International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2012

Supplement 1

(07/2006)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Frameworks and functional architecture models

---

Functional requirements and architecture of the NGN release 1

Supplement 1: Session/border control (S/BC) functions

ITU-T Recommendation Y.2012 – Supplement 1

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	**Y.2000–Y.2099**
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Y.2012

Functional requirements and architecture of the NGN release 1

Supplement 1

Session/border control (S/BC) functions

Summary

This Supplement provides the functions and implementation realization associated with the session/border control (S/BC).

Source

Supplement 1 to ITU-T Recommendation Y.2012 was agreed on 28 July 2006 by ITU-T Study Group 13 (2005-2008).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation Y.2012

Functional requirements and architecture of the NGN release 1

Supplement 1

Session/border control (S/BC) functions

1 Scope

In existing VoIP networks, session/border control (S/BC) functions have already been introduced for network interconnection of NGN/IP networks. S/BCs can play a role in VoIP services by controlling borders to resolve VoIP-related problems such as NAT or firewall traversal. S/BC is already being used in existing VoIP services and is thought to be essential in the NGN architecture. This Supplement provides the functions and implementation realization associated with the S/BC.

2 References

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

3 Definitions

This Supplement defines the following term:

3.1 session/border control: Session/border control is a set of functions that enables interactive communication across the borders or boundaries of disparate IP networks. It provides 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 signalling protocols.

4 Abbreviations

This Supplement uses the following abbreviations:

AAA Authentication, Authorization and Accounting

ABG-FE Access Border Gateway Functional Entity

AGC-FE Access Gateway Control Functional Entity

AMG-FE Access Media Gateway Functional Entity

ANI Application-to-Network Interface

APL Application

AS-FE Application Server Functional Entity

A-TRC-FE Access Transport Resource Control Functional Entity

BGC-FE Breakout Gateway Control Functional Entity

CCSP Call Control Signalling Path

C-TRC-FE Core Transport Resource Control Functional Entity

DoS Denial of Service

DTMF	Dual Tone Multi Frequency
ETS	Emergency Telecommunications Service
FE	Functional Entity
IBC-FE	Interconnection Border Gateway Control Functional Entity
IBG-FE	Interconnection Border Gateway Functional Entity
I-CSC-FE	Interrogating Call Session Control Functional Entity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MGC-FE	Media Gateway Control Functional Entity
MLT-FE	Multimedia Services Functional Entity
MP	Media Path
MRB-FE	Media Resource Broker Functional Entity
MRC-FE	Media Resource Control Functional Entity
MRP-FE	Media Resource Processing Functional Entity
NACF	Network Attachment Control Function
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NGN	Next Generation Network
NNI	Network-to-Network Interface
P-CSC-FE	Proxy Call Session Control Functional Entity
PD-FE	Policy Decision Functional Entity
QoS	Quality of Service
RACF	Resource and Admission Control Function
S/BC	Session/Border Control
S/BC-AC	Access to Core S/BC
S/BC-CA	Customer to Access S/BC
S/BC-CC	Core to Core S/BC
S-CSC-FE	Serving Call Session Control Functional Entity
SG-FE	Signalling Gateway Functional Entity
SIP	Session Initiation Protocol
SS7	Signalling System No. 7
TCP	Transmission Control Protocol
TDR	Telecommunications for Disaster Relief
TMG-FE	Trunk Media Gateway Functional Entity
TRC-FE	Transport Resource Control Functional Entity
UDP	User Datagram Protocol
UNI	User-to-Network Interface

USIW-FE User Signalling Interworking Functional Entity

VPN Virtual Private Network

5 Conventions

None.

6 Functions

The media path and signalling path functions are listed below.

