NGN Architecture: Generic Principles, Functional Architecture, and Implementation

Keith Knightson, Consultant

Naotaka Morita, NTT Corporation

Thomas Towle. Lucent Technologies — Bell Laboratories

ABSTRACT

This article summarizes the architectural aspects of a next-generation network in terms of general principles, functional representation, and typical implementation. According to the general reference model, which assumes decoupling of services and transport, NGN can be represented by multiple functional groups. One of the key implementations for session-based services, utilizing an IP multimedia subsystem, is introduced with enhanced features to meet both fixed and mobile network requirements.

INTRODUCTION

Given the existing "universal nature" of the Internet and its associated infrastructure, which includes an addressing plan, address assignment and resolution by domain name servers, and applications such as email, file transfer, and the World Wide Web, it can be assumed that IP-based systems will form the basis of a next-generation network (NGN). Thus, we conclude that an NGN is an enhanced IP-based network.

The new applications and deployment requirements, however, introduce needs that were not originally envisaged when the first generation of packet networks was designed. With this in mind, International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) Recommendation Y.2001 [1] identifies a number of characteristics considered necessary in an NGN. Additionally, ITU-T Recommendation Y.2011 [2] provides a general framework for the architectural underpinnings required to obtain the basic characteristics.

It is generally agreed that the main difference between traditional telecommunications services and an NGN is the shift from separate vertically integrated application-specific networks to a single network capable of carrying any and all services. For telephone services, this includes a shift from a circuit-switched infrastructure to a packet-switched infrastructure. Current NGN activity is aimed at ensuring that next-generation IP-based networks will be able to meet the standards of service normally associated with public telecommunications networks, not only for telephone services, but also for the widest possible set of present and future multimedia applications.

ITU-T RECOMMENDATION Y.2001: A GENERAL OVERVIEW OF NGN

The main purpose of Y.2001 is to provide a general definition of an NGN, as follows:

Next-generation network (NGN): A **packet-based** network able to provide telecommunication services and able to make use of multiple broadband **QoS-enabled** transport technologies and in which **service-related functions** are **independent** from underlying *transport-related technologies*. It enables unfettered access for users to networks and competing service providers and/or services of their choice. It supports **generalized mobility** that will allow consistent and ubiquitous provision of services to users.

The bold terms (highlighted solely for the purposes of this article) indicate the significant issues related to NGNs. The separation between services and transport is clearly recognized, and the addition of quality of service (QoS) to IP-based transport is also called out. The second sentence covers the capability for innovative service provision, allowing service providers to easily establish themselves and users to freely select services. The final sentence covers the extension of mobility between fixed and mobile systems, and between fixed systems as appropriate.

The fundamental characteristics defined in Recommendation Y.2001 are described in the companion article by C. S. Lee and D. Knight.

0163-6804/05/$20.00 © 2005 IEEE

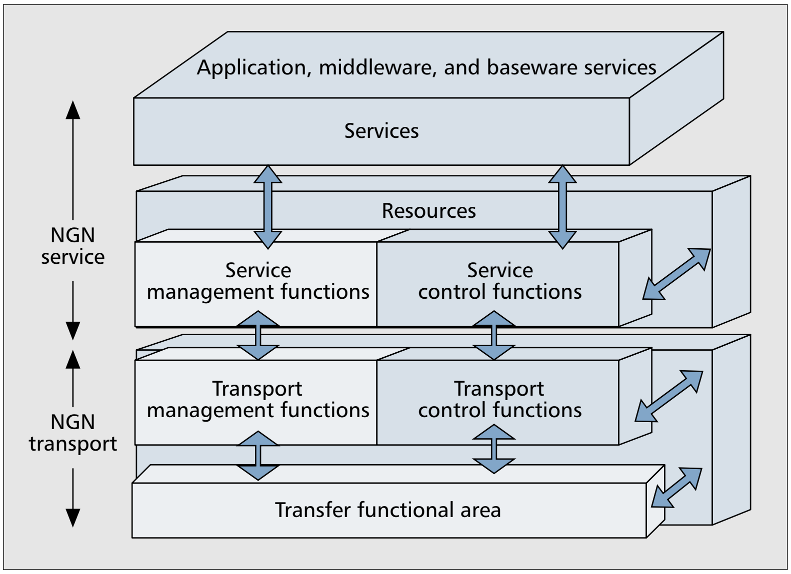

Figure 1. *General functional model.*

ITU-T Recommendation Y.2011: General Principles and General Reference Model for NGN

The primary purpose of Y.2011 is to provide a basis for developing functional models for NGN-based services.

