CHAPTER 5

IMS AND CONVERGENCE MANAGEMENT

Keizo Kawakami, Kaoru Kenyoshi, and Toshiyuki Misu

5.1 IMS ARCHITECTURE

Service providers (SPs) recently have gained momentum with the migration to the Next Generation Networks (NGN) and the move towards full IP-based networks. This trend is based on the intensifying competition environment among the carriers and the long-term decrease of the incomes from the telephone communication fees. Both fixed and mobile carriers are accelerating the migration to full IP-based network in order to reduce the network operation cost and to provide new value-added services to make difference from other competitors. In particular, fixed mobile convergence (FMC) enables the integration of both fixed and mobile phones facilitating the creation of new value-added services. FMC is expected to create new market and new source of revenue for fixed and mobile service providers. In NGN, various services are provided by the service control function called IP Multimedia Subsystem (IMS), which is located in the service stratum of NGN. By introducing IMS, IP-based multimedia services are provided to various terminals (mobile terminal, wireless LAN (WLAN) terminals, etc.) independently of the access networks. Thus, in NGN, IMS is expected to be the common service control architecture applied to both fixed and mobile. Figure 5-1 shows the NGN architecture overview, which is defined in the ITU-T Recommendation Y.2012 [4].

IMS standardization was set by the 3rd Generation Partnership Projects (3GPP/3GPP2). IMS Phase 1 was completed by Release 5 issued by the 3GPP in 2003. Only the basic call connection was defined in Phase 1, however as a result of the following continuous functional extensions such as provisioning of multimedia services, Release 8 specification is currently being defined. IMS has been initially defined for mobile network and in later years IMS has been expanded by ETSI TISPAN and ITU-T as the NGN service control function for both fixed and mobile networks. Currently, 3GPP is also studying and developing common IMS standards for the fixed and mobile networks.

IMS comprises CSCF (Call Session Control Function), which controls sessions and services, MRF (Multimedia Resource Function), which controls multimedia

Next Generation Telecommunications Networks, Services, and Management, Edited by Thomas Plevyak and Veli Sahin

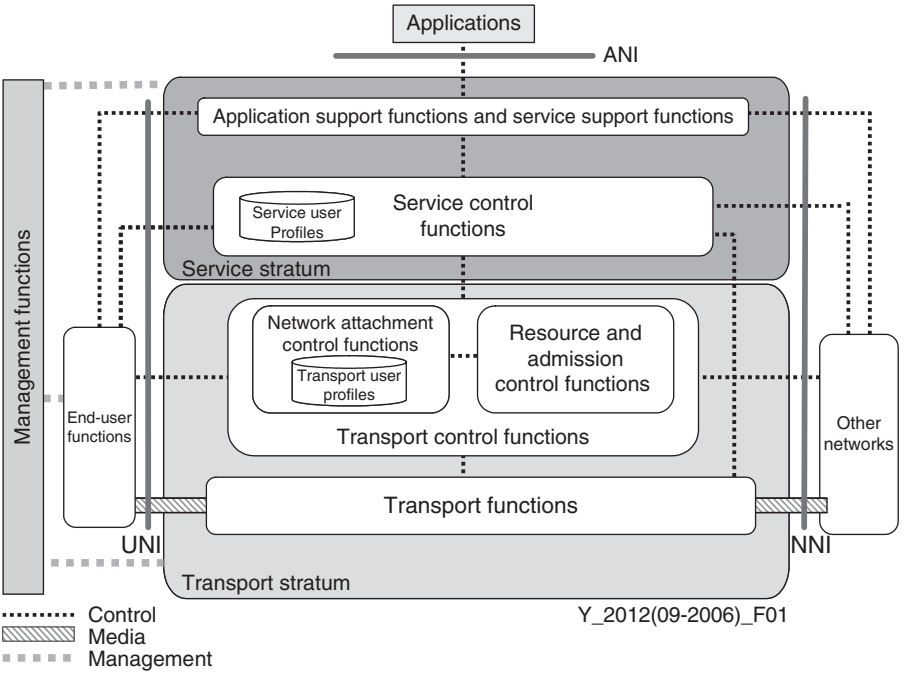


Figure 5-1. NGN architecture overview (ITU-T Rec.Y.2012 [4])

resources, HSS/SLF (Home Subscriber Server/Subscription Locator Function), which manages user profiles, media gateway MGW/MGCF (Media Gateway/Media Gateway Control Function), which performs the inter-working with the existing networks, and the application server (AS), which provides services and applications to be used in IMS. CSCF is a SIP server that controls sessions and services using the SIP protocol, and realizes the core features of the IMS architecture including user terminal access control, roaming control, and activation of the services that are provided by AS. Figure 5-2 shows the reference architecture of the IP Multimedia Core Network Subsystem, which is specified in 3GPP TS 23.228 [7].

5.1.1 Serving CSCF (S-CSCF)

S-CSCF performs session routing based on the destination address (SIP-URI, telephone number, etc.) specified by the initiating user and sets, manages, and releases the session between the initiating and terminating users by using user profile information and user location information managed by HSS. S-CSCF uses SIP-based standard interface called ISC (IMS service control) to connect with the common enablers (general-purpose function realizing individual services such as presence, messaging, etc.) shared by different services and the application servers controlling each service. S-CSCF can provide various services through the connection with multiple application servers. Open service environment (OSE) is introduced to

