ATIS-1000026.2008(R2013)

Session Border Controller Functions and Requirements

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle – from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000026.2008(R2013), *Session Border Controller Functions and Requirements*

Is an American National Standard developed by the **Signaling, Architecture, and Control (SAC)** Subcommittee under the **ATIS Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

(R2013)

ATIS-1000026.2008

SESSION BORDER CONTROLLER FUNCTIONS AND REQUIREMENTS

Alliance for Telecommunications Industry Solutions

Approved April 9, 2008

American National Standards Institute, Inc.

Abstract

This Standard defines the Session Border Controller (SBC) functions and requirements that reside within a service provider's network. Implementation realizations of SBCs are also described. An SBC comprises of Call Control Signaling Path (CCSP) functions and Media Path (MP) functions. The separation of an SBC into its component functions is described; and call/session control, bearer/media, and OAM&P requirements are provided. In addition, the CCSP and MP functions are mapped onto the ATIS NGN Architecture (described in ATIS-1000018).

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following roster:

J. Zebarth, PTSC Chair (Nortel)

V. Shaikh, Technical Editor (Telcordia)
M. Dolly, Technical Editor (AT&T)
C. Underkoffler, ATIS Chief Editor

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

American National Standard
for Telecommunications –

Session Border Controller Functions and Requirements

1 INTRODUCTION

In existing VoIP networks, Session Border Controller (SBC) functions, have already been introduced for network interconnection of NGN/IP networks. SBCs can play a role in VoIP services by controlling borders to resolve multiple VoIP-related problems such as Network Address Translation (NAT) or firewall traversal. SBCs are already being used in existing VoIP service networks and thought to be essential in the Next Generation Network (NGN) architecture.

There are various implementations and deployments of SBCs that perform functions in service provider, enterprise, access and end-user (home) networks, however most are vendor specific, thereby causing interoperating problems and hence increasing implementation costs time to market. Defining common and agreed upon carrier requirements for these functions and for mapping these functions to physical implementations is of paramount importance to allow for vendor product interoperability and facilitate carrier network interconnection.

2 SCOPE, PURPOSE AND APPLICATION

This Standard defines the Session Border Controller (SBC) functions and requirements that reside within a service provider's network. The functions performed depend on the interface supported.

The following interfaces are supported by an SBC located within a Service Provider's Network:

- To another Service Provider;
- To an Enterprise Network;
- To a Transit Network;
- To a Residential Customer Network;
- To an Access Network;
- To an Application Network.

This Standard defines the SBC functions and requirements for the above interface types. The physical realization of the functions will vary depending on implementations and deployments. The unification and/or distribution of the functions will depend on scale, operational and application needs.

The SBC functions include (but are not limited to):

- Access admission and resource policy enforcement
- Firewall
- Topology hiding
- Traffic monitoring and shaping
- QoS marking and mapping
- Priority marking and mapping
- Protocol normalization and or repair
- Protocol interworking (e.g., SIP and H.323)
- IPv4/IPv6 interworking
- Signaling transport protocol interworking
- NAT traversal
- Transcoding and DTMF interworking
- Media and/or call/session control signaling encryption and decryption
- Support of Lawful Intercept
- Support of Emergency Telecommunications Service (ETS)
- Authentication, Authorization and Accounting (AAA)
- Privacy and Identity control
- VPN bridging or mediation
- Protect against DoS attacks
- User/endpoint registration.

The main sections of the document are:

- Section 6, Deployment Area: defines logical relationships at the call/session control and bearer/media layers.
- Section 7, SBC Functions: defines the functions related to the call control signaling path and media path.

- Section 8, SBC Requirements: define the requirements on the functions independent of the physical realization.
- Section 9, Composition of SBCs: provides the rationale for SBCs.
- Section 10, Mapping to ATIS NGN Architecture: identifies the architecture functional entities that perform SBC functions for the media and signaling paths.

3 NORMATIVE REFERENCES

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

3.1 ATIS References[1]

- ATIS-1000009.2006, IP Network-to-Network Interface (NNI) Standard for VOIP
- ATIS-1000018.2007, ATIS NGN Architecture.
- ATIS-1000020, ETS Packet Priority for IP NNI Interfaces – Requirements for a Separate Expedited Forwarding Mechanism.
- ATIS-1000678.2006,, Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2.

3.2 ITU References[2]

- Supplement 1 to ITU-T Recommendation Y.2012, Session/Border Control (S/BC) Functions.
- ITU-T Recommendation H.323, Packet-Based Multimedia Communications Systems.
- ITU-T Recommendation H.248, Gateway Control Protocol.

3.3 IETF References[3]

- RFC 3261, SIP: Session Initiation Protocol.

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[2] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[3] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

- RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP).

4 DEFINITIONS

Border B2BUA: A border back-to-back user agent (B2BUA) is a SIP B2BUA that performs IP network border functions in its reformulation of SIP messages. These functions include NAT/NAPT editing of IP address, port number of the call/session, and application content of SIP messages. They may also include media relay resource assignments with corresponding execution of control functions that establish NAPT building in the media relay.

CAC (Connection/Call Admission Control): CAC is the set of actions taken by a network during the call/session set-up phase in order to determine whether a connection request should be accepted or rejected.

DoS (Denial of Service): DoS is the prevention of authorized access to resources or the delaying of time-critical operations, or the result of any action or series of actions that prevents any part of an information system (IS) from functioning.

Firewall: A system designed to protect a network from unauthorized access.

NAT: Network Address Translation (NAT) is a method of converting one IP address space to another IP address space. It is primarily used to interface the internal (private) IP address space of a network with the global (public) address space of the Internet.