First, it points out the potential differences between NGN layered systems and the seven-layer open systems interconnection basic reference model (OSI BRM) as defined in ITU-T Recommendation X.200 [3]. For example, difficulties arise in considering the number and specific characteristics of the seven layers of the OSI BRM. As far as NGN systems (non-OSI systems) are concerned, some or all of the following situations may be encountered:

- The number of layers may not be seven.
- The functions of the individual layers may not correspond to those of the OSI BRM.
- Certain prescribed or proscribed conditions/definitions in the OSI BRM may not be applicable.
- The protocols involved may not be OSI protocols (one notable example being IP).
- The compliance requirements of the OSI BRM may not be applicable.

The annexes of Y.2011 detail the clauses of the OSI BRM that are retained for NGN purposes, and those considered inappropriate for an NGN.

The services and functions are related to each other, since the functions are used to build services. It is convenient to divide functions into two distinct groups, or planes: one comprising all control functions, and the other all management functions. Grouping functions of the same type (i.e., control or management) allows the functional interrelationships and information flows between functions within a given group to be defined.

With this in mind, Y.2011 then goes on to consider the functional aspects of system implementation. In particular, it develops a high-level model, illustrated in Fig. 1, which shows how functions may be grouped for the purposes of system development. The functional blocks shown in the figure may then be further decomposed into subgroups to obtain a grouping convenient for implementation and distributed system depiction.

NGN Architecture

This section highlights the status of NGN architecture as discussed in the Focus Group for Next Generation Networks (FGNGN) under ITU-T. It should be noted that the final description might be changed according to the results of further study.

NGN services will include session-based services, such as IP telephony, videoconferencing, and video chatting, and non-session-based services, such as video streaming and broadcasting. Moreover, NGNs support public switched telephone network/integrated services digital network (PSTN/ISDN) replacement (PSTN/ISDN emulation in ITU-T terminology).

Figure 2 shows an overview of the NGN architecture. The NGN functions are divided into service and transport strata according to Recommendation Y.2011.

End-user functions are connected to the NGN by the user-to-network interface (UNI), while other networks are interconnected through the network-to-network interface (NNI). Clear identification of the UNI and NNI is important to accommodate a wide variety of off-the-shelf customer equipment while maintaining business boundaries and demarcation points in the NGN environment. The application-to-network interface (ANI) forms a boundary with respect to third-party application providers.

Transport Stratum Functions

Transport stratum functions provide connectivity for all components and physically separated functions within the NGN. IP is recognized as the most promising transport technology for NGN. Thus, the transport stratum will provide IP connectivity for both end-user equipment outside the NGN, and controllers and enablers that usually reside on servers inside the NGN. The transport stratum is responsible for providing end-to-end QoS, which is a desirable feature of the NGN. The transport stratum is divided into access networks and the core network, with a function linking the two portions.

Access Functions — The access functions manage end-user access to the network. The access functions are access-technology-dependent, such as wideband code-division multiple access (W-CDMA) and digital subscriber line (xDSL). The access networks include functions related to cable access, DSL technology, wireless technology, Ethernet technology, and optical access.

Access Transport Functions — These functions are responsible for transporting information across the access network. They also provide QoS control mechanisms dealing directly with user traffic, including buffer management, queu-

