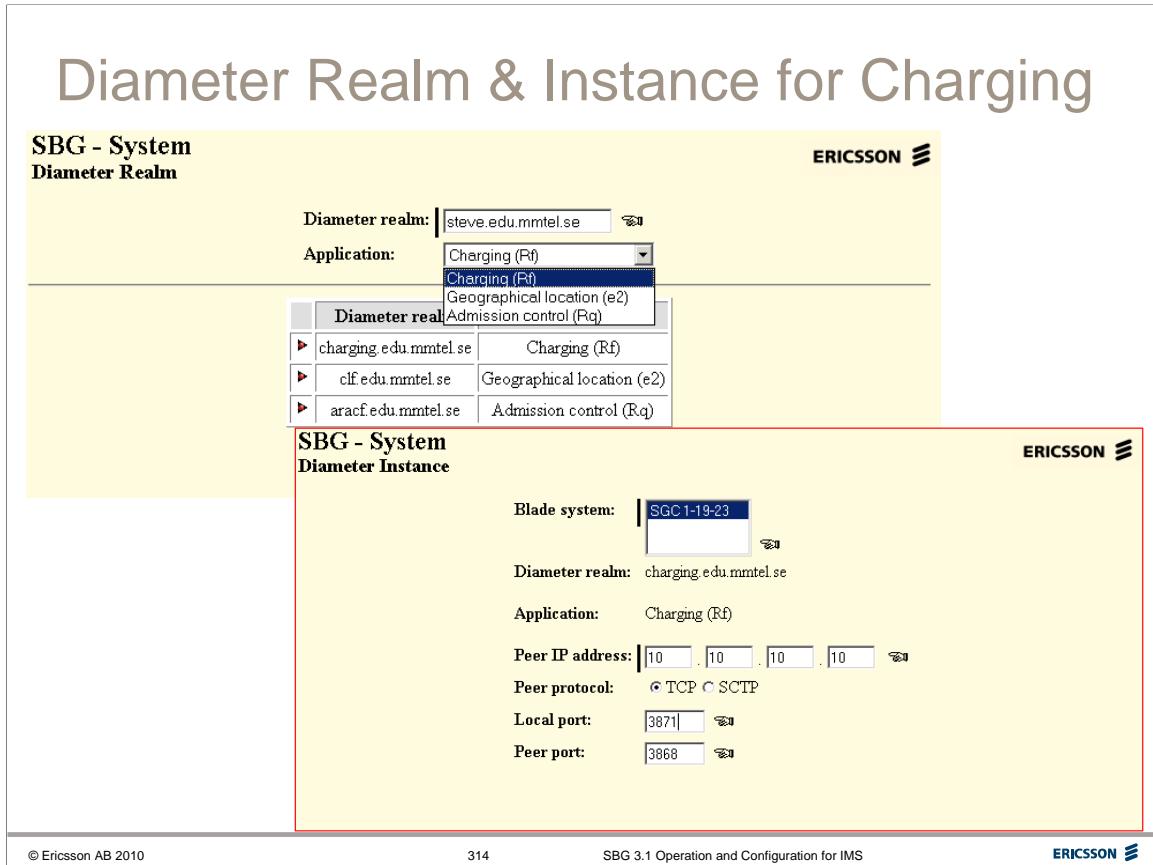
The IP Address and Port of the Diameter Server are defined; The local (SBG) Port can be specified ('0' means SGC can select); and the Transport Protocol selected.

All Rq, e2 and Rx Diameter Instances use the same source IP address in the SGC.

The **Charging Diameter Instance** uses a separate IP address (see later).

SBG 3.1 Operation and Configuration for IMS

Charging



Diameter based off-line charging

An SGC supports Diameter based off-line charging. The SGC uses the Rf interface to report the accounting records.

During periods when there is no connectivity to the Diameter server for charging data, all generated charging data is stored locally on disc. An alarm, *diameterServerAlarm* is issued per charging server.