NAPT: Network Address and Port Translation (NAPT) is a method of converting one IP address space and port number to another IP address space and port number. It is primarily used to interface the internal (private) IP address space/port number of a network with the global (public) address space/port number of the internet.

NNI (Network to Network Interface): NNI is the border interconnection between two carriers.

UNI (User to Network Interface): UNI isthe border interconnection between the carrier and its customers.

Session Border Controller (SBC) Functions: SBC functions is a set of functions that enables interactive communication across the borders or boundaries of disparate IP networks.

It provides calls/sessions of real-time IP voice, video and other data across borders between IP networks and provides control over security, quality of service, service level agreements and other functions using IP signaling protocols.

SIP B2BUA: A SIP back-to-back user agent (B2BUA) is a concatenation of a SIP User Agent Client (UAC) and User Agent Server (UAS).

The IETF defines the B2BUA in RFC 3261 as “a logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its’ behavior”. (UAC and UAS behavior is defined in RFC 3261.) A B2BUA reformulates messages before sending them as new requests.

Transcoding: Transcoding refers to the conversion of a data stream from one format to another. Examples include conversion from one codec standard (e.g., G.711, G.729) to another, or from one video compression standard (e.g., MPEG-1, H.264) to another.

5 ABBREVIATIONS

This document uses the following abbreviations:

AAA	Authentication, Authorization, and Accounting
A-BGF	Access Border Gateway Function
ANI	Application Network Interface
AS	Application Server
ATIS	Alliance for Telecommunications Industry Solutions
B2BUA	Back-to-Back User Agent
BFE	Bearer Functional Entity
BGCF	Breakout Gateway Control Function
BGP	Border Gateway Protocol
CAC	Call (or Connection) Admission Control
CC	Call Content
CCFE	Call Control Functional Entity
CCSP	Call Control Signaling Path
CDR	Call Data Record
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSP	Data Services Platform
DTMF	Dual Tone Multiple Frequency
ETS	Emergency Telecommunication Service
GW	Gateway
HSS	Home Subscriber Server
I-BGF	Interconnection Border Gateway Function
I-CSCF	Interrogating Call Session Control Function
IBCF	Interconnection Border Control Function
ID	Identifier
IETF	Internet Engineering Task Force
IMS	Internet Protocol (IP) Multimedia core network Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISUP	ISDN User Part
IWF	Interworking Function
MGCF	Media Gateway Control Function

MIME	Multipurpose Internet Mail Extension
MP	Media Path
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MS	Media Server
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NGN	Next Generation Network
NNI	Network to Network Interface
OAM&P	Operations, Administration, Maintenance, and Provisioning
PAI	P-Asserted Identity
P-CSCF	Proxy Call Session Control Function
PDF	Policy Decision Function
QoS	Quality of Service
QSIG	Q Signaling protocol
RFC	Request for Comments
RTP	Real time Transport Protocol
SCIM	Service Capability Interaction Manager
S-CSCF	Serving Call Session Control Function
SBC	Session Border Controller
SAC	Session Access Control
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SGF	Signaling Gateway Function
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLF	Subscription Locator Function
SNMP	Service Network Management Protocol
SS7	Signaling System number 7
T-MGF	Trunking Media Gateway Function
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
UNI	User to Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network

6 DEPLOYMENT AREA

Figure 1 illustrates the location of the SBC Call Control Signaling Path (CCSP) functions and Media Path (MP) functions. There is a need for different functions, e.g., at the customer edge, between the access network and a core network, between transit networks, and between service provider core networks. At the customer edge, either at the customer side or at the network entrance, the SBC provides functionality on behalf of the customer, such as protecting the customer, hiding the customer's IP address and enforcing QoS. This is also applicable for enterprise customers. Between the access network and the core network, the SBC provides functionality on behalf of each network segment (independent of access technology) such as the access network and the service provider core network. Between service provider core networks, it provides functionality on behalf of each service provider's core network.