Functions related to media path

– *VPN bridging or mediation*

  • This function allows the connection or bridging of different types of VPNs to enable media packets to pass through. Signalling 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 signalling 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 be notified by signalling-related functions to terminate the 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 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 receiving user.
  - 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 stream (e.g., IPSec).
– *Support for emergency telecommunications service/telecommunications for disaster relief (ETS/TDR)*
  - Identification of ETS/TDR traffic and priority handling for the IP flows of the ETS/TDR traffic.
  - Conformance checking and mapping (if applicable) of priority marking based on policy for ETS/TDR communications.
  - Enforcement of security functions to protect ETS/TDR communications based on policies. For example, authenticating source for handing off and receiving traffic for ETS/TDR communications.
– *Support for emergency calls*
  - Identification of emergency call and priority handling for the IP flows of the emergency call traffic.
  - Conformance checking and mapping (if applicable) of priority marking based on policy for emergency calls.
  - Transfer of the emergency call to emergency call handling system.

Functions related to signalling path

– *Traffic control for signalling messages*
  - Restriction of session establishment in case of signalling-level congestion.
  - Load balancing among receiving or target servers.
– *Authentication, authorization and accounting (AAA)*
  - User/endpoint authentication.
  - Session admission control.
  - Detail record generation for a session.
– *Signalling protocol translation*
  - Translation of signalling protocol including protocol normalization, compensation and repair.
– *Signalling protocol interworking*
  - SIP and H.323 protocol interworking.
  - Termination and generation of different signalling transport protocols such as TCP and UDP.
  - Interworking at IP layer such as between IPv4 and IPv6.

– *Session-based routing*
  - Session-based routing – Ability to assign sessions to servers in the case of point-to-multipoint transmission.
  - User/endpoint registration – Ability to assign user/endpoint registration request to a server.
  - Session routing – Ability to assign session to route in the case that it crosses multiple operators.
– *DSP service control*
  - Codec negotiation and control of lower layer service.
– *End-user information hiding*
  - Hiding identity and address.
– *Topology and infrastructure hiding*
  - Hiding information included in the signalling message.
– *DoS protection*
  - Protecting the C-plane from DoS attacks.
– *Signalling encryption and decryption*
  - Encryption and decryption of signalling stream (e.g., IPSec).
– *Support for ETS/TDR*
  - Identification of ETS/TDR signalling and priority handling for the ETS/TDR session set-up based on policy for ETS/TDR signalling.
  - Verifying and conformance checking, and mapping (if applicable) of priority information based on policy for ETS/TDR signalling.
  - Enforcement of security functions to protect ETS/TDR signalling based on policies. For example, authenticating source for handing off and receiving ETS/TDR signalling.
– *Support for emergency calls*
  - Identification of emergency call signalling and priority handling for the emergency call set-up based on policy for emergency call signalling.
  - Analyse the caller's geographical information and transfer it to the emergency call handling system to locate the caller's position.

7 Deployment area

Figure 1 illustrates the location of the S/BC call control signalling path (CCSP) and media path (MP) functions. There are different functions at the customer edge, access network, transit network, and service provider core network. At the customer edge, either at the customer side or at the network entrance, the S/BC provides functionality on behalf of the customer, such as protecting the customer, hiding the customer's IP address and enforcing QoS. This is applicable for enterprise customers. At the access network, the S/BC provides functionality on behalf of each network segment such as the access network and the service provider core network. At the service provider core network, it provides functionality on behalf of each service provider core network.