The SBG will buffer charging data for one hour per charging server. If all selectable charging servers (obtained from P-Charging-Function-Addresses) for a session have been down for an hour, no charging will be performed, but the session continues, and new sessions will be accepted.

When the connectivity to a failing Diameter server is re-established, the stored charging data will be issued to the Diameter server in parallel with new charging data.

Diameter Realm & Instance

The *Diameter Realm* and *Diameter Instances* for the Rf interface must first be defined as described earlier.

See the figure above.

Network Configuration
IS VLANs

Viewing Latest [View Published](#)

Create IS VLAN

IS VLAN Id	Description
1	IS Internal Oam Boot VLAN
1021	Media
1047	SBG_h248
1048	SBG_mp_1_int
1050	SBG_sgc_1_int
1060	SBG_charging
1200	SBG_sg_core
1220	SBG_sg_access
3045	IS NodeDome 4.1.7 LAN
404	SBG - System
404	Charging IP Address
404	
405	
405	

Blade system: SGC 0-5_17

Charging IP address: . . .

Next hop address: . . .

Subnet mask length:

VLAN ID:

Creating the Charging IP address

A Charging VLAN must be defined in the IS and a Virtual Router for Charging defined in the ISERs.

The **System → Charging IP Address** page allows the configuration of the **Charging IP Address, Next Hop Address, Subnet mask & VLAN** for a particular SGC.

The parameters are:

- **Blade system** - The name of the SGC blade system
- **Charging IP address** - The local IP address used to send charging data from
- **Next hop address** - The next hop address used for charging data.
- **Subnet mask length** – The charging subnet for the charging IP address.
- **VLAN ID** – VLAN ID used for charging

Diameter Instance – Charging (Rf) 1

SBG - System
Diameter Instance

Blade system:	SGC 0-5_17
Diameter realm:	ee1mm01.edu.ims.se
Application:	Charging (Rf)
Peer IP address:	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="7"/> . <input type="text" value="10"/> 
Local port:	<input type="text" value="3867"/> 
Peer port:	<input type="text" value="3868"/> 
Peer protocol:	TCP
Operational state:	Disabled
Origin host:	ee1is01.edu.ims.se
Origin realm:	edu.ims.se
Peer origin host:	192.168.7.10
Peer origin realm:	ee1mm01.edu.ims.se
Successful requests:	0
Protocol errors:	0
Transient failures:	0
Permanent failures:	0

© Ericsson AB 2010 316 SBG 3.1 Operation and Configuration for IMS ERICSSON

Diameter Instance for Charging

Once the Charging IP Address has been defined, the Charging Diameter Instance page allows for more configuration of the Charging function, as shown above and on the next page.

The Diameter Instance for Rf allows the operator to *set charging on or off* and to configure a number of parameters setting the content of Accounting Requests.

The figure above shows the first part of the page, the fields display:

The Diameter Realm,

The IP address & port of the Charging Server

The Operational state of the connection to the Charging Server.

- Enabled means the Charging Server is reachable and working.

There are other non-configurable parameters and counters shown.

Diameter Instance – Charging (Rf) 2

SBG - System Diameter Instance

ERICSSON

Charging Parameters:

IBCF Charging:	<input type="radio"/> on <input checked="" type="radio"/> off
P-CSCF Charging:	<input type="radio"/> on <input checked="" type="radio"/> off
A-ALG Charging:	<input type="radio"/> on <input checked="" type="radio"/> off
ACR for Event messages:	<input type="radio"/> on <input checked="" type="radio"/> off
Charge session with no P-CFA:	<input type="radio"/> true <input checked="" type="radio"/> false
Interval reporting of Interim messages:	<input type="radio"/> true <input checked="" type="radio"/> false
Include Acct-Application-Id:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Event-Timestamp:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Event-Type:	<input checked="" type="radio"/> true <input type="radio"/> false
Include User-Session-ID:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Calling-Party-Address:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Called-Party-Address:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Time-stamp:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Inter-Operator-Identifier:	<input checked="" type="radio"/> true <input type="radio"/> false
Include IMS-Charging-Identifier:	<input checked="" type="radio"/> true <input type="radio"/> false
Include SDP-Session-Description:	<input checked="" type="radio"/> true <input type="radio"/> false
Include SDP-Media-Component:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Cause:	<input checked="" type="radio"/> true <input type="radio"/> false
Include Media-Statistics:	<input type="radio"/> true <input checked="" type="radio"/> false
Include Access-Network-Info:	<input type="radio"/> true <input checked="" type="radio"/> false
Include Served-Party-IP-Address:	<input type="radio"/> true <input checked="" type="radio"/> false
Include Session-Priority:	<input type="radio"/> true <input checked="" type="radio"/> false
Include User-Agent:	<input type="radio"/> true <input checked="" type="radio"/> false