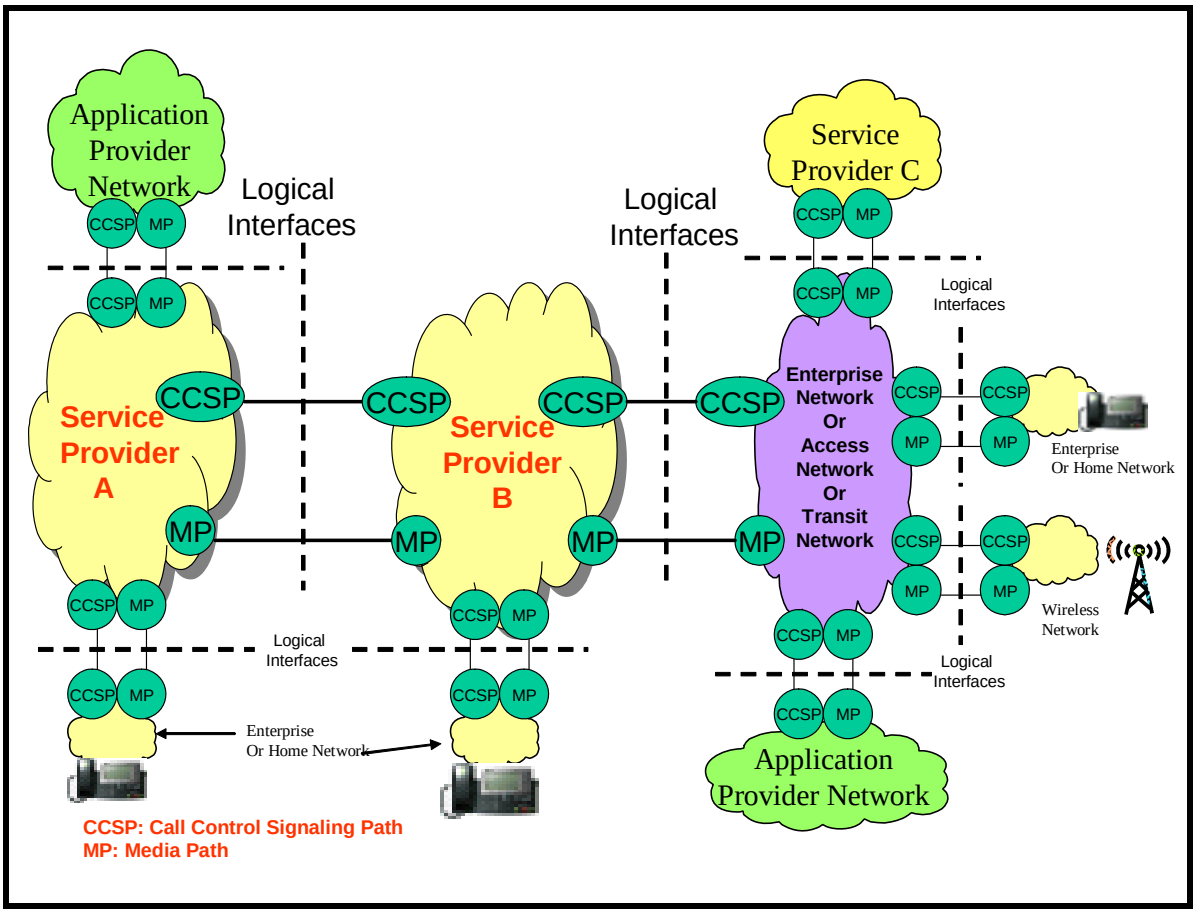


Figure 1 - Locations of SBC Functions

7 SBC FUNCTIONS

The SBC MP functions and SBC CCSP functions are listed below.

7.1 Functions Related to Media Path

The following functions are related to the SBC MP:

– *VPN bridging or mediation*

- Allows the connection or bridging of different types of VPNs to enable media packets to pass through. Signaling packets may be interrupted in order to control media packets. Specific mechanisms for this function depend on VPN types and interconnection patterns.

– *Opening and closing of a pinhole (firewall)*

- Triggered by signaling packets, a target IP flow is identified by "5-tuples" (i.e., source/destination IP addresses, source/destination port number and protocol identifier) and the corresponding pinhole is opened to pass through the IP flow.

– *Policing and marking*

- Conformance checking of the IP flow against the traffic contract.
- Policing or rate limiting of the IP flow up to the limits defined in the traffic contract.
- Packet marking for overflow traffic of the IP flow.
- Traffic shaping to reduce burstiness.
- Packet marking by overriding the allocated traffic class regardless of the incoming class.

– *Detection of inactivity*

- Metering the target IP flow traffic and detecting an inactive period which may result in signaling-related functions to terminate the call/session.

– *NAT and NAPT*

- Rewriting source/destination IP addresses as well as source/destination port number in case of NAPT.

– *Assisting remote NAT/NAPT traversal*

- Performing an agent function to make the target IP flow pass through a remote NAT/NAPT.

– *Resource and admission control*

- For links directly connected to the element, and optionally networks behind the element, resource availability is managed and admission control is performed for the target call/session.

– *IP payload processing*

  - Transcoding (e.g., between G.711 and G.729) and DTMF interworking.

– *Performance measurement*

  - Quality monitoring for the target IP flow in terms of determined performance parameters, such as delay, jitter and packet loss. Performance results may need to be collected for aggregated IP flows.

– *Denial of service (DoS) detection and protection*

  - Detection of unusual incoming IP packets which may then be blocked to protect the intended receiving user or network.
  - To prevent distributed denial of service (DoS) attack, destination specific monitoring, regardless of the source address, may be necessary.

– *Media encryption and decryption*

  - Encryption and decryption of media streamd (e.g., IPSec).

– *Support for Emergency Telecommunications Service (ETS)*

  - Identification of ETS traffic and priority handling for the IP flows of ETS traffic.
  - Conformance checking and mapping (if applicable) of priority marking based on policy for ETS communications.
  - Enforcement of security functions to protect ETS communications based on policies. For example, authenticating source for handing off and receiving traffic for ETS communications.

– *Support for emergency calls/sessions*

  - Identification of emergency call/session and priority handling for the IP flows of emergency call/session traffic.
  - Conformance checking and mapping (if applicable) of priority marking based on policy for emergency calls/sessions.
  - Transfer of an emergency call/session to an emergency call/session handling system.

– *Support for lawful intercept*

  - Capturing media streams.

– *Security control*

  - *Enforcement of security policy for media.*

7.2 Functions Related to Signaling Path

The following functions are related to the SBC CCSP:

– *Traffic control for signaling messages*

  - Restriction of call/session establishment in case of signaling-level congestion.
  - Load balancing among receiving or target servers.

– *Authentication, Authorization and Accounting (AAA)*

  - User/endpoint, customer gateway and network element authentication and authorization.
  - Session admission control.
  - Detail record generation for a call/session.

– *Signaling protocol translation*

  - Translation of signaling protocol including protocol normalization, and repair.

– *Signaling protocol interworking*

  - SIP and H.323 protocol interworking.
  - Termination and generation of different signaling transport protocols such as TCP and UDP.
  - Interworking at IP layer such as between IPv4 and IPv6.