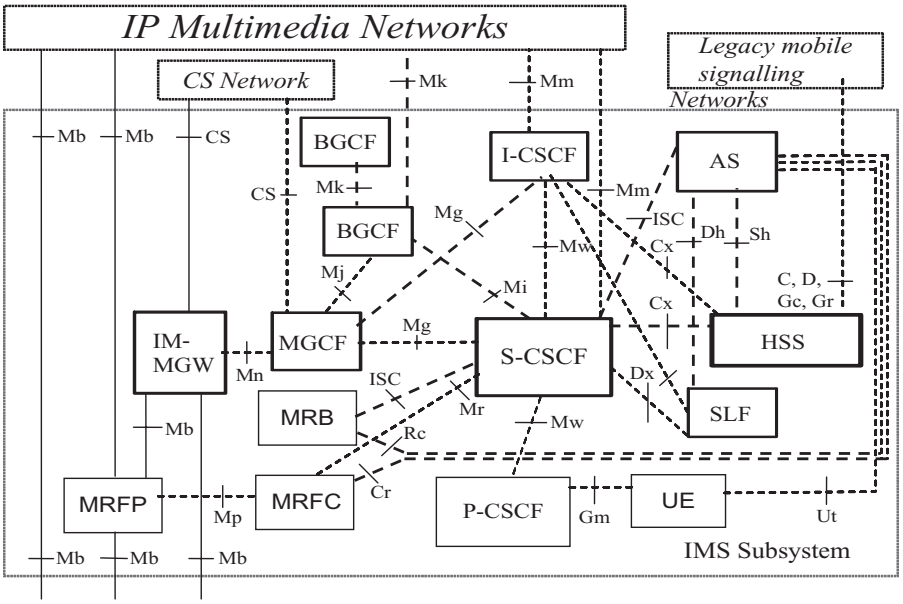


Figure 5-2. Reference architecture of the IP Multimedia Core Network Subsystem (3GPP TS 23.228 [7]). AS, Application Server; BGCF, Breakout Gateway Control Function; CS, Circuit Switched; HSS, Home Subscriber Server; I-CSCF, Interrogating-CSCF; MGCF, Media Gateway Control Function; MGF, Media Gateway Function; MRB, Media Resource Broker; MRFC, Multimedia Resource Function Controller; MRFP, Multimedia Resource Function Processor; P-CSCF, Proxy-CSCF; S-CSCF, Serving-CSCF; SLF, Subscription Locator Function; UE, User Equipment

facilitate the integration between IMS and various applications by converting the IMS service control (ISC) interface provided by S-CSCF into a logical easy-to-use API for the applications. As a result, it becomes possible to use the functions for setting and releasing sessions provided by IMS and acquisition of user location information from various applications and servers, thereby enabling flexible development and deployment of new services. In NGN, the application support function allocated in the service stratum realizes service reusability and service portability, and achieves connection with external applications provided by third parties through application network interface (ANI). Figure 5-3 shows the extended NGN architecture positioning the OSE which is specified in ITU-T Y.2234 [5].

5.1.2 Proxy CSCF (P-CSCF)

P-CSCF is connected to a user terminal through the access network and it is allocated during the connection of the user terminal. The network connection with a user terminal is realized through a packet switch called Gateway GPRS Support Node (GGSN) in the W-CDMA network, and through a relay router in the access type IP network for fixed broadband access and access from wireless LAN. For the user

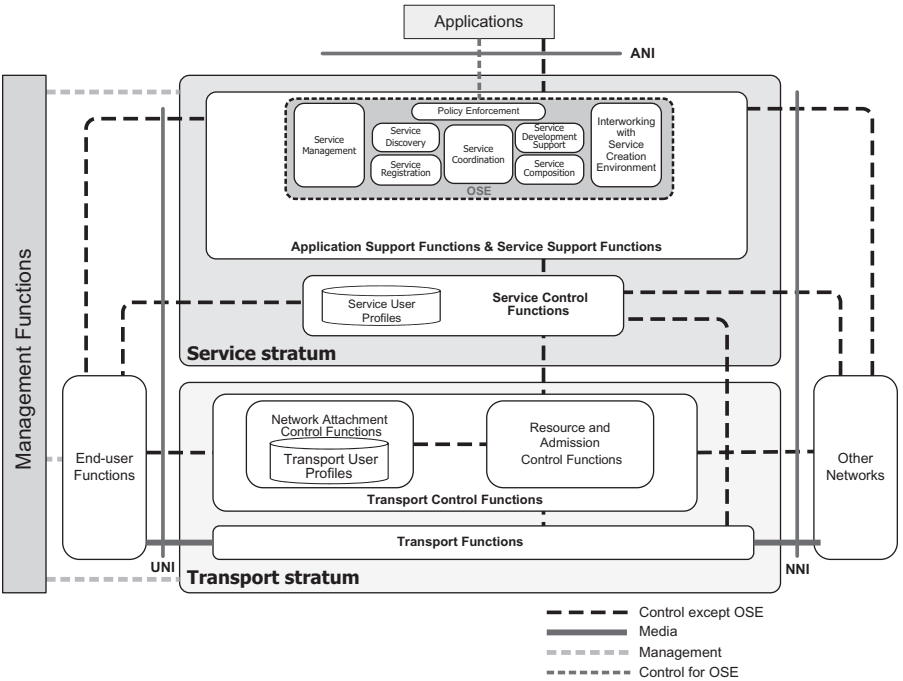


Figure 5-3. Extended NGN architecture positioning the OSE with expanded view of the OSE functional group

terminal connected to the access network, an IPsec tunnel is established with the user terminal after the authentication is performed at connection, and SIP messages from the user are transferred through IPsec, and the integrity of the messages is checked by P-CSCF. For efficient transfer of SIP messages between users, P-CSCF compresses and encodes messages as required. This function is particularly useful in the case of wireless access with limited signal channel bandwidth. Users can use either P-CSCF of the visited network or P-CSCF of the home network at roaming. When P-CSCF of the home network is used if the IMS function is not available in the visiting network, user traffic such as VoIP will also be routed through the home network. By contrast, if P-CSCF of the visited network is used, the traffic between users on the visited network is efficiently transferred locally within the same network. However, P-CSCF of the home network is always used when the user is in the home network.