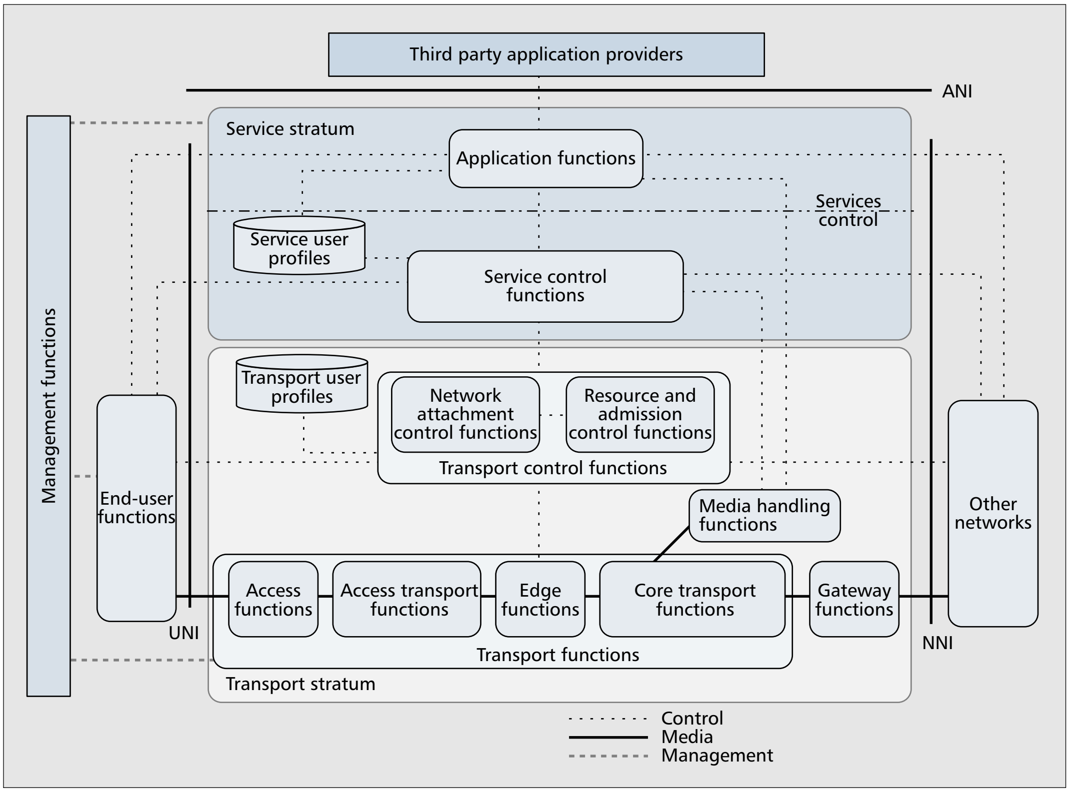

Figure 2. *NGN architecture overview. (Note: The final drawing might be changed according to the results of further study.)*

Admission control involves checking authentication based on user profiles, through the network attachment control functions. It also involves authorization based on user profiles, taking into account operator-specific policy rules and resource availability.

ing and scheduling, packet filtering, traffic classification, marking, policing, and shaping.

Edge Functions — Edge functions are used for traffic processing when access traffic is merged into the core network.

Core Transport Functions — These functions are responsible for ensuring information transport throughout the core network. They provide the means to differentiate the quality of transport in the network, according to interactions with the transport control functions. These functions also provide QoS mechanisms dealing directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing and shaping, gate control, and firewalls.

Network Attachment Control Functions — These functions provide registration at the access level and initialization of end-user functions for accessing NGN services. They provide network-level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of the NGN service and application functions to the end user. That is, the network attachment control functions assist end-user equipment in registering and starting use of the NGN.

Resource and Admission Control Functions — The RACFs provide admission control and gate control functionalities, including control of network address and port translation (NAPT) and differentiated services field code points (DSCPs). Admission control involves checking authentication based on user profiles, through the network attachment control functions. It also involves authorization based on user profiles, taking into account operator-specific policy rules and resource availability. Checking resource availability means that the admission control function verifies whether a resource request (e.g., for bandwidth) is allowable given the remaining resources, as opposed to resources that are already provisioned or used.

The RACFs interact with transport functions to control one or more of the following functionalities in the transport layer: packet filtering, traffic classification, marking and policing, bandwidth reservation and allocation, NAPT, anti-spoofing of IP addresses, NAPT/FW traversal, and usage metering.

Transport User Profile Functions — This functional block represents the compilation of user and other control data into a single "user profile" function in the transport stratum. This function may be specified and implemented as a set of cooperating databases with functionality residing in any part of the NGN.

Gateway Functions — These functions provide capabilities to interwork with other networks, including many existing networks, such as PSTN/ISDN-based networks and the Internet. These functions even support interworking with other NGNs belonging to other administrators.

An IMS is based on a model where a network operator and a service provider control access to the network and the services, respectively for which customers are billed. This is in contrast to the usual Internet model, where the network is transparent and all services are provided by endpoints.

The NNI for other networks applies to both the control and transport levels, including border gateways. Interactions between the control and transport levels may take place directly or through the transport control functionality.

Media Handling Functions — The series of media handling functions are media resource processes for providing services, such as generating tone signals, transcoding, and conference bridging.

SERVICE STRATUM FUNCTIONS

These functions provide session-based and non-session-based services, including subscribe/notify for presence information and a message method for instant message exchange. The service stratum functions also provide all of the network functionality associated with existing PSTN/ISDN services and capabilities and interfaces to legacy customer equipment.