© Ericsson AB 2010 317 SBG 3.1 Operation and Configuration for IMS **ERICSSON**

Charging Parameters

Charging can be enabled/disabled for the different SBG Roles – **A-ALG, P-CSCF and IBCF**.

ACR for Event Messages can be set on/off. i.e. after a 200 OK for a SIP Message message.

Charge Session with no P-CFA (P-Charging-Function-Address)

The selection of the charging servers is based on the SIP header **P-Charging-Function-Addresses**.

P-CFA and P-Charging-Vector (P-CV) are normally blacklisted in signalling messages to and from a Foreign Network.

The SBG supports sending accounting information to the charging servers specified in the received P-CFA. P-CFA supports two servers.

If no P-CFA is received, or if the P-CFA is removed by the blacklist, and also if the charging attribute *Charge sessions with no P-CFA* is true, a server that is up is used to report charging data.

Include

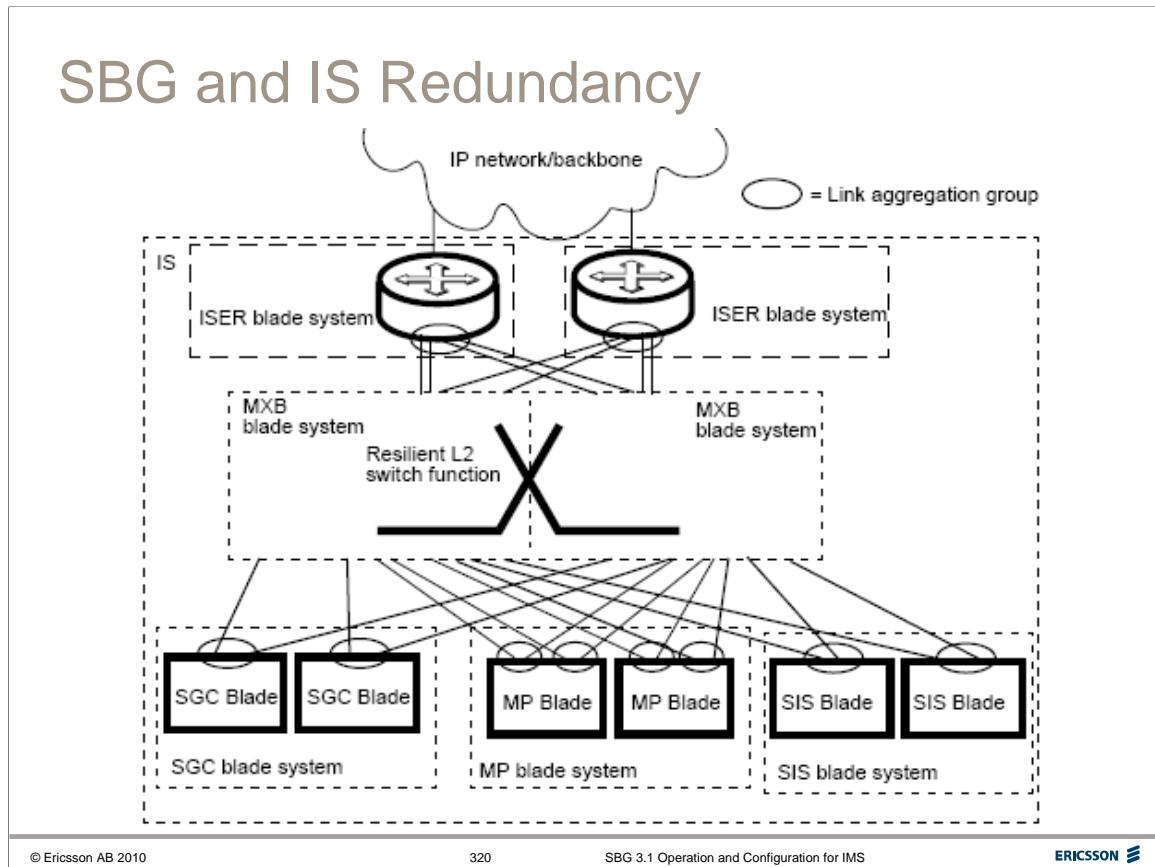
The Include fields allow a number of optional Charging AVPs to be set to be included in ACRs.