5.1.3 Interrogating CSCF (I-CSCF)

I-CSCF, located in the home network, accesses the SLF when required at user registration and identifies the HSS that contains the subscriber information. Based on the instructions from HSS, I-CSCF passes registration processing to the S-CSCF that serves the user. When there are multiple HSS in the network, I-CSCF performs the load balancing smoothly and hides the network configuration from external resources.

5.2 IMS SERVICES

5.2.1 Push to Talk over Cellular (PoC) Service

The PoC service realizes 1-to-1 or 1-to-n voice connection between mobile phones. The first commercial service started by Nextel (currently known as Sprint Nextel) of the United States in 2002, this service helped to make difference from other competitors and attracted much attention due to its success related to its high average revenue per user (ARPU) and low customer churn. In Japan, the service started in November 2005 as a new way of communication, different from the traditional voice and mail services. The PoC service platform consists of the IMS platform (handling SIP session control (S-CSCF/P-CSCF) and managing subscriber data (HSS)) and the application server (PoC (AS)), which provides "session initiating/terminating control," "voice initiation control," and "floor re-entry control." Flexible service expandability is also achieved by concentrating the service-dependent features in the application server (PoC (AS)). The main role of PoC (AS) in the session initiating/terminating control function is as follows:

5.2.1.1 Service Authentication This function allows the verification and the authentication of the user before starting the PoC connection; when a mobile terminal requests PoC connection, validation of the terminal and check of the maximum allowed number of members is performed before starting the connection.

5.2.1.2 Floor Information Management A floor is created when a PoC service call occurs as a unit to manage the session. The floor information (identifier, establishment time, number of members, etc.) and information of members joining the floor (member names, status (calling, online, offline, etc.)) can be managed in an integrated manner. By managing the status of each member, the floor information management function notifies the user about the current status of opponent user.

5.2.1.3 Message Duplication and Transmission in 1-to-n Communication 1-to-n communication, which is a feature of the PoC service, is achieved by installing the function that duplicates and distributes the messages from an initiating mobile unit to all the receiving mobile units.

The PoC service requires voice initiation control since it applies a half-duplex communication mode. Voice initiation control is performed through RTP Control Protocol (RTCP) after receiving a voice initiation request from a mobile unit. By managing which user requests the voice initiation, the function enables deterring the voice initiation from other users. 1-to-n communication is enabled by duplicating voice data from the mobile unit with voice initiation and distributing it to other users using Real-time Transport Protocol (RTP). The service provides a re-entry function to enable the user who once left the floor to re-participate in the floor that is continuing. This function is necessary in the mobile environment, since nodes can be disconnected due to the absence of network signals or failures. When receiving a request from a user, the function checks whether the floor that the user wishes to join still exists. If the floor exists, the function connects the mobile unit to the floor. In addition

to the presence of the floor as a condition to approve re-entry, adding extra conditions for re-entry based on the service specification of the carrier is also possible.

5.2.2 IMS-Based FMC Service

IMS based FMC service commenced in July 2008 in Japan. In this service, when indoor, 3G/WLAN dual-mode terminal can use the home antenna (Wireless LAN Router) to get connected to a broadband environment (FTTH etc.) through the wireless LAN and then access the internet. with high speed packet transmission/reception up to 54Mbps. IMS based FMC service allows to use 3G services in the 3G service area (outdoors etc.) and when in the WLAN service area (indoors: inside the house), it allows to use VoIP and data access services provided by the IMS core functions; Call Session Control Function (CSCF) and Packet Data Gateway (PDG).

The function of each node that provides the IMS based FMC service is as follows.

5.2.2.1 CSCF As the core function of IMS, CSCF provides session (connection) control, management, authentication, routing, etc. through the SIP based call control. In the IMS-based FMC service, CSCF provides the VoIP service to 3G/WLAN dual terminal using SIP.

5.2.2.2 PDG PDG is a gateway that provides the functions required for the interconnection between the wireless LAN network inside the house and the 3G network. PDG ensures the security when the user connects to a 3G service from the wireless LAN network. Through this gateway, PDG provides users with the services difficult to be achieved by the 3G network only, such as large contents distribution service and low-cost IP telephone service.

In the IMS-based FMC service, initiating/receiving processing is performed using the number starting with 050 in the WLAN area and the number starting 080/090 in the 3G area at the initial commencement of the service. However, currently, one number is provided (number starting with 090/080) for both the 3G service area and the WLAN area for initiating/receiving processing. By using a single-number service, 3G/WLAN dual-mode terminal users can perform initiating/receiving processing with a single number (number starting with 090/080) in either the 3G or WLAN area. The single number service is realized by the interconnection between CSCF, which provides WLAN, and the 3G core network that provides the 3G services. The initiating user can transmit messages using a number starting with 090/080 without being conscious of the location of the receiving IMS based FMC service user, and receiving messages from the IMS based FMC service user is displayed with a number starting with 080/090 regardless of the location of the IMS based FMC service user. Thus, the usability of the FMC service has been enhanced.

5.2.3 IMS-Based IPTV Service

The standardization of IPTV provided by NGN is being promoted by various standardization organizations such as Open IPTV Forum, ATIS, ETSI TISPAN, and

ITU-T. In ITU-T, since 2006, three types of architectures of IPTV in Focus Group-IPTV have been discussed, namely non-NGN, non IMS based NGN, and IMS based NGN architectures. From 2008, the related SG such as SG9, SG11, SG13, and SG16 hold joint meetings as IPTV-GSI, and the formulation of recommendation is still under work. In this discussion, IMS is expected to be the service control platform which provides IPTV. In IPTV-GSI, formulation of recommendation for network architecture Y.1910 [2] was approved in May 2008 and at the same time, the service use case, Supplement 5 [3] to Y-series Recommendations, was approved as the supplementary document. In September 2008, the formulation of recommendation for the IPTV requirement condition Y.1901 [1] was approved, completing the basic recommendations for providing IPTV through IMS-based NGN. QoS (Bandwidth/Priority Control) Guarantee, user authentication, billing, profile management, mobility, FMC realization, provision of services for users in different networks during roaming etc. are the key merits of selecting the IMS as a service control platform for IPTV services. By integrating services provided by IMS such as VoIP, realization of blend services such as display of the call ID on the screen while receiving a call or messages during viewing of IPTV. Realization and control of seamless contents delivery to the terminal by integrating IPTV with presence information is being studied.