– *Call/session-based routing*

  - Call/session-based routing – Ability to assign calls/sessions to servers in the case of point-to-multipoint transmission.
  - Call/session routing – Ability to assign a call/session to a route in the case that it crosses multiple operators.
  - User/endpoint registration – Ability to assign user/endpoint registration request to a server.

– *DSP service control*

  - Codec negotiation – Determination of a common codec based on the codec of the initiating User Equipment (UE) and of the called UE. If a common codec cannot be found, then the DSP service control function requests a suitable codec from either local DSP resources or a regional transcoder media server.
  - Media relay interworking - DTMF telephone event relay is commonly used and relay mechanisms are also defined for other signaling and media types. Where one UE requests a relay mechanism but the other UE does not support this, then the DSP service control function may request interworking from either local DSP resources or a regional interworking function.
  - Control of lower-layer service – Determination of bandwidth requirements to support the chosen codec. Forwarding bandwidth and priority requirement of the call/session to the Admission Control Function in the Media Plane.

– *End-user information hiding*

- Hiding identity and address.

– *Topology and infrastructure hiding*

- Hiding information included in the signaling message.

– *DoS protection*

- Protecting the control plane from DoS attacks.

– *Signaling encryption and decryption*

- Encryption and decryption of signaling stream (e.g., IPSec).

– *Support for ETS*

- Identification of ETS signaling and priority handling for the ETS call/session set-up based on policy for ETS signaling.
- Verifying and conformance checking, and mapping (if applicable) of priority information based on policy for ETS signaling.
- Enforcement of security functions to protect ETS signaling based on policies. For example, authenticating source for handing off and receiving ETS signaling.

– *Support for emergency calls/sessions*

- Identification of emergency call/session signaling and priority handling for an emergency call/session set-up based on emergency call/session policy .
- Analyze the caller's geographical information and transfer it to the emergency call/session handling system to locate the caller's position.

– *Support for lawful intercept*

- Capturing call/session control signaling.

– *Security control*

- Enforcement of security policy for call/session control signaling.

8 SBC REQUIREMENTS

This section defines specific detailed requirements associated with the call/session control and bearer/data functions. A requirement for a function shall be the same independent of the physical realization of the function (except where noted).

8.1 Requirements related to the Call Control Signaling Path

- Access Admission Control and Resource Policy Enforcement: The SBC shall support access admission control and resource policy enforcement based on user profiles (e.g., authentication at UNI and IP Sec based token passing at NNI) and interaction with Resource Access Control Functions (RACFs).

The access control function shall make it possible for a carrier to restrict and control access to its network.

- Topology Hiding: The SBC shall support topology hiding to allow service providers to hide internal network configuration, capacity, topology and routing information to outside parties.

  Topology hiding is a general networking technique that hides the IP addresses of end points in a network from elements of a peer network. When topology hiding is performed, new call/session IDs shall be generated and SIP headers shall be modified to prevent any protected IP addresses and route information to be transmitted to external peers.

- Topology Hiding: The SBC shall support topology hiding of any SIP calls/sessions by:

  o Removing or encrypting SIP Via header list for outgoing SIP requests.

  o Removing or encrypting SIP Record-Route headers for outgoing SIP requests and responses.

  o Removing or encrypting Route headers for outgoing SIP requests.

  o Removing or encrypting Service-Route headers for outgoing SIP responses.

  o Performing NAT/NAPT function by rewriting the source/destination IP addresses in the case of NAT and as well as source/destination port numbers in the case of NAPT.

- Firewall: The SBC shall inspect incoming signaling messages to instruct the bearer (data) function to open and close pinholes as needed for the media stream.

- Protection Against DoS Attacks: The SBC shall protect against VoIP specific and general DoS attacks, on VoIP network elements.

- SIP Protocol Normalization: The SBC shall support SIP/SDP Protocol normalization and/or repair, including adjustments of encodings to a core network profile. This may be done in order to facilitate backward compatibility with older devices that may support a deprecated version of SIP/SDP. For example, it is necessary to rewrite the Party ID of older protocol stacks with PAI (P-Asserted Identity) for RFC3262 compliance.

- NAT and NAPT Traversal: The SBC shall perform NAT traversal for authorized calls/sessions using the SIP, H.323 and H.248 protocols. The SBC must be able to recognize that a NAT or NAPT has been performed on Layer 3 but not above and correct the signaling messages for SIP, H.248, H.323 protocols.

- IPv4/IPv6 Interworking: The SBC shall enable interworking between networks utilizing IPv4 and networks using IPv6 through the use of dual stacks, selectable for each SBC interface. All valid IPv4 addresses and parameters shall be translated to/from the equivalent IPv6 values. An example of this interworking is the modification of the SIP headers (e.g, R-URI, To:, From:, Via, Contact, etc.).

- Signaling Transport Protocol Support: The SBC shall support SIP over the following protocols: TCP, UDP, TLS-over-TCP, and SCTP. Protocols supported must be selectable for each SBC interface to external systems. These transport layer protocols are generated and terminated at each interface to external systems (i.e., there is no “pass-thru” of transport layer information).

- VPN Bridging or Mediation: The SBC shall support terminating the publicly routable IP signaling received from a foreign carrier onto the private VPN address space used by the carrier in its internal network. The SBC shall support Back to Back User Agent functions to enable the VPN bridging.

- Call/Session Signaling Message Mirroring in Support of Lawful Intercept (LAES, CALEA support): The SBC shall support the mirroring (i.e., replication) of call/session signaling messages (CII – Call Identifying Information) so that a copy can be sent to a LAES device (CII Delivery Function - see ATIS-1000678) in a manner undetectable by the end user.