Charging Header Fields

- P-Charging-Vector in A-ALG/P-CSCF
 - The SBG 3.1 FD1 will generate a P-Charging-Vector
- P-Charging-Vector in IBCF
 - The IBCF in SBG 3.1 FD1 will generate a P-Charging-Vector even if charging is turned off.
- ICID
 - In SBG 3.1 FD1 the icid parameter generated by SBG will include either a FQDN or an IP-address

SBG 3.1 Operation and Configuration for IMS

Configure a Secure and Redundant SBG



SBG and IS Redundancy

As can be seen from the figure above, the SBG is built on the IS framework, which already has redundancy from the hardware architectural view.

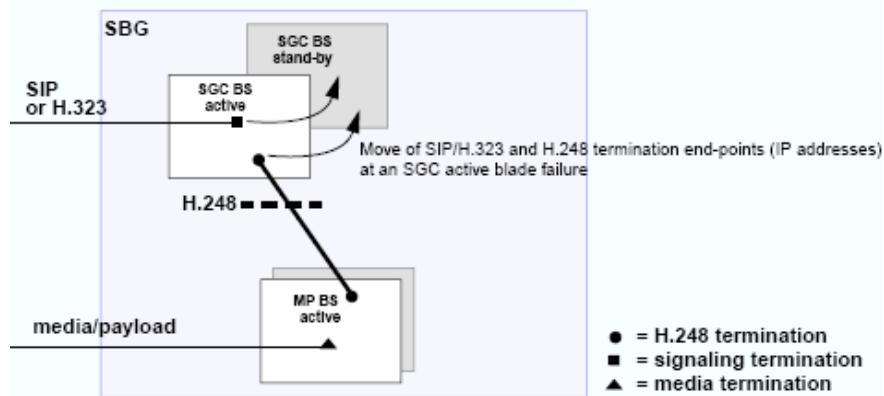
IS redundancy:

- 2 MXB blade systems
- 1 SIS blade system (2 SIS blades)
- 2 ISER blade systems
- Duplicate Gigabit Ethernet on backplane
- Duplicate power on backplane

SBG redundancy:

- 1 or more SGC blade systems (2 SGC blades each)
- 1 or more MP blade systems (2 MP blades each)