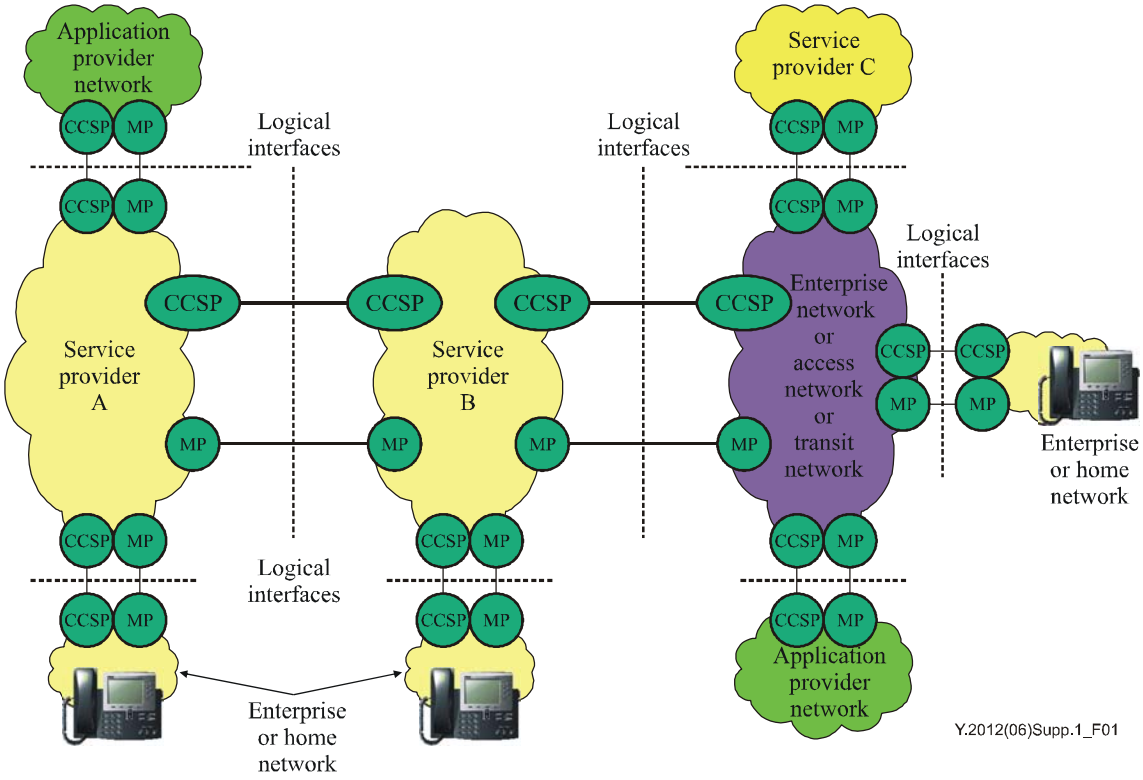


Figure 1 – Locations of S/BC functions

8 Composition of session/border control

The separation of S/BC functionality as currently shown in Figure 3 of [ITU-T Y.2012], is appropriate and necessary for several reasons:

– In the NGN architecture, there is a need for multiple functions (instantiated in multiple devices) to control the media portion of the S/BC function. In particular, the interconnection border gateway control FE (IBC-FE) and the policy decision FE (PD-FE) will both need to interface with the interconnection border gateway FE (IBG-GE). In addition, there may be a need for media resource control FE (MRC-FE) and proxy call session control FE (P-CSC-FE) to interface with the interconnection border gateway FE (IBG-FE) for S/BC functions. Similar considerations govern the access border gateway FE (ABG-FE) and its relationship to the proxy call session control FE (P-CSC-FE). A fully integrated S/BC would complicate this interworking.

– Signalling interworking may be separate from the S/BC 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 completion, the type of signalling interworking that is required. In addition, as networks evolve, it is likely that the need for signalling interworking will decrease over time. Because of this, it must be possible to flexibly insert signalling interworking functionality into the session, perhaps initiated by the interrogating call session control FE (I-CSC-FE).

– Initial deployments of NGN networks may find an integrated approach to S/BC a useful mechanism to satisfy all initial architectural requirements. As NGN networks expand, separation of the various functional entities related to S/BC will allow networks to scale more efficiently, especially when the requirements for signalling/control functions and media functions evolve independently.

S/BC functions can be logically split into two types: signalling-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 signalling-related functions and media-related functions which co-reside within the same physical component. Hence the relationship between signalling-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 signalling functions. This allows multiple accesses to a single media resource from different types of signalling or application-specific functions.
   - The N:M configuration allows for multiple media-related functions to be controlled by multiple signalling functions; a signalling-related function is selected depending on the status of the multiple signalling-related functions. Once one signalling-related function is selected, it will determine which media-related function is served for that signalling-related function. This configuration is the most reliable configuration among the three distributed models. However, it requires more considerable technology to determine which signalling-related function and media-related function will be served.