5.3 QoS CONTROL AND AUTHENTICATION

This section describes QoS Control function and authentication function required for NGN. These functions are provided respectively by Resource and Admission Control Subsystem (RACS) and Network Attachment Subsystem (NASS) in the transport stratum. Figure 5-4 shows the system configuration including RACS and NASS.

RACS and NASS, cooperating with the Service Control Function in the service stratum, perform QoS control and authentication. The details are described in the following sections.

5.3.1 QoS Control in NGN

Different from the traditional networks individually assuring the service quality, NGN, which is fully IP-based and handles a wide variety of media and services in an integrated manner, is required to provide these services without failure or downgrading the quality level. In an IP-based environment, it becomes easier to implement on-demand broadcasting and services cooperating with Web applications, however, the quality of existing services (e.g., telephone services) must be guaranteed. Specifically, assurance must cover voice service without delay or loss, priority control of emergency calls, quality of calls from start to end, etc., all of which require QoS control at end-to-end level.

NGN performs packet transfer according to the priority when service traffic passes through a network. In this case, since the priority control can be performed separately to each call session based on the authentication information of the relevant

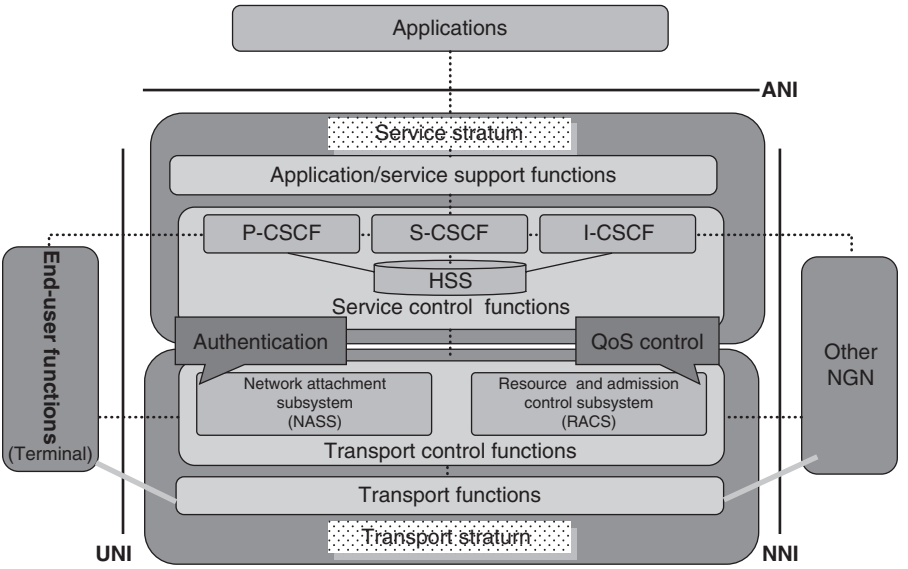


Figure 5-4. Overview of NGN architecture

session, the service levels can be provided by classifying the voice calls into emergency calls and ordinary calls, or per-user charging basis.

NGN also performs admission control for QoS assurance. Specifically, by managing the network bandwidth, NGN secures the bandwidth used by priority traffic for which communication is permitted through acceptance control, and controls malicious/congested traffic. Since the edge router opens and closes the RTP port interlocking with call control through the control from RACS, calls during congestion and the spoofing traffic not compliant to the formal SIP negotiation can be restricted. As a result, the legacy call quality and security are ensured.

5.3.2 RACS

RACS is a subsystem that provides admission control function and gate control function defined by the ETSI TISPAN standard. QoS control in NGN is implemented by RACS, thereby added values such as service levels can be provided.

5.3.2.1 Functions Provided by RACS RACS provides the following functions:

1. *Admission control.* Performs admission of QoS resource requests based on the user profile, operator-specific policy rules, and resource reservation provided by NASS.
2. *Resource reservation.* Verifies if the QoS resource request is within the permitted bandwidth in the access network, and reserves the resource.
3. *Gate control.* Provides NAPT (Network Address Port Translation) control and priority traffic control, and performs gate control of the edge router based on the approved QoS resource request.

5.3.2.2 Function Blocks Comprising RACS RACS consists of the following function blocks:

1. *A-RACF (Access-Resource Admission Control Function).* Performs QoS control to ensure the communication quality for the access network.
2. *SPDF (Service Policy Decision Function).* Receives a resource reservation request, and determines the policy.

Figure 5-5 shows the network components associated with QoS control and the control procedure. The control procedure is as follows.

<1> In the access authentication when starting the access to the network from a terminal, RACS receives and retains the QoS profile from NASS.

<2> The originating terminal sends a session initiation request (SIP message) to CSCF.

<3> CSCF sends a QoS resource request to RACS together with the information such as the bandwidth required for service execution, service class, and reservation priority.

<4> After receiving the QoS resource request, RACS collates the requested conditions with the retained user profile and edge router information, and performs admission control. RACS also calculates the bandwidth value required for guaranteeing the service quality.

<5> RACS performs gate control for the edge router based on the calculated bandwidth value.

<6> RACS responds about the securing of the QoS resource to CSCF.

<7> CSCF sends a session initiation request to the terminating terminal.