Service and Control Functions — These functions include session control functions, a registration function, and authentication and authorization functions at the service level. They can include functions controlling media resources (i.e., specialized resources).

Service User Profile Functions — These functions represent the compilation of user data and other control data into a single user profile function in the service stratum. This function may be specified and implemented as a set of cooperating databases with functionality residing in any part of the NGN.

Application Functions — NGNs support open APIs enabling third-party service providers to apply NGN capabilities to create enhanced services for NGN users. All application functions (both trusted and untrusted) and third-party service providers access NGN service stratum capabilities and resources through servers or gateways in the service stratum.

MANAGEMENT FUNCTIONS

Support for network management is fundamental to the operation of an NGN. The management functions enable the NGN operator to manage the network and provide NGN services with the expected quality, security, and reliability.

These functions are allocated in a distributed manner to each functional entity (FE). They interact with network element (NE) management, network management, and service management FEs.

The management functions include charging and billing functions. These functions interact with each other in the NGN to collect accounting information, which provides the NGN operator with resource utilization data enabling the operator to properly bill users. The charging and billing functions support the collection of data for both later processing (offline charging) and near-real-time interactions with applications such as those for prepaid services (online charging).

END-USER FUNCTIONS

The interfaces to the end user are both physical and functional (control) interfaces, as shown in Fig. 2. No assumptions are made about the diverse customer interfaces and customer networks that may be connected to the NGN access network. All customer equipment categories are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

IP MULTIMEDIA SUBSYSTEM FOR NGN

INTRODUCTION TO IMS

An IP multimedia subsystem (IMS) is a set of core network FEs and interfaces used by a network service provider to offer SIP-based services to subscribers, where SIP is the Session Initiation Protocol defined by the Internet Engineering Task Force (IETF) [4]. For the most part, an IMS is independent of the access network technology, although there are some links between the IMS and the underlying transport functionality, and these may be access specific. An IMS is built on IETF protocols, with specific profiles and enhancements to provide a complete, robust multimedia system. The enhancements and operational profiles provide support for operator control, charging and billing, and security.

In addition to the enhancements and profiles, an IMS requires a set of vertical interfaces to provide the following:

- Common interfaces to application servers for accounting, security, subscription data, service control, and to service building blocks such as presence functions
- Coordinated and enforced QoS (session layer negotiation can be matched with resources granted at the transport layer, per operator policy)
- Session-based media gating under operator control
- Correlated accounting and charging among the service, session, and transport layers

These capabilities make IMSs different from the usual Internet applications for session control. An IMS is based on a model where a network operator and service provider control access to the network and services, respectively, for which customers are billed. This is in contrast to the usual Internet model, where the network is transparent and all services are provided by endpoints. As a result of this more controlled environment, users get an improved experience with managed QoS, single-sign-on security, and customer support, at least in theory.

IMS ARCHITECTURE

Core Networks vs. Access Networks — As mentioned earlier, an IMS is a collection of core network FEs. This terminology, differentiating *core* and *access*, comes from the wireless network model, where one or more radio access networks are connected to a common core. The