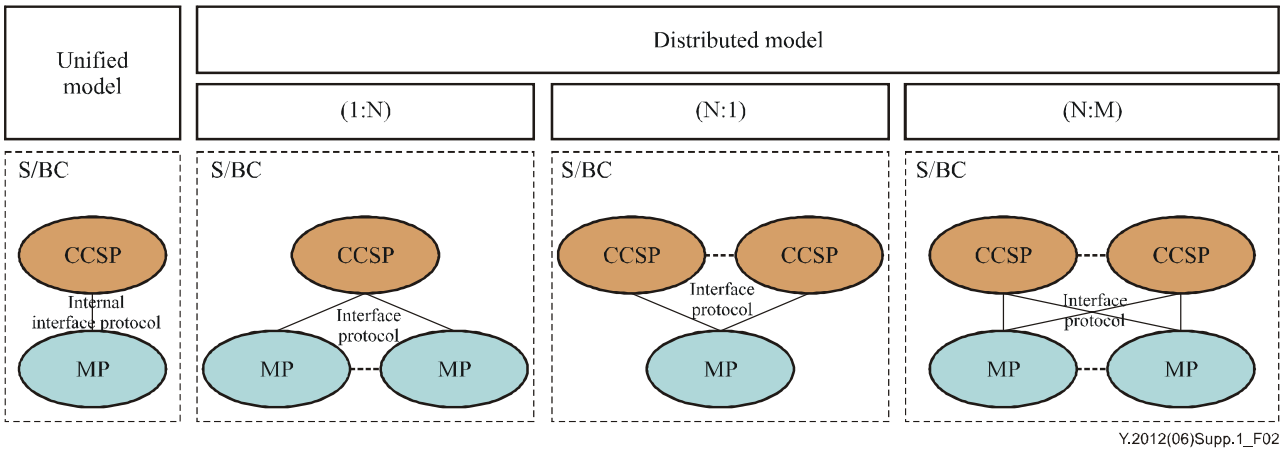


Figure 2 – Two models of S/BC

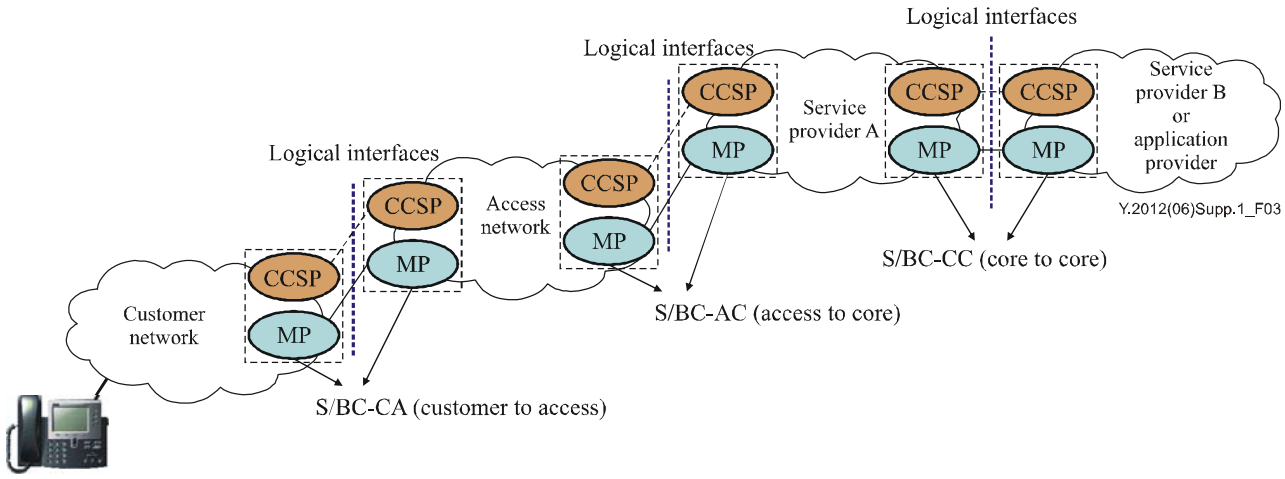
9 Mapping to NGN architecture

Figure 3 illustrates three types of S/BC depending on its location:

1) S/BC-CA (customer to access S/BC): S/BC-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) S/BC-AC (access to core S/BC): S/BC-AC is located at the network edge, either at the enterprise access network or residential access network to service provider network.