- QoS/Priority Packet Markings: The SBC shall be capable of populating the layer 2 and layer 3 headers/fields, based on call/session type (e.g., ETS) in order to facilitate priority routing of the packets. Refer to LB S093, ETS Packet Priority for IP NNI Interfaces – Requirements for a Separate Expedited Forwarding Mechanism for the details on the markings based technology.

- ETS: The SBC shall be capable of identifying, marking, and processing with priority an ETS call/session.

- Identity Control: The SBC shall be capable of:

    - Honoring privacy if the calling/called numbers are restricted;

    - Remove the ISUP MIME body on a per route/address basis.

- Routing: The SBC shall support layer 4 routing based on call/session control information.

- Authentication and Authorization: The SBC shall support authentication and authorization functions.

- Call Detail Recording: The SBC shall be capable of producing CDRs based on call/session control information (e.g., SIP/SDP). These CDRs can be used to manage the network and for SLA auditing.

- IPv4/IPv6 Interworking: The SBC shall perform IPv4/IPv6 IP address translation. The IPv6 network is responsible for performing the address translation.

- Transcoding: The SBC shall support transcoding.

- Encryption: The SBC shall support encryption.

- Security Control: The SBC shall enforce security policy for call/session control signaling across UNIs and NNIs.

8.1 Requirements related to the Media Path

- Access Admission Control and Resource Policy Enforcement: The SBC shall support access admission control and resource policy enforcement for directly connected links, and optionally for networks that are not directly connected.

- Access Admission Control and Resource Policy Enforcement: The SBC shall support bandwidth allocation based on access admission control and resource policy enforcement.

- Access Admission Control and Resource Policy Enforcement: The SBC shall support Call Admission Control (CAC) functions and Session Admission Control (SAC) functions based on either bandwidth restriction and/or on maximum number of simultaneous calls/sessions restrictions and on either an interface or logical group basis.

    - The SBC shall monitor the total rate of all incoming requests, from and to any endpoint.

    - Each SBC shall be configured with a maximum permissible rate and it shall reject additional requests that would cause it to exceed the rate limit, thereby preventing network congestion and DoS and DDoS attacks.

    - The SBC shall support configuration of rate limit of VoIP signaling messages (e.g., Notify messages), either per call/session/port/subscriber/group of subscriber/network/customer VPN or a global limit.

    - The SBC shall support configuration of rate limit per message type, either per call/session/port/subscriber/group of subscriber/network/customer VPN or a global limit.

    - The SBC shall support configuration with maximum concurrent call/session limit to prevent total network resource use from exceeding the maximum capacity, and to prevent subscribers from exceeding their SLAs. The limit can be based on per call/session/port/subscriber/group of subscriber/network/customer VPN or a global limit.

- Access Admission Control and Resource Policy Enforcement: The SBC shall monitor bandwidth usage and availability and inform the Call/Session Admission Control (C/SAC) function.

- Access Admission Control and Resource Policy Enforcement: At minimum, the SBC shall support access control based on IP address of the incoming packet. In addition, resource policy enforcement may be applied.

- Access Admission Control and Resource Policy Enforcement: The SBC shall always permit emergency service calls/sessions to terminate.

- Topology Hiding: The SBC shall support topology hiding, performing NAT/NAPT function by rewriting the source/destination IP addresses in the case of NAT and as well as source/destination port numbers in the case of NAPT.

- Firewall: The SBC shall support the opening and closing of pinholes for media streams based on instructions from call/session control firewall function.

- Firewall: The SBC will support identification and call admission control of a target IP flow. The IP flow is identified by “5-tuples”, e.g., source/destination IP addresses, source/destination port number and protocol identifier. The corresponding pinhole is then opened to allow the pass through of the IP flow.

- Protection Against DoS Attacks: The SBC shall support DoS detection by screening/filtering unusual/suspicious incoming IP packets so that they do not reach intended receiving users/elements/interfaces.

- Protection Against DDoS Attacks: The SBC shall support DDoS detection by destination specific monitoring, regardless of the source address.

- NAT and NAPT Traversal: The SBC shall open and close "pinhole" for media via signal control. The SBC shall ensure that the pinhole is closed at the end of a call/session.

- Call/Session Managed Media Control: The SBC shall always anchor the media when the originating and terminating parties are across peer networks. Media for calls/sessions across peer networks should always pass through the SBC to enable establishing paths between the peer networks, for which SLAs may be created.

- Call/Session Managed Media Control: The SBC shall allow the carrier network to assign a pool of RTP ports to enable the networks to manage the media traffic across peer networks.

- Call/Session Managed Media Control: The SBC shall be capable of marking media packets with the proper QoS markings to receive voice-grade QoS in SBC's network. The SBC shall have the capability to independently mark incoming media packets and outgoing media packets as per the requirements/expectations of the receiving carrier.

- Call/Session Managed Media Control: The SBC shall police the bandwidth on each individual flow so that it only consumes the bandwidth and QoS indicated in the call/session signaling.

- Call/Session Managed Media Control: The SBC shall monitor RTP media-stream quality and collect RTCP reports from the two UEs. The two sets of local statistics and the two sets of remote statistics, if available, shall be provided to the Call/Session Control Function for insertion into the CDR.

- Data Mirroring in Support of Lawful Intercept: The SBC shall support the mirroring (i.e., replication) of call/session data (CC – Call Content) so that a copy of this call/session data can be sent to a LAES device in a manner undetectable by the end user.

- QoS/Priority Packet Markings: The SBC shall be capable of populating the layer 2 and layer 3 headers/fields, based on call/session type (e.g., ETS) in order to facilitate priority routing of the packets.