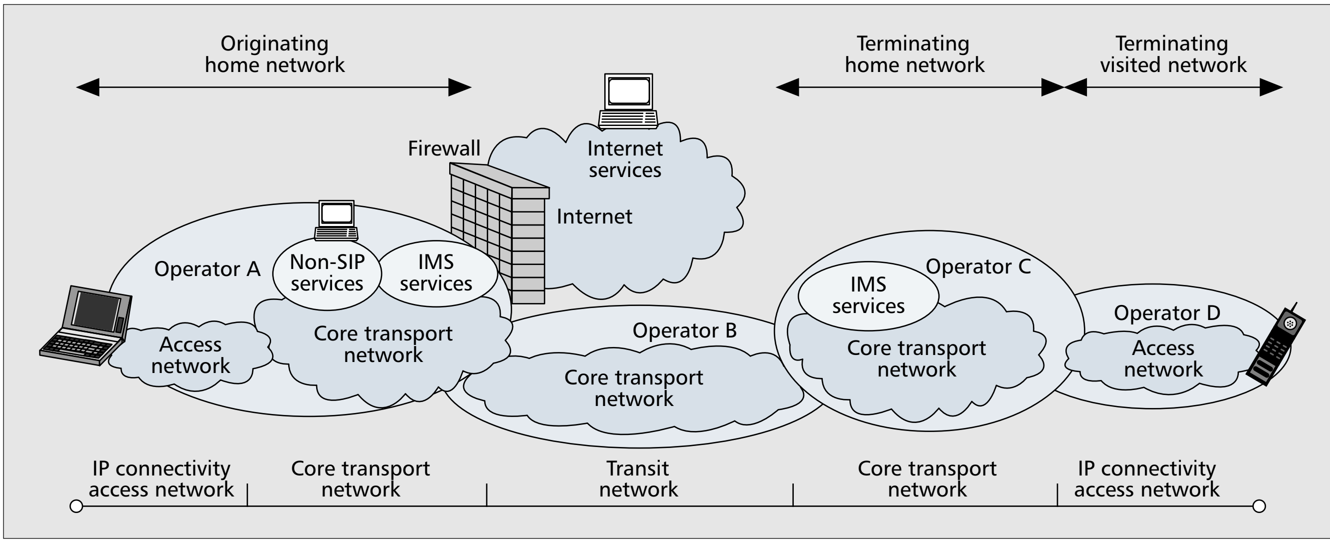

Figure 3. *Network partitioning.*

radio access networks provide connections from terminals to the services provided in the core.

With respect to an IMS, an access network is a collection of entities providing IP transport connectivity between a user domain and a core transport network. Access networks are distinguished from one another according to the underlying technology, ownership, or administrative partitioning. The point at which an access network is attached to a core transport network may be chosen administratively.

The core network is then a collection of entities providing IP transport connectivity between an access network and another core transport network, between two access networks, or between two other core transport networks. The core transport network also provides connectivity to service layer entities, such as IMSs. Core transport networks also can be distinguished from one another according to the underlying technology, ownership, or administrative partitioning.

One of the fundamental characteristics of an IMS is support for user mobility; thus, the distinction between the core and access networks becomes important in partitioning the functions necessary to support an IMS. Figure 3 shows one example of such a partitioned collection of networks. As a user moves from one access network to another, access to the same core network services can be provided. This is true for non-real-time movement such as roaming, as well as for real-time movement when the access technology supports mobility, such as handoffs.

As shown in Fig. 3, an IMS also supports the concept of a home network, as opposed to a visited network. In this paradigm the home network is the core network supporting the IMS services that hold the IMS subscription. The visited network is the network currently providing the user with connectivity to his/her IMS services. Therefore, in Fig. 3 operator A owns the home network of the laptop user, while operator C owns the home network of the mobile phone user, who happens to be roaming in operator D's network.

IMS Functional Entities — Figure 4 shows the collection of functional entities and reference points that comprise the IMS functional architecture. Each of these entities is covered in more detail in the following sections. Figure 4 also shows how IMS entities may be distributed between the home and visited networks.

Application Server — An application server (AS) provides service control for the IMS. The AS may be directly connected to an S-CSCF, or it may be connected via an Open Services Architecture (OSA) gateway for third-party based applications over an ISC reference point. The ISC interface is SIP-based. Thus, SIP messages may be forwarded over this interface to or from a serving call session control function (S-CSCF). The AS may interact with the home subscriber server (HSS) over the Sh interface in order to obtain subscriber profile information. Application servers are used to support various telephony-type services, such as call forwarding and number translation, and may also support such services as presence, conference control, and online charging.

Breakout Gateway Control Function — A breakout gateway control function (BGCF) receives session requests forwarded by an S-CSCF or another BGCF, and it selects the network in which PSTN breakout is to occur. It selects a local MGCF or peer BGCF in another network. This ability to select a BGCF in another network provides the capability to optimize routing from the visited network to the PSTN, where desired and supported by the operators involved.

Call Session Control Functions — The CSCFs provide session control for the IMS. They coordinate with other network elements to control session features, routing, and resource allocation. There are three different types of CSCFs in the IMS architecture:

- Serving CSCF (S-CSCF) — the main home network session control point for the user