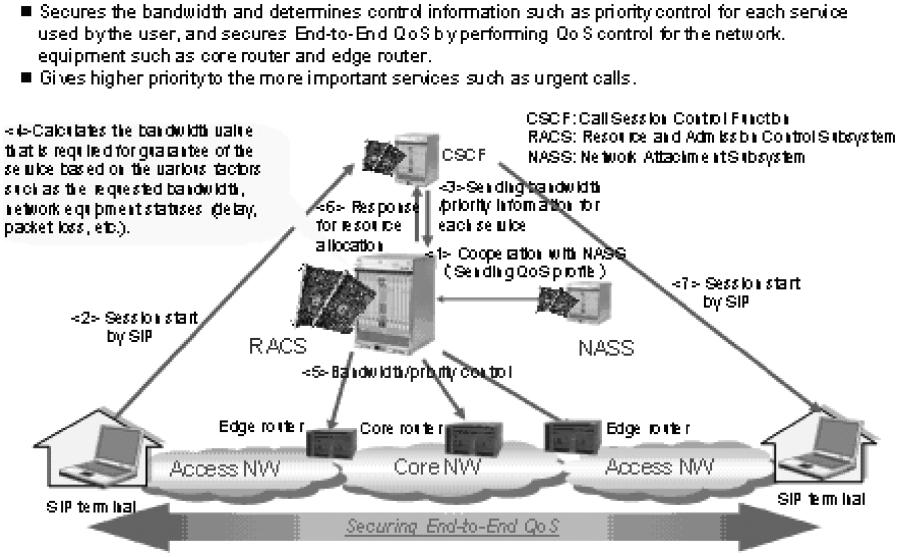


Figure 5-5. Network components and control flow for QoS

5.3.3 Authentication in NGN

In NGN, authentication is defined in two layers: authentication at the access level for allocating IP addresses and authentication at the service application level in order to use SIP. NASS performs authentication at the network access level based on the user profile.

Roles and functions are specified as follows:

1. *Profile management.* Manages user profiles (subscriber ID, access ID, location information, etc.).
2. *Access authentication.* Receives a connection request from a terminal and performs authentication at the access level based on the user profile.
3. *DHCP (Dynamic Host Configuration Protocol) server function.* Assigns an IP address to the terminal.
4. *Connection information management.* Manages the connection information and the IP addresses of the currently connected terminals.
5. *RACS Interaction.* Manages QoS profile information required for RACS bandwidth management, and provides QoS profile information to RACS.

5.3.4 NASS

NASS is a function to perform IP address distribution and authentication defined in the ETSI TISPAN standard. NASS consists of NACF, CLF, UAAF, PDBF, AMF, and CNGCF functions blocks.

1. *NACF (Network Access Configuration Function).* It assigns IP addresses.
2. *CLF (Connectivity Session Location Function).* Manages the assigned IP address information, and transfers QoS profile information containing the IP address and QoS information to RACS.
3. *UAAF (User Access Authorization Function).* Performs authentication based on the user profile information.
4. *PDBF (Profile Database Function).* Manages user profile information (e.g., subscriber ID, subscribed services etc.).
5. *AMF (Access Management Function).* Distributes requests from terminals to NACF/UAAF.
6. *CNGCF (Customer Network Gateway Configuration Function).* Performs additional terminal settings not implemented by NACF.

Figure 5-6 shows the authentication procedure and related network components. The authentication procedure is described as follows:

<1> Terminal requests access authentication to NASS when initiating the access to the network.

<2> NASS verifies the profile information such as the subscriber ID, physical access ID, and logical access ID for the terminal connection request, and performs authentication.

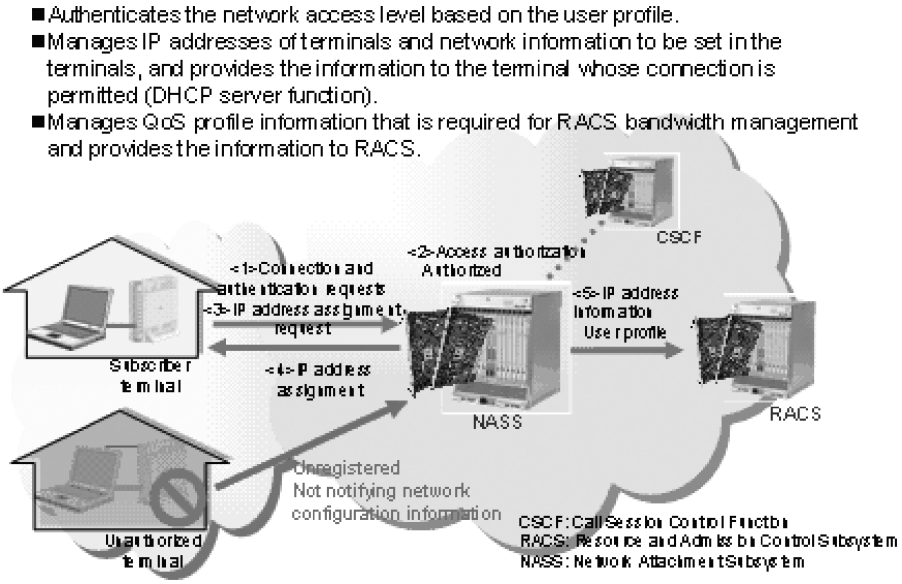


Figure 5-6. Network components and procedure for authentication

<**3**> The authenticated terminal requests IP address assignment to NASS by sending a DHCP request.

<**4**> NASS assigns an IP address to the terminal through DHCP.

<**5**> When interacting with RACS, NASS sends the QoS profile information to RACS together with the subscriber ID and the IP address. (See <1> of the QoS control procedure in Section 5.3.2.2)

5.4 NETWORK AND SERVICE MANAGEMENT FOR NGN

5.4.1 Introduction

Considering the diversity of services provided in NGN, demands for high quality, evolution of network technologies, and diversity of providers conducting businesses on the NGN environment, the NGN management functions must meet not only the requirements for traditional existing networks but also those from multifaceted aspects.