  Refer to ATIS-xxxxxxx.2007, ETS Packet Priority for IP NNI Interfaces – Requirements for a Separate Expedited Forwarding Mechanism for the details on the markings based technology.

- ETS: The SBC shall provide priority IP transport for ETS signaling and bearer/media traffic.

- Transcoding: The SBC shall support transcoding.

- Encryption: The SBC shall support encryption.

- Security Control: The SBC shall enforce security policy for media streams across UNIs and NNIs.

8.3 Requirements related to OAMP

- Access Admission Control and Resource Policy Enforcement: A management function or tool shall be required to verify CAC/SAC policy between two different SBCs.
- Access Admission Control and Resource Policy Enforcement: SLAs shall be verified between SBCs.
- Firewall: The SBC shall report the pinhole management reporting and call/session debugging results to a management tool. The tool shall be able to provide mapping of a media IP address and port combination on the ingress interface to a media IP address and port combination on the egress interface.
- Reporting of DoS Attacks: The SBC shall report DoS attacks on a periodic basis to a data collection entity.
- Reporting of DDoS Attacks: The SBC shall report DDoS attacks on a periodic basis to a data collection entity.

9 COMPOSITION OF A SBC

The separation of SBC functionality is appropriate and necessary for several reasons:

- In the ATIS NGN architecture (as defined in ATIS-1000018), there is a need for multiple functions (instantiated in multiple devices) to control the media portion of the SBC function. In particular, the Interconnection Border Control Function (IBCF) and the Policy Decision Function (not shown in Figure 4 between interconnecting networks) will both need to interface with the Interconnection Border Gateway Function (I-BGF). In addition, there may be a need for the Media Server and Proxy Call Session Control Function (P-CSCF) to interface with the I-BGF for SBC functions. Similar considerations govern the Access Border Gateway Function (A-BGF) and its relationship to the P-CSCF. A fully integrated SBC would complicate this interworking.
- Signaling interworking may be separate from the SBC because it will not be required in many network scenarios. When it is required, there will be a need for the network to determine, before call/session set up completion, the type of signaling interworking that is required. In addition, as networks evolve, it is likely that the need for signaling interworking will decrease over time. Because of this, it must be possible to flexibly insert signaling interworking functionality into the call/session initiated by the IBCF.
- Initial deployments of NGN networks may find an integrated approach to SBC a useful mechanism to satisfy all initial architectural requirements. As NGN networks expand, separation of the various functional entities related to SBC will allow networks to scale more efficiently, especially when the requirements for signaling/control functions and media functions evolve independently.

SBC functions can be logically split into two types: signaling-related functions and media-related functions. According to whether these functions are co-located or not, it can be considered that there are two different models: the unified model and the distributed model. Figure 2 illustrates the two different models.

1) Unified model: This model includes both signaling-related functions and media-related functions which co-reside within the same physical component. Hence the relationship between signaling-related functions and media-related functions is 1:1.

2) Distributed model: The two functions are separated with a protocol as the interface between them. The relationships between the two functions are 1:N, N:1, N:M.

   - The 1:N configuration should be considered in cases of redundant configuration for media-related functionality that assumes synchronization of a pair or set of media-related functions.
   - In case of the N:1 configuration, a single media-related function is controlled by multiple signaling functions. This allows multiple accesses to a single media resource from different types of signaling or application-specific functions.
   - The N:M configuration allows for multiple media-related functions to be controlled by multiple signaling functions; a signaling-related function is selected depending on the status of the multiple signaling-related functions. Once one signaling-related function is selected, it will determine which media-related function is served for that signaling-related function. This configuration is the most reliable configuration among the three distributed models. However, it requires considerably more sophisticated technology to determine which signaling-related function and media-related function will be served.

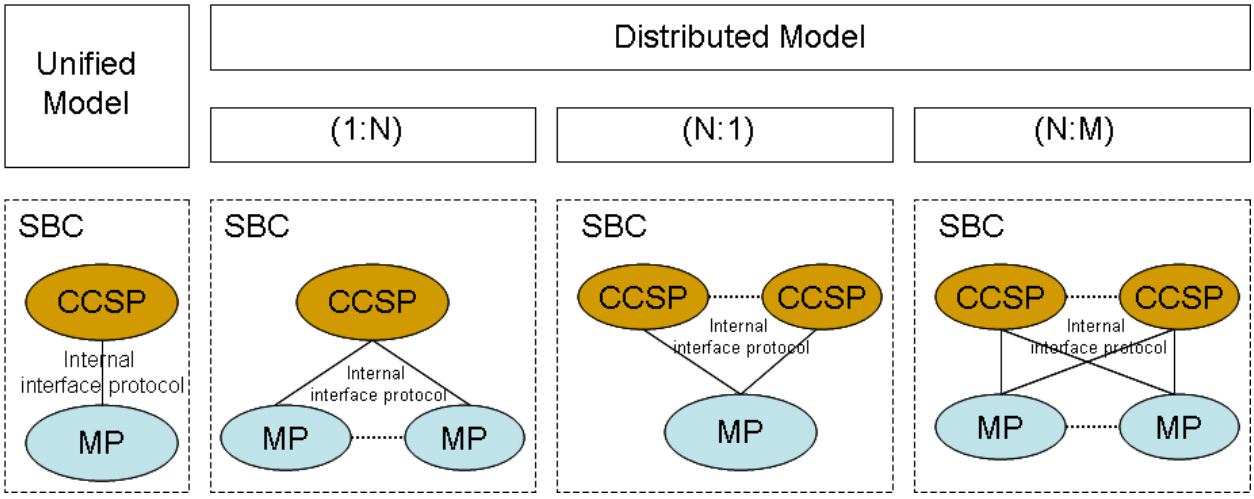


Figure 2 - Two models of SBC

10 MAPPING TO ATIS NGN ARCHITECTURE

Figure 3 illustrates three types of SBC functionally, depending on its location:

1) SBC-CA (customer to access SBC): SBC-CA is located at the customer edge, either at the customer side or at the access network entrance. It provides functionality on behalf of the customer, such as protecting the customer, hiding the customer's IP address, and enforcing QoS. It is applicable for enterprise customers and residential customers.