Failure of SGC Scenario

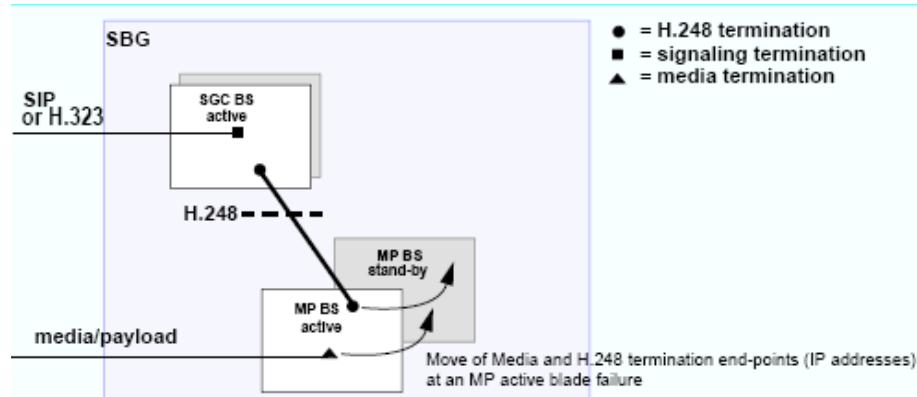


Resilience of internal interfaces

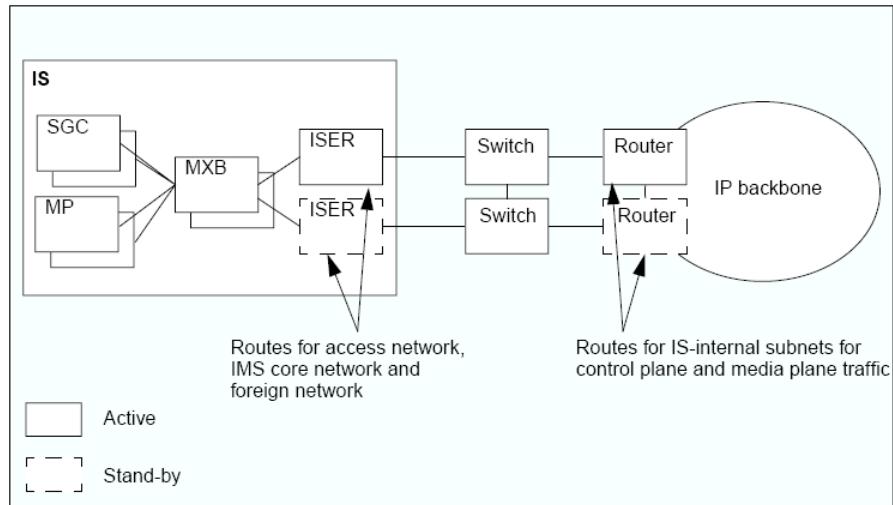
The interfaces for H.248 traffic, control plane traffic, and media plane traffic are always present on the active blade in the blade pair. If a blade changes from stand-by to active, its interfaces are activated. This can be seen in the figure above for the SGC failure scenario and figure on the next page for the MP failure scenario. Note that for the SGC and MP the interfaces have different MAC addresses. The MAC addresses are not moved. To inform all other hosts and routers on the subnet that the IP address has been moved, a gratuitous ARP request is broadcasted on the subnet.

The ISER uses the Virtual Router Redundancy Protocol (VRRP) to move the IP address and MAC address if the active ISER blade system fails.

Failure of MP Scenario



SBG site connectivity



SBG site connectivity

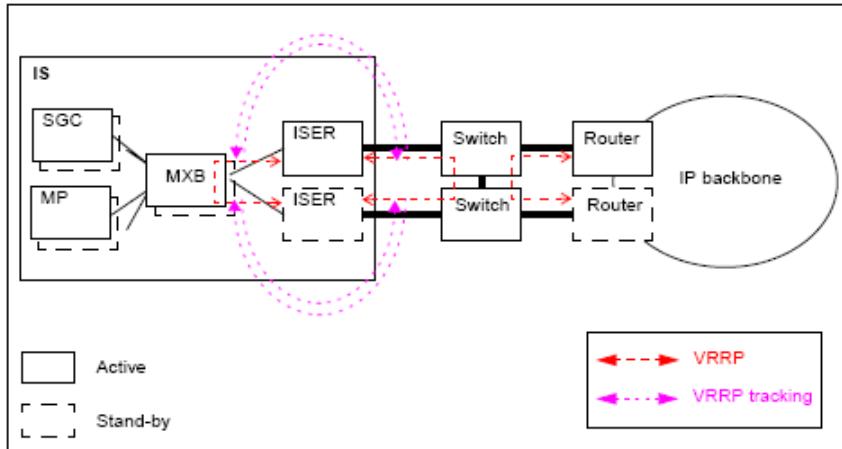
It is recommended to use static routes between the ISERs and the routers that are connected to the IP backbone.