This chapter describes the requirements of NGN management by classifying them into the following categories:

- Network management operation requirements
- Service management operation requirements
- Service enhancement requirements

- B2B realization requirements
- Compliance with legal regulations requirements

In each category, the requirements for FCAPS are listed and described in Table 5.1. FCAPS refers to the Fault management, Configuration management, Accounting management, Performance management, and Security management. They are represented as the general management functionalities in the ITU-T Recommendation M3400 [6].

TABLE 5-1. Requirements for FCAPS

No.	Function	Description
1	Fault management	The fault management allows detecting a fault event in the network, identifying the cause of fault, locating and minimizing the impacts of the fault on services, arranging operations (issuing a trouble ticket), analyzing faults, and providing fault recovery. The fault management supports the following features: • Fault monitoring • Fault isolation and identification of the major causes • Fault diagnosis • Fault recovery • Trouble management
2	Configuration management	The configuration management provides NE (Network Element)/Path Route configuration management, NE parameter management, synchronization and modification management of configuration information with current network, status data collection, configuration information setting to NE, and NE control. The configuration management supports the following features: • Network planning and designing • Network construction • Service planning • Service provisioning • Status management and control
3	Accounting management	The accounting management allows measuring the network services usage amount per user, and notifying the amount to the service provider (service department). The account management also allows sending notifications to the users about their network services usage fees. The performance management supports the following features: • Measurement of the services used amount • Usage fee management • Billing, payment, and credit management • Settlement among service providers

TABLE 5-1. Continued

No.	Function	Description
4	Performance management	The performance management allows measuring, analyzing, and reporting the performance and the quality of the NE and the network. The performance management also allows collecting of NE and Network statistic information, either periodically or at ad-hoc, comparing the threshold values, analyzing the data, and confirming the existence or absence of problems. NE performance data, network traffic data, and QoS data are object to analysis. The performance management supports the following features: • Performance data collection/traffic data collection • Performance analysis/traffic analysis • Network capacity analysis • QoS data collection • SLA (Service Level Agreement) determination QoS data includes, for example, packet loss, delay, and jitter as flow quality for VoIP and video services. If these are defined as the SLA conditions, the performance management compares the measured values with the conditions, and determines the quality of service.
5	Security management	The security management provides functions to detect security abnormal events on networks (e.g., security violation event) and to audit security. The security management also provides management functions such as user authentication among systems and among user systems in the Network Management system, access control, and operation log history. The security management supports the following features: • Security abnormality monitoring • Security abnormality prevention • Security recovery • Security auditing

5.4.2 Network Management Operation Requirements

From the viewpoint of network operation management, reduction of network operating cost must be compatible with high-quality network maintenance. The major requirements include efficiency in providing network resources satisfying the demands, assurance for service provisioning quality, prompt and immediate interventions during failures, proactive handling against failure warnings, and real-time accounting. These requirements are described below:

Configuration Management:

- Providing the ability to manage NGN system resources, both physical and logical (including resources in the core network, access networks, interconnect components, and customer networks and their terminals)
- Integrating an abstracted view on Resources, which is hiding complexity and multiplicity of technologies and domains in the resource layer
- Efficient network expansion according to the network utilization status
- Provision of efficient test tools during network expansion

Fault Management, Performance Management, and Security Management:

- Provision of integrated monitoring
- Monitoring of network service quality (QoS)
- Early detection of network failures and QoS deterioration and identification and isolation of failure causes at early point.
- Advance detection of failure indicators
- The ability to have proactive trend monitoring

Accounting Management:

- Collection and accounting (rating) of service usage information in real time
- Supporting the availability of management services any place any time to any authorized organization or individual (e.g., access to billing records)

Common Functions:

- Automation and acceleration of end-to-end operation process

5.4.3 Service Management Operation Requirements

From the viewpoint of service management operation, service provisioning quality maintenance must be compatible with operating cost reduction. Since the quality of services has a direct relation with customer satisfaction, addressing the requirements from customers is quite important. The requirements from the viewpoint of service management operation are as follows.

Configuration Management:

- Automation and acceleration of service provisioning
- Automation of provisioning from service level to network level
- Automatic testing linked with service orders
- Customers' self-service provisioning

Fault Management, Performance Management, and Security Management:

- Monitoring at SLA provisioning level
- Early detection of SLA violation and early identification of failure causes
- Analysis of affected range at failure occurrence or QoS deterioration, and early notification to customer

- Prompt notification to customer at SLA violation
- Service quality confirmation test at customer inquiry, dispatch of maintenance operation, and operation progress status notification

Accounting Management:

- SLA-based accounting adjustment
- Service usage logs and provided quality tracing
- Real time information on accounting and settlement status for users

5.4.4 Service Enhancement Requirements

Increase in highly sophisticated services due to the high-functionality equipments and the advancement of video services increases the needs for device remote control, video quality of experience (QoE) measuring, and other customer support requirements. In addition, it is also required to cope with service personalization based on the user access method and context information (location and presence). Since the advancement of services involves in the reduction of services lifecycle, lifecycle management has become necessary as a service management platform.