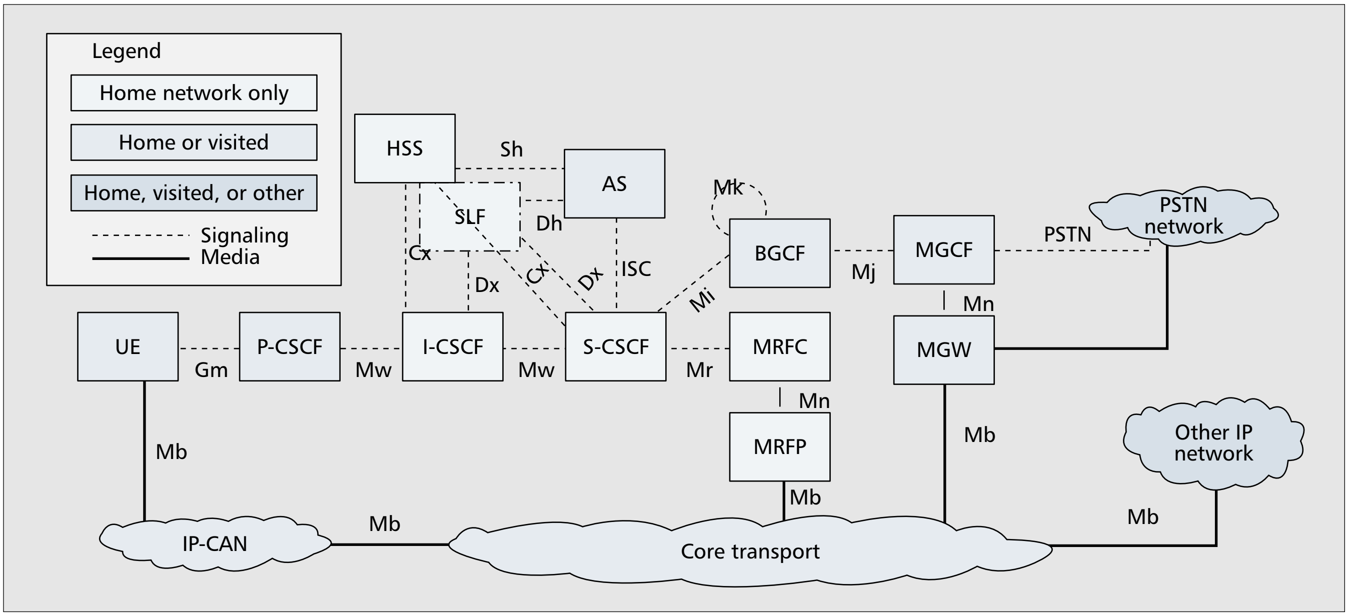

Figure 4. *IMS functional entities and reference points.*

equipment (UE) for originating or terminating sessions
- Interrogating CSCF (I-CSCF) — the contact point into the UE's home network from other networks
- Proxy CSCF (P-CSCF) — the contact point into the IMS from the UE

An S-CSCF acts as a registrar, as defined in IETF RFC 3261 [1]. In this role it accepts SIP REGISTER requests and creates a binding between the public user ID and the terminal location. The S-CSCF retrieves the subscriber profile from the HSS, including filter criteria that indicate the ASs providing service control for this user. To support service control, the S-CSCF interacts with these ASs during SIP signaling. During session establishment or modification, the S-CSCF monitors the Session Description Protocol (SDP) to ensure that the session is within the boundaries of the subscriber's profile.

The S-CSCF uses the filter criteria to involve ASs as needed in order to provide the services and features to which the user subscribes. It forwards SIP messages to each AS in the order indicted by the filter criteria. After the last AS is contacted, the SIP message is then sent toward the intended destination. The filter criteria can be set on various service trigger points, including any known SIP method (e.g., REGISTER, INVITE), the presence or absence of any header, the content of any header, the direction of the request with respect to the served user, and SDP.

The S-CSCF also performs routing of SIP messages on behalf of the originating UE. It obtains the address of an I-CSCF (or other IP endpoint) for the network operator serving the destination subscriber from a domain name server (DNS) by using the destination name of the terminating subscriber; it then forwards the SIP request toward the destination. If the destination name of the terminating subscriber is determined to be a PSTN address, the S-CSCF forwards the request to a BGCF for routing toward the PSTN. On behalf of the destination endpoint, the S-CSCF forwards the SIP request to a P-CSCF according to the subscriber's registered location, or, for an unregistered subscriber, it may send or redirect the SIP request to an alternate endpoint according to call forwarding or a similar service.

The I-CSCF serves as the initial point of contact to the IMS home network from other networks. It performs a stateless SIP proxy function. It routes received SIP requests to the S-CSCF assigned to the user or selects an S-CSCF if one is not currently assigned. The I-CSCF assigns S-CSCFs upon initial UE registration and when terminating services for unregistered users.