Routes for the IS-internal subnets used for media plane traffic (if routed via ISER) and control plane traffic need to be configured on the router that is connected to the IP backbone with the ISER as next hop.

Routes per destination subnet in the access, IMS core, and foreign networks need to be configured on the ISER with the router that is connected to the IP backbone as next hop.

For the MP external interfaces, only static routes are supported. Routes per destination subnet in the access, IMS core, and foreign networks must be configured on the MP with the router that is connected to the IP backbone as next hop.

ISER Resilience



ISER Resilience

VRRP (Virtual Router Redundancy Protocol) is used by the ISER to dynamically assign the routing responsibilities to one of the ISER blade systems, the master router. In the event of a router or link failure of the master ISER, the IP address and MAC address are moved to the backup ISER. An L2 switch is required to run the VRRP protocol between the ISERs at the external side. In order to scale VRRP resiliency in the ISER for a large number of VRs, it is possible to set up several passive VRRP groups to follow one active VRRP session.

VRRP is recommended to be used on the interfaces both on the ISER and on the IP backbone router to protect against link failures and router failures. Static routes and VRRP provide faster switch-over times than the routing protocols do. Note that the support of the number of VRRPs in the IP backbone router may be limited when an SBG serves many access networks (VLANs).

The ISER also supports BFD (Bidirectional Forwarding Detection) for detection of failures in links and its peer router.

MP resilience (MP external interfaces)

A failover to the stand-by MP is based on the following criteria, in consecutive order:

- The active MP blade is down
- The stand-by MP has a higher number of operational Ethernet links
- The stand-by MP has a higher number of operational next hops.

MP resilience when the external interfaces on the MP are used

If the connection between the MP and the IP backbone router peer fails, a failover is performed if the stand-by MP offers better connectivity. A failover to the stand-by MP is based on the following criteria, in consecutive order:

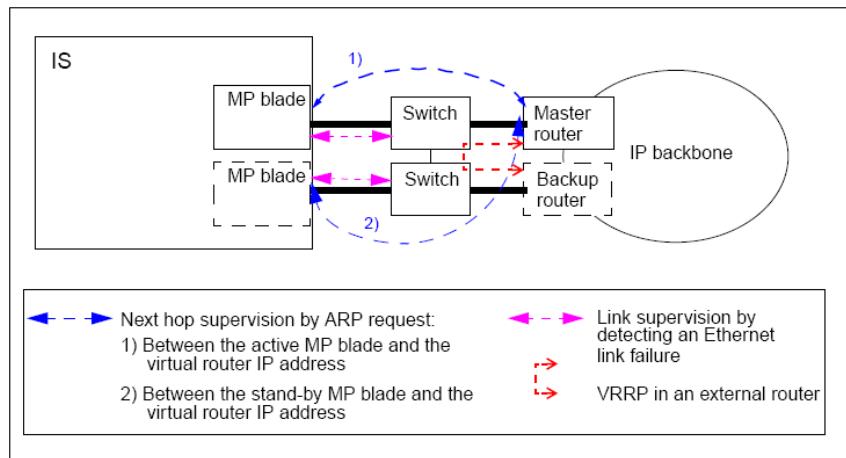
1. The active MP blade is down
2. The stand-by MP has a higher number of operational Ethernet links
3. The stand-by MP has a higher number of operational next hops.

The active and stand-by MP have additional non-moveable IP interfaces per virtual router and external interface for the purpose of supervision of the next hops towards the external networks. The next hops can be configured for fast or slow supervision.

It is possible to assign next hop groups for all next hops that, in the event of a failure, are likely to be affected by the same problem, for example if all of them use the same router port.

One next hop in a group is then configured with fast supervision and the remaining next hops are configured with slow supervision. This will reduce the rate of ARP requests in the network when having many next hops to supervise.