Based on this background, the following requirements need to be considered:

Configuration Management:

- Remote settings for terminals (mobile terminals and CPE) and firmware update
- Service provisioning function corresponding to service lifecycle reduction

Fault Management, Performance Management, and Security Management:

- Collection of quality information from terminals (mobile terminals and CPE)
- Monitoring quality of experience (QoE)

Accounting Management:

- Accounting function corresponding to service lifecycle reduction
- Accounting model corresponding to user segmentation and access method

Common Functions:

- Collection of user context information (presence, location, preference, etc.) from terminals
- Providing user context information to service functions
- Protection of user context information

5.4.5 B2B Realization Requirements

In NGN, it is necessary to realize B2B process between the service providers, as well as between NGN providers. The requirements for B2B realizations are as follows:

Configuration Management:

- Service provisioning functions covering multiple providers

Fault Management, Performance Management, and Security Management:

- SLA-based SLA monitoring among multiple providers, and dispatching of SLA violation notification to the provider

Accounting Management:

- Inter-provider settlement function for distributing income among multiple providers

Common functions:

- Disclosure of user context information to 3rd parties

5.4.6 Compliance with Legal Restrictions Requirements

In NGN, the legal regulations imposed on the existing communication services must be observed continuously and the operation functions must be provided for the following requirements:

- Emergency communication
- Lawful interception
- Confidentiality of communication contents
- Storage of communication records
- Protection of personal information

5.5 IMS ADVANTAGES

This section describes various advantages of the IMS platform to be constructed under a multi-vendor environment according to the international standards. Cost reduction for operation and maintenance, and quick provisioning of a wide variety of services using open interface installed in the upper level of the Service Delivery Platform (SDP) over IMS, will be described particularly in this section.

5.5.1 Reduction of Maintenance and Operating Cost

The IP-based network enabled the integration of fixed and mobile networks allowing not only the migration of telephone networks but also the diversity of communication services such as FMC and rich multimedia services and the shifting of businesses to the non-traffic field. Under such circumstances, communication carriers find themselves required to shift their investments to the service and IT fields more than ever by improving the operation efficiency while ensuring safe and secure networks.

On the other hand, IMS, whose specifications are defined by 3GPP, is a system that provides IP-based multimedia services to mobile phones and WLAN terminals independently of the access network. Rather than providing only IP-based services, IMS can also provide services by interacting with PSTN and the Internet. IMS employs SIP as the core control protocol. In the traditional architecture, since SIP depends a lot on the implementation specifications, the interconnectivity needs to

be thoroughly examined. However, by employing SIP as IMS, interconnectivity among communication carriers has become simple.

In these circumstances, the following advantages can be listed for communication carriers to introduce IMS from the viewpoint of business investments.

5.5.1.1 Reduction of Time Required for Introducing New Services (Time to Market) By providing an open interface through employment of the open service architecture, service development and deployment become faster. Using the open interfaces, personalized services can be created and provided by service operators and third-party application providers.

5.5.1.2 Cost Merits Introduction of IMS enables effective use of facilities, for example, voice and data that have been handled separately in the traditional method can be integrated. In the traditional architecture, a system has been individually constructed for each service; however, in IMS a variety of services can be implemented in the common service platform, which facilitates inter-working among these services and leads accordingly the reduction of costs for development, maintenance, and operation. By realizing a multi-vendor environment based on the standard architecture, optimum components can be installed with less cost. Interconnections among communication carriers for basic services become easy, enabling communication carriers to provide differentiating services and make investments by introducing services at higher levels.

5.5.2 Roles of SDP and Development and Introduction of New Services

In NGN, the key issues for communication carriers and service providers are how to develop and deploy efficiently new nontraditional differentiating services. The Service Delivery Platform (hereinafter referred to as SDP) responds to the above demands. SDP is attracting much attention as a common platform to provide various functions ranging from service development, operation and maintenance, and accounting to user management functions.

5.5.2.1 Positioning of SDP in NGN Figure 5-7 shows the positioning of SDP in the NGN architecture. SDP is a platform belonging to the application layer positioned in the upper level of IMS. SDP consists of a set of service execution functions called service enablers and various service control/management functions. The following are examples of service enablers (Application Servers (AS)):

- Call Control AS
- Presence AS
- Media Resource Control AS

These application servers use SIP and other protocols to inter-work with the nodes in the control layer. The application servers also provide open APIs as easy-to-use programming and interfaces to realize the interaction with external systems. These open APIs allow developers to develop and deploy services easily without requiring knowledge of the network control layer configuration and protocols.

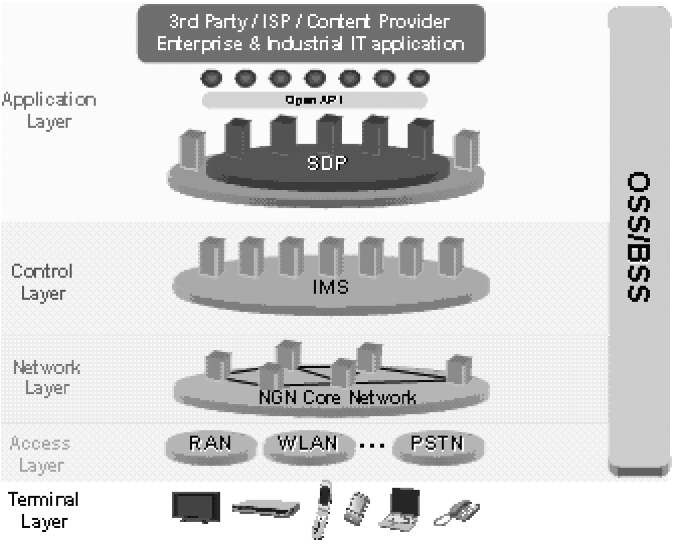


Figure 5-7. Service delivery architecture for NGN

SDP realizes the integration of IT applications (e.g., business systems) and Internet-based Web services with the SIP-based communication platform, enabling quick development and fast delivery of new services as well as expansion of service area.

5.5.2.2 Features of SDP This section describes the features of the SDP.

1. *Fast service development/deployment.* Java/SOAP (Simple Object Access Protocol)/REST (Representational State Transfer) and others provide easy-to-use Open APIs to improve the development time-frame and allow fast deployment of new services.
2. *User-friendly programming.* The SIP support interface verifications and connection tests required during each services development in the traditional structure are no longer necessary; SDP hides the complicated SIP call control procedures.
3. *Flexible system configuration.* In the SDP configuration, the application servers providing individual services are located on top of the commonly used application servers providing the control of services. This configuration allows easy deployment of new services and flexible scalability of the system depending on the type and scale of the services.