2) SBC-AC (access to core SBC): SBC-AC is located at the network edge, either at the enterprise access network or residential access network to service provider network.

3) SBC-CC (core to core SBC): SBC-CC is located at the service provider core network and provides functionality on behalf of each service provider core network.

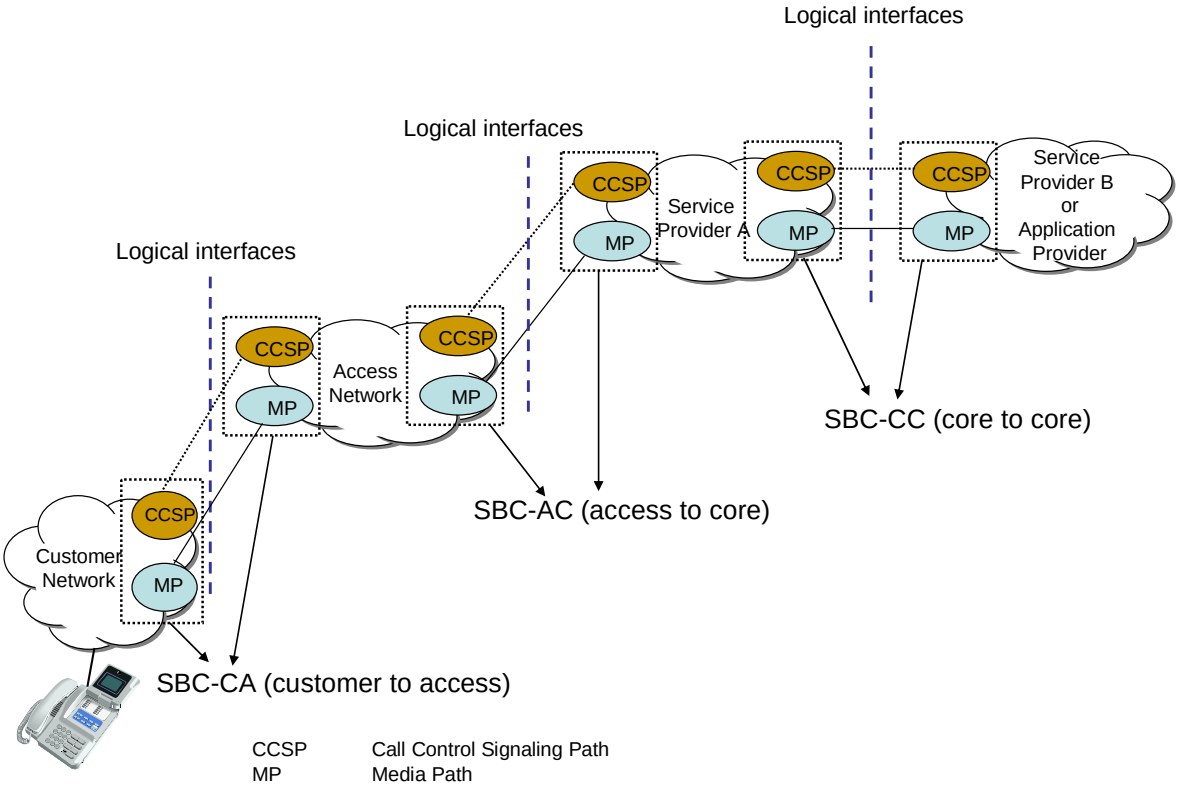
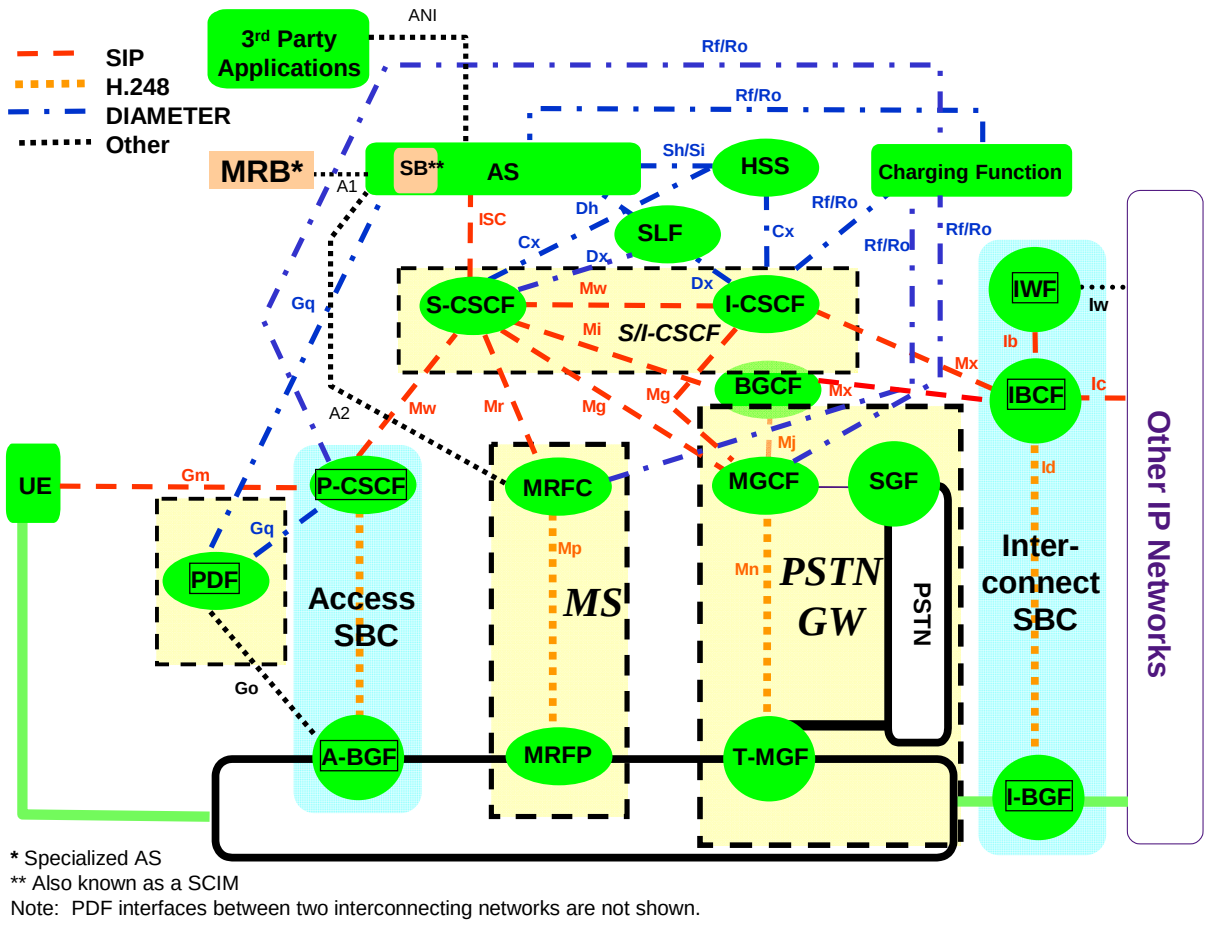