The P-CSCF serves as the initial point of contact for a user terminal to the IMS. It performs a stateful SIP proxy function, sending SIP REGISTER requests from the UE to an I-CSCF in the home network, which is determined using the home domain name provided by the UE. The P-SCCF sends all subsequent SIP messages received from the UE to the S-CSCF whose name it has received as a result of the registration procedure.

The P-CSCF also ensures that a valid public user identity for the IMS user is inserted into UE-initiated SIP requests. It performs SIP message compression to reduce the amount of data sent to or from the UE. It may also support resource and admission control capabilities by interacting with the transport layer for networks where this approach is employed.

Home Subscriber Server — The HSS contains a subscription database for the IMS, including subscription-related information to support the network entities that actually handle calls or sessions. It supports IMS-level authentication and authorization and holds the IMS subscriber profiles. The HSS also stores the currently assigned S-CSCF.

A home network may contain one or several

HSSs. The number of HSSs depends on the number of subscribers, the capacity of the equipment, and the organization of the network.

Media Gateway Control Function — The MGCF supports interworking between the IMS and the PSTN. It supports SIP-to-ISUP protocol conversion and controls the media gateway for bearer-level conversion.

Media Gateway — The MGW operates under the control of the MGCF to support interworking between the IMS and the PSTN. It terminates bearer channels from circuit-switched networks and media streams from packet-switched networks, and performs media conversion functions such as transcoding. In addition, it supports dual tone multifrequency (DTMF) detection and generation.

Media Resource Function Controller — The MRFC controls the media stream resources of the MRFP. It interprets information from an AS or SIP endpoint and controls the MRFP accordingly to support media services such as transcoding and conferencing. The MRFC may be collocated with an AS to provide specialized AS services.

Media Resource Function Processor — The MRFP provides resources under the control of the MRFC for media processing. It supports media stream mixing, tone and announcement generation, transcoding, media analysis, and other functions.

Subscription Locator Function — The SLF serves as a front-end for distributed HSS systems. It may be queried by an I-CSCF during registration and session setup to get the name of the HSS containing the required subscriber-specific data. The SLF may also be queried by the S-CSCF during registration, or by the AS in conjunction with the Sh interface.

The SLF is not required in a single-HSS environment, or in certain other HSS environments such as a server-farm architecture. It is also not required when an AS is configured and managed to use a predefined HSS.

User Equipment — The UE represents the functionality of a variety of user terminal devices. It supports the specific capabilities of the access network within which it is used. In addition, it supports the user agent capabilities of an IMS client. The UE supports the SIP methods, as defined by the IMS, for REGISTRATION, INVITE, and so forth.

USE OF SIP AND SDP BY IMS

The IMS uses a specific SIP profile. It defines extensions to headers and parameters to address the specific needs of telecommunications operators. Some specific parameter examples include the following:

• A new auth-param parameter defined for the Web-authenticate header, which is used to pass the integrity key and cipher key during the registration process for setting up the integrity-protected relationship between a UE and a P-CSCF

• A new tokenized-by parameter, which is used to carry encrypt/decrypt strings within SIP headers to implement the I-CSCF's topology-hiding interworking gateway function

• A new icn-charging-info parameter defined for the P-Charging-Vector header, which is used to include IP connectivity network charging information

• A new parameter defined for P-Access-Network-Info, which provides information on the access network serving the UE

The IMS architecture has introduced several private headers (P-Headers) into IETF in order to meet telephony needs. P-Headers are optional extensions to SIP:
- P-Asserted-Identity — Enables the network (e.g., a P-CSCF) to assert a public user identity for a calling user.
- P-Called-Party-ID — Enables the terminating UE to learn the dialed public user identity that triggered the call
- P-Access-Network-Info — Enables the UE to provide information related to the access network that it is using (e.g., a cellular ID)
- P-Visited-Network-ID — Enables the home network to discover, via registration, the identities of other networks utilized by the user
- P-Associated-URI — Enables the home network (e.g., an S-CSCF) to return a set of uniform resource identifiers (URIs) associated with the public user identity under registration
- P-Charging-Function-Addresses — Enables distribution of the addresses of charging functional entities
- P-Charging-Vector — Enables sharing of charging correlation information

The IMS architecture also has some specific restrictions with respect to the use of SDP. It bans encryption of SDP payloads, so the operator network is able to read them and can enforce QoS and policies when processing INVITE requests. For an initial INVITE, the IMS requires the SDP payload to include terminal capabilities, with codecs listed in priority order. For video and audio media types, the proposed bandwidth for each media stream will be included in the SDP payload.