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



CCSP Call control signalling path
MP Media path

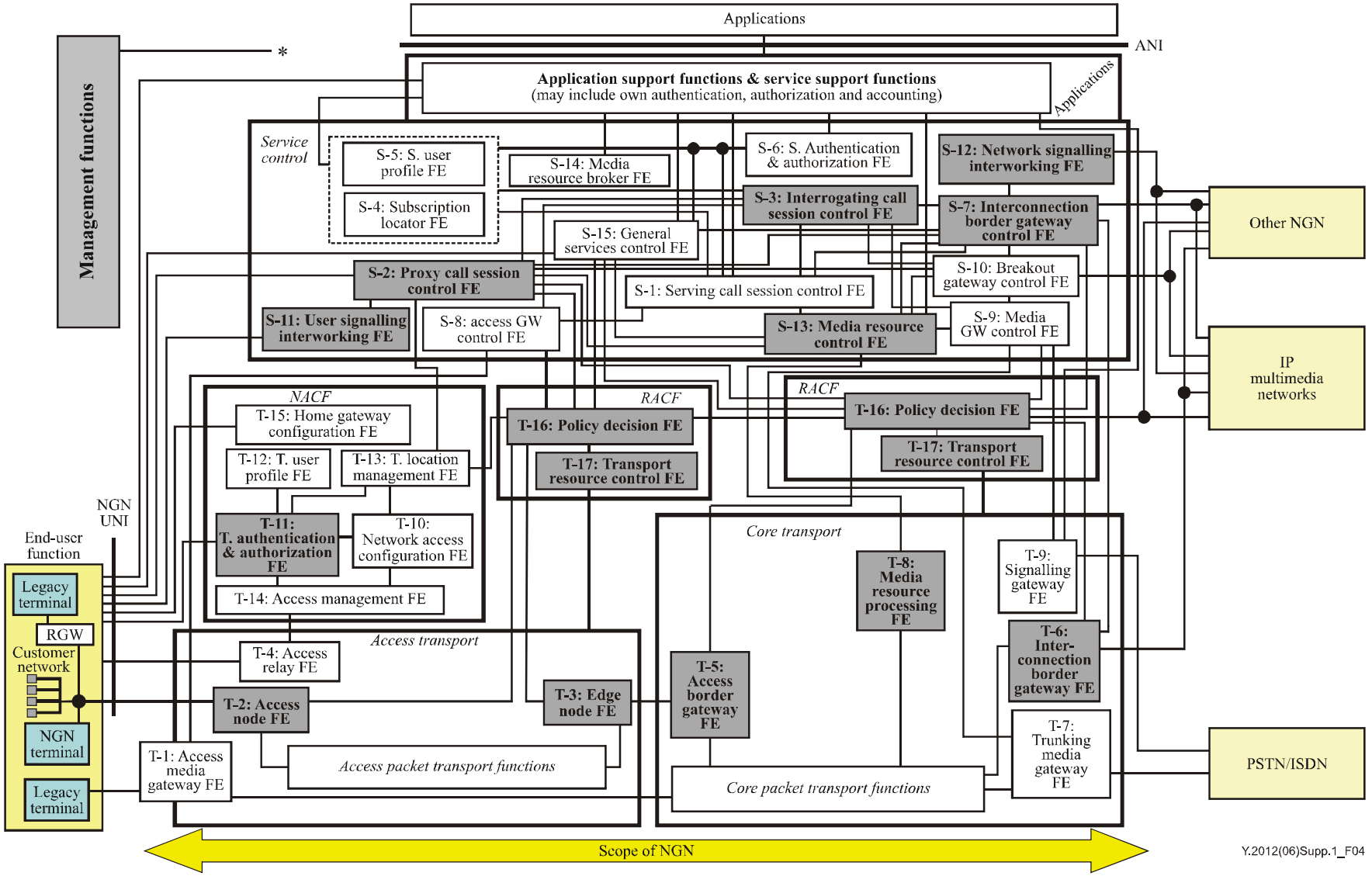
Figure 3 – Location of S/BC functions

Table 1 identifies the architecture functional entities that perform S/BC functions for the media and signalling paths.