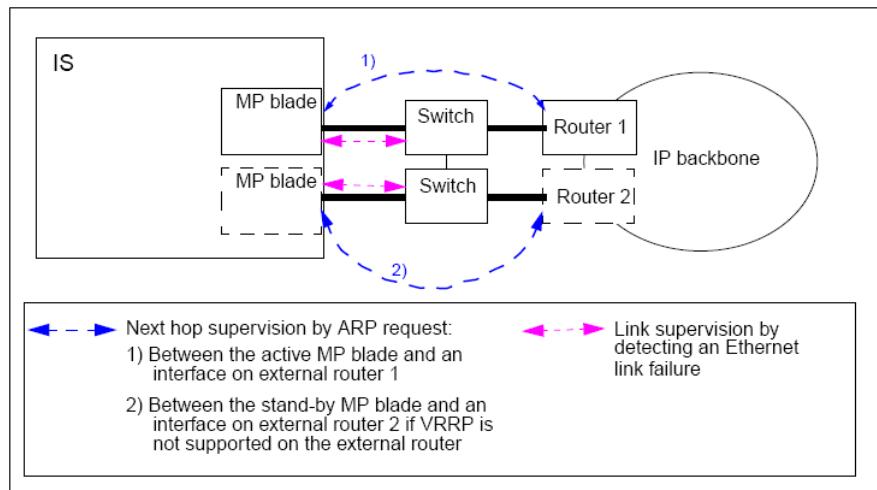
Redundancy methods in the MP



Redundancy methods in the MP for link and router failures when VRRP is applied to the external router

The figure above shows the redundancy methods supported in SBG site solutions when VRRP is applied to the external router peers. The next hops for supervision at both the active and stand-by blades must be configured to the IP interfaces on the “virtual router” (seen as a single router from the MP).

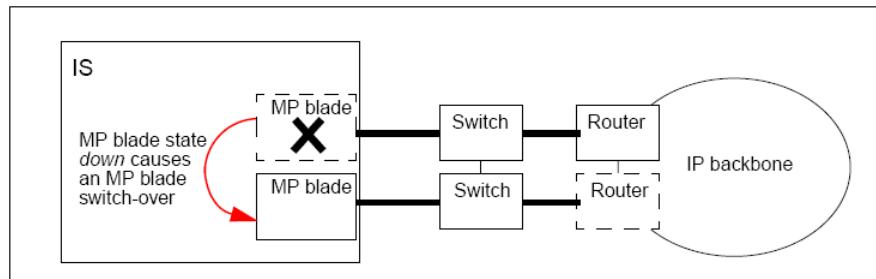
Redundancy methods in the MP for link and router failures when VRRP is not applied to the external router



Redundancy methods in the MP for link and router failures when VRRP is not applied to the external router

The figure above shows the redundancy methods supported in SBG site solutions when VRRP is not used on the external router peers. The active MP blade will supervise the next hops to one external router, and the stand-by MP will supervise the next hops to the other external router.

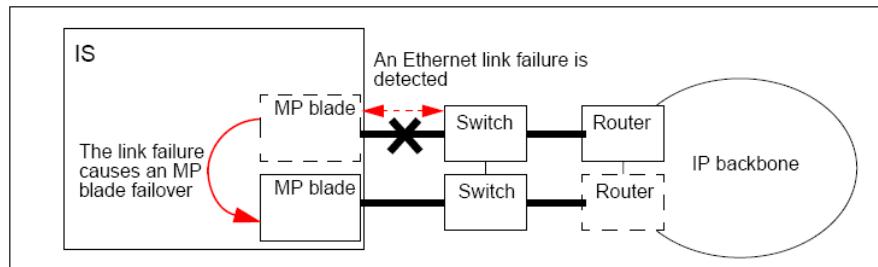
Failure scenario – MP blade down



Failure scenario – MP blade down

This is the example of a failure scenario where the active MP goes down, which will trigger a failover to the stand-by MP blade (first failover criteria).