ENHANCEMENTS TO IMS FOR NGN APPLICATIONS

The IMS specifications were developed for use with cellular access networks and were based on certain assumptions regarding the access network, such as the available bandwidth. The inherent differences between different types of access networks will have concrete consequences on the IMS specifications. Examples of such consequences include the following:

• To support xDSL-based access networks, the IMS may also need to interface with the network attachment functions of the IP-CAN for the purpose of accessing location information. No equivalent interface exists in the base IMS specifications.

• Support for IPv4 has to be taken into account, leading to a requirement to support NAPT functionalities. There are at least two rea-

The IMS specifications were developed for use with cellular access networks and were based on certain assumptions regarding the access network, such as the available bandwidth. The inherent differences between different types of access networks will have concrete consequences on the IMS specifications.

The necessary changes to the IMS architecture are expected to be made to the base IMS standards owned by the Third Generation Partnership Project (3GPP) and 3GPP2 as part of future releases.

sons for this. First, some operators have to face IPv4 address shortages. Second, the privacy of IP addresses for media streams cannot rely on RFC 3041 (Privacy Extensions for Stateless Address Auto-Configuration in IPv6), as would be the case for IPv6. NAPT provides an alternative for hiding terminal addresses.

• Support for NAPT functionality is covered in the NGN functional architecture. Extensions for working with configurations containing NAPT need to be provided in the IMS specifications.

• Relaxing the constraints on bandwidth scarcity may lead to consideration of optional support for some features that are currently considered mandatory (e.g., SIP compression).

• Differences in location management will impact various protocols that convey this information, in terms of both signaling interfaces and charging interfaces.

• Differences in resource reservation procedures in the access network will require changes to the IMS resource authorization and reservation procedures, as the resource reservation procedures for xDSL access networks will have to be initiated by a network entity (i.e., a P-CSCF in the case of SIP-based services), on behalf of end-user terminals.

The above extensions are being examined by various standards bodies in order to support the use of IMSs in NGNs. The necessary changes to the IMS architecture are expected to be made to the base IMS standards owned by the Third Generation Partnership Project (3GPP) and 3GPP2 as part of future releases.

CONCLUSION

This article has presented the general principles and reference model for a next-generation network, as specified in ITU-T Recommendations. We have examined the latest concepts in terms of functional architecture, which will appear soon as new ITU-T Recommendations. The IMS architecture and its standardized entities and interfaces are being applied in NGNs to provide support for SIP-based services provided by network operators.

REFERENCES

[1] ITU-T Rec. Y.2001, "General Overview of NGN."

[2] ITU-T Rec. Y.2011, "General Principles and General Reference Model for Next Generation Network."

[3] ITU-T Rec. X.200, "Information Technology — Open Systems Interconnection — Basic Reference Model: The Basic Model," 1994.

[4] IETF RFC 3261, "SIP: Session Initiation Protocol."

BIOGRAPHIES

KEITH KNIGHTSON has more than 30 years experience in the design of network protocols and architectures, and use of open standards. He has provided consulting services to a number of organizations, in the area of network design and interconnection. Currently, special emphasis is being placed on the strategic and technical implications of NGNs and related IP-based infrastructures. He is a co-leader of working group 2, Functional Architecture and Mobility Group in FGNGN.

NAOTAKA MORITA received his B.E. and M.E. degrees from Nagoya University, Aichi, Japan, in 1985 and 1987, respectively. In 1987 he joined the Research and Development Center of NTT Corporation, where he engaged in the research of ATM systems. Since 2000 he has been studying VoIP and interactive multimedia technology. Since October 2004 he has been a Vice Chair of SG13 in ITU-T. He is a coleader of working group 2, Functional Architecture and Mobility Group in FGNGN.

THOMAS TOWLE is currently a consulting member of technical staff at Lucent Technologies — Bell Laboratories. He joined Bell Laboratories in 1978 after receiving his Master of Science in Electrical Engineering from the University of Illinois. He spent several years in Lucent's Computer Systems Division in operating system and network software development. More recently he has worked in the Wireless Systems Division on standards development. He has worked on the development of GSM standards in the European Telecommunications Standards Institute (ETSI), on cdma2000 in the Telecommunications Industry Association (TIA), and on IMT2000 in the ITU. Currently he participates in 3GPP, 3GPP2 and the ITU-T NGN Focus Group working on IMS related standards. He is a co-leader of working group 2, Functional Architecture and Mobility Group in FGNGN.