Figure 3 - Location of SBC Functions

Figure 4 shows the ATIS NGN architecture. An access SBC (access to core) is comprised of a PDF, an A-BGF, and optionally a P-CSCF. Similarly, an interconnect SBC (core to core) is comprised of an IBCF, an IWF, and an I-BGF. Although, the ATIS NGN architecture does not show a customer to access SBC, it was not intended to propose that it be disallowed.



***** Specialized AS
** Also known as a SCIM
Note: PDF interfaces between two interconnecting networks are not shown.

Figure 4 - Functional Entities Corresponding to the SBC (highlighted with rectangular shading ( ) around the FE)

Table 1 identifies the architecture functional entities that perform SBC functions for the MP and CCSP. It shows the mapping between the FEs in Figure 4 and the corresponding functions in Figure 3.

Table 1- ATIS NGN architecture functional entities with SBC functions

	Customer to access	Access to core	Core to core
Media Path	N/A	A-BGF PDF	I-BGF
Call Control Signaling Path	N/A	P-CSCF	IBCF IWF

Table 2 describes the possible mapping of SBC functions within the ATIS NGN architecture.

Table 2 - SBC Functions to FE Mapping

	Deployment area in NGN	**Access-to-core network boundary**		**Core-to-core network boundary**	
	NGN stratum	**Transport**	**Service**	**Transport**	**Service**
SBC functions related to media path	Opening and closing of a pinhole	A-BGF, PDF	-	I-BGF	-
	Policing and marking	A-BGF, PDF	-	I-BGF	-
	Detection of inactivity	A-BGF, PDF	-	I-BGF	-
	NAT and NAPT	A-BGF, PDF	-	I-BGF	-
	Assisting remote NAT/NAPT traversal	A-BGF, PDF	-	I-BGF	-
	Resource and admission control	A-BGF, PDF	-	I-BGF	-
	IP payload processing	A-BGF, PDF	-	I-BGF	-
	Performance measurement	A-BGF, PDF	-	I-BGF	-
	Denial of service (DoS) detection and protection	A-BGF, PDF	-	I-BGF	-
	Media encryption and decryption	A-BGF, PDF	-	I-BGF	-
	Support for ETS	A-BGF, PDF	-	I-BGF	-
	Support for emergency calls/sessions	A-BGF, PDF	-	I-BGF	-
	Support for lawful intercept	A-BGF		I-BGF	-

	Deployment area in NGN	Access-to-core network boundary		Core-to-core network boundary	
	NGN stratum	**Transport**	**Service**	**Transport**	**Service**
SBC functions related to call control signaling path	Traffic control for signaling messages	-	P-CSCF	-	IBCF
	Authentication, Authorization and Accounting (AAA)	-	P-CSCF	-	IBCF
	Signaling protocol translation	-	P-CSCF	–	IBCF, IWF
	Signaling protocol interworking	-	P-CSCF	–	IBCF, IWF
	Call/Session-based routing	-	P-CSCF	–	IBCF
	DSP service control	-	P-CSCF	–	IBCF
	End-user information hiding	-	P-CSCF	–	IBCF
	Topology and infrastructure hiding	-	P-CSCF	–	IBCF
	DoS protection	-	P-CSCF	-	IBCF
	Signaling encryption and decryption	–	P-CSCF	–	IBCF
	Support for ETS	-	P-CSCF	-	IBCF
	Support for emergency calls/sessions	-	P-CSCF	-	IBCF
	Support for lawful intercept		P-CSCF	-	IBCF