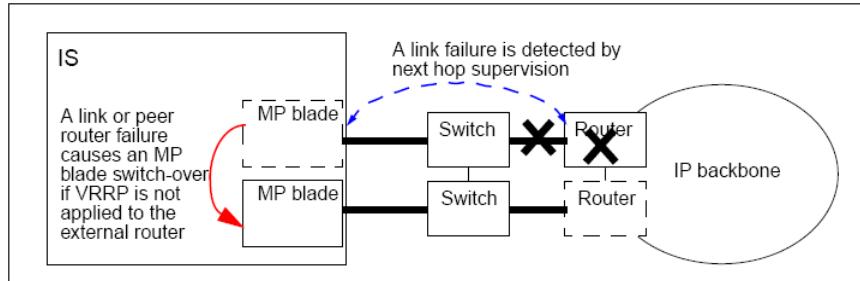
Failure scenario – Ethernet link failure



Failure scenario – Ethernet link failure

This is the example using the second failover criteria. The figure shows failure scenario where one or both Ethernet links at the active MP blade are detected as not operational, which will trigger a failover to the stand-by MP blade.

Failure scenario – remote link failure



Failure scenario – remote link failure

Finally, the figure above shows an example of a failure scenario where VRRP is not applied to the IP backbone routers, and the connectivity with the IP backbone router peer is partly or completely lost (some or all next hops with the peer are detected as lost), which will trigger a failover to the stand-by MP blade (third failover criteria).

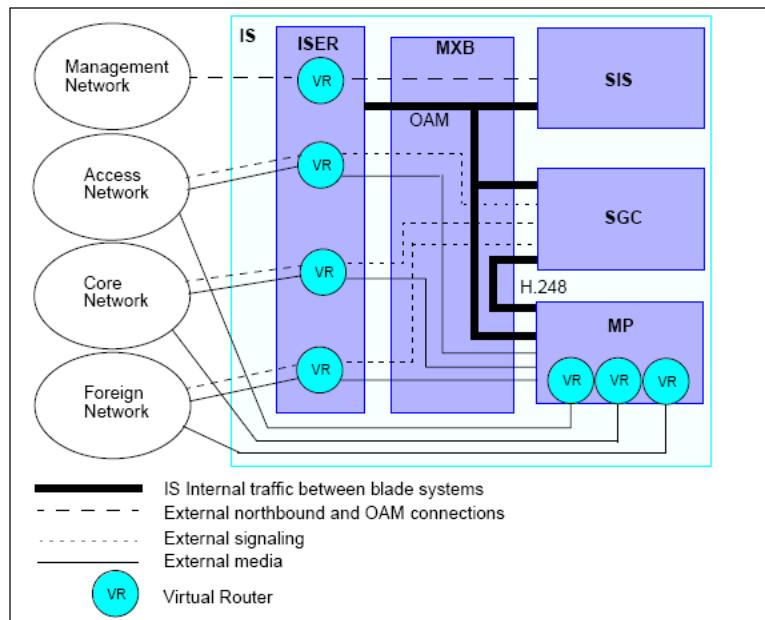
If VRRP is applied to the external routers, the failover is instead done in the IP backbone router by moving the IP addresses.

The MP blades will not detect any failure in that case and accordingly will not make a failover.

Changing the default passwords

- **ISER**
 - Create new user with privilege SecAdm
 - Change password for predefined users; sysadmin and debug
- **SIS**
 - Change predefined password of system administrator.
 - Modify expert and/or operator role
 - Create new user with expert or operator role.
 - Delete the predefined users.

Traffic Separation through VLAN



There are many ways to ensure that the SBG is secured. One of them is through traffic separation.

Traffic Separation

The different IP traffic categories are kept separated, or are separated in the ISER, before being forwarded to SGC or MP blade systems. Traffic separation prevents access from one traffic category to another, for example signalling, media and OAM traffic.

From a security point of view this traffic separation prevents direct access from one network to another (for example between different access networks or from an access network to the core network).

Traffic separation is achieved through virtual routers and virtual LANs. The main traffic categories are:

- IS internal traffic
- External management traffic
- External signalling traffic
- External media traffic
- Charging traffic (only for N-SBG)



ERICSSON