Table 1 – Architecture functional entities with S/BC functions

	Customer to access	**Access to core**	**Core to core**
Functions relating to media path			
Transport stratum	Access node FE (T-2) Transport resource control FE (T-17) Policy decision FE (T-16) Authentication & authorization (T-11)	Edge node FE (T-3) Access border gateway FE (T-5) Policy decision FE (T-16) Transport resource control FE (T-17)	Interconnection border gateway FE (T-6) Policy decision FE (T-16) Transport resource control FE (T-17) Media resource processing FE (T-8)
Functions relating to signalling path			
Service stratum	Proxy call session control FE (S-2)	Proxy call session control FE (S-2) User signalling interworking FE (S-11)	Interconnection border GW control FE (S-7) Interrogating call session control FE (S-3) Network signalling interworking FE (S-12) Media resource control FE (S-13)

Figure 4 shows the NGN architecture contained in [ITU-T Y.2012] highlighting the FEs that support S/BC functions.



NOTE – Explanatory notes to this figure are given in Figure 3 of [ITU-T Y.2012].

Figure 4 – Functional entities corresponding to S/BC (highlighted)

Table 2 describes the possible mapping of S/BC functions within the NGN architecture [ITU-T Y.2012].

Table 2 – S/BC functions to FE mapping

	Deployment area in NGN	**Customer to access network boundary**		**Access-to-core network boundary**		**Core-to-core network boundary**	
	NGN stratum	**Transport**	**Service**	**Transport**	**Service**	**Transport**	**Service**
S/BC functions related to media path	Opening and closing of a pinhole	(T-2, T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Policing and marking	(T-2, T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Detection of inactivity			(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	NAT and NAPT			(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Assisting remote NAT/NAPT traversal			(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Resource and admission control	(T-2, T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	IP payload processing	(T-2, T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Performance measurement	(T-2, T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Denial of service (DoS) detection and protection	(T-2 , T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Media encryption and decryption	(T-2, T-16 & T-17)		(T-3/T-5, T-16 & T-17)		(T-6, T-16 & T-17)	
	Support for ETS/TDR	(T-2) (T-16 & T-17)		(T-3/T-5) (T-16 & T-17)		(T-6, T-16 & T-17)	
	Lawful interception	(T-2) (T-16 & T-17)		(T-3/T-5) (T-16 & T-17)		(T-6, T-16 & T-17)	
	Support for emergency calls	(T-2) (T-16 & T-17)		(T-3/T-5) (T-16 & T-17)		(T-6, T-16 & T-17)	

Table 2 – S/BC functions to FE mapping

	Deployment area in NGN	Customer to access network boundary		Access-to-core network boundary		Core-to-core network boundary	
	NGN stratum	**Transport**	**Service**	**Transport**	**Service**	**Transport**	**Service**
S/BC functions related to signalling path	Traffic control for signalling messages			(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-7 & S-3)
	Authentication, authorization and accounting (AAA)	(T-11, T-16 & T-17)		(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-7 & S-3)
	Signalling protocol translation	(T-16 & T-17)		(T-16 & T-17)	(S-2 & S-11)	–	(S-7, S-3 & S-12)
	Signalling protocol interworking	(T-16 & T-17)		(T-16 & T-17)	(S-2 & S-11)	–	(S-7, S-3 & S-12)
	Session-based routing	(T-16 & T-17)		(T-16 & T-17)	(S-2)	–	(S-7 & S-3)
	DSP service control	–	–	(T-16 & T-17)	(S-2)	–	(S-7 & S-3)
	End-user information hiding	–	–	(T-16 & T-17)	(S-2)	–	(S-7 & S-3)
	Topology and infrastructure hiding	–	–	(T-16 & T-17)	(S-2)	–	(S-7 & S-3)
	DoS protection	(T-16 & T-17)		(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-7 & S-3)
	Signalling encryption and decryption	–	–	–	(S-2)	–	(S-7 & S-3)
	Support for ETS/TDR	(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-7 & S-3)
	Support for emergency calls	(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-2)	(T-16 & T-17)	(S-7 & S-3)

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007