5.5.2.3 Examples of Application Servers This section describes the key Application Servers of the common service execution layer.

Call Control. Call control AS realizes various connection controls as value-added services. Call control provides simple programming APIs to be easily handled

by the application programmers, and allows the control of SIP-based services (e.g., two-party call, voice distribution etc.) from the application.

The call control performed based on program logic, on manual operation, or on event occurrence is referred to as 3PCC (3rd Party Call Control). The call control AS is considered as the SIP application server realizing the 3PCC function. In addition to the basic call control, the APIs provided by the call control AS enable also transferring and combining of the calls in progress. For example, it is possible to play voice guidance during the call, transfer the call, or switch from two-party call into a conference call.

Presence. Presence AS manages the presence status of either a person or a machine, allows the search and the update of the presence information from terminals and applications, and notifies terminals and applications about the new presence information when updated. The contents of presence information could be an "activity"; Available/Busy/At Lunch, "location"; Home/Office/Café, "mood"; Happy/Angry/Puzzled, "privacy"; Public/Private, or "detailed location"; Latitude/Longitude and Tokyo/New York/London.

In the presence service, the party that references or views the presence information is called "watcher" and the party whose presence information is referenced is called "presentity." Presence AS provides access control function to prevent the "watcher" from referencing the presence information without the permission of the "presentity" or of the presence AS administrator. Both the "watcher" and the "presentity" can be either a terminal or an application. For example, the "watcher" can be a terminal while the "presentity" can be another terminal, or the "watcher" can be an application while the "presentity" can be a terminal etc.

The presence information is used in various scenes. For instance, the presence information is very helpful in selecting the convenient communication media when trying to contact another party. If the opponent is in the office at work for example, then a phone call may be appropriate, but if he or she is in the middle of a conference, then the caller can either choose to call in a later time or send an instant message. The Presence AS also allows the calls to subscriber's home phone to be forwarded to his or her mobile phone when the subscriber's presence status is set to "Outside." This kind of call forwarding is called "presence-based call forwarding."

Media Resource Control. Media Resource Control AS provides the audio and video control functions. It is used for example to transmit voice messages or to set a video conference etc. The following are examples of provided media control functions:

Media transmission: This is used for example to send a voice message to a terminal, or to play selected calling tone (CRBT (customized ring back tone)) to the caller while waiting for the Callee to answer the phone, or also to play IVR (interactive voice response) synthetic speech, etc.

Media mixing and media distribution: This is used to mix the media from multiple members participating in a voice or video conference and then distribute it to the conference participants.

Media recognition: This function includes DTMF detection and speech recognition. The application is notified about the detection and recognition results.

Media storage: This function enables the user to store and play of recorded voices similarly to the answering machine (voice mail) service.

Messaging. By the interaction with the applications, messaging AS performs transmission/reception of SMS (short message service) and MMS (multimedia message service). Message types include texts, images, videos, and ringtones. Messages can be sent from an application by specifying the message type and the recipient address (terminal URI). The message transmission result notification can either be received automatically or stored to be checked later.

One of the service examples is a simultaneous broadcasting service used in emergency cases, such as transmission of evacuation messages to the residents of a specific area during Tsunami forecast.

Location. Location AS manages the location information (latitude, longitude, precision, time stamp, etc.) of the terminal and provides this information as a response to the request from the application. Several methods are used to determine the terminal location; the method of using a GPS device in the terminal, the method of determining the location information of the base station to which the mobile terminal is connected, and the method of determining the location information of the nearest wireless LAN access point to the terminal.

The PULL type and the PUSH type are available for obtaining location information of a terminal from an application. In the PULL type, the application specifies an URI (such as SIP-URI and TEL-URI) used to obtain the location information, of a specific terminal, stored in the server. The PUSH type includes the periodic notification of the location information of a specific terminal, and the notification of the URI of all terminals that entered or exited a specific area to the application.

As examples of services using location AS, sale/discount information provided by the shops can be transmitted to the subscribers passing by the shop, and also warning messages can be sent to the person who intruded into a prohibited area.

Device Management. Device management AS provides remotely and in a centralized manner the management of devices; mobile phone/PDA/PC/car navigator/game equipment/etc. Management functions include updating of the firmware, collecting of devices power status (ON/OFF), remotely locking the devices, and restrict/release of specific device functions.

For example, Device Management AS can provide a “device fault remote diagnosis service” where device failures are analyzed remotely through the collection of the device logs and status, and repairs are performed promptly and automatically. The log data collected from devices used to play games for long time can be used for marketing. If a device is lost or stolen, the device can be locked and the data can be remotely wiped from the device (Lock & Wipe) increasing user security.

AAA. AAA AS is a server that performs authentication, authorization, and accounting. Authentication is to authenticate an individual or service provider based on the ID and the password. Authorization is to check the utilization authorization or access authorization before approving the access. Accounting is to record approved conducts. AAA AS can perform authentication based on the NGN authentication or IMS-AKA authentication. Interaction with OpenID enables using IDs simultaneously in multiple websites. Authentication adopting the single login feature allows the user to automatically log-into the other services once he logged into one service. Online settlement feature can also be realized through the interaction with settlement systems (e.g., electronic money, credit card).

User Profile Management. User profile management AS manages personal information and preference information of end users. Personal information includes the name, date of birth, address, telephone number etc., and preference information refers to the field of interest of each user (baseball, travel, jewel, etc.). As a service example, the "recommendation service" that allows providing suitable goods information to the user based on the user profile and user's purchase history. Another example is the "target advertisement system" that based on the user preference, user activity history, and time, selects appropriate persons from those who are near the restaurant, and sends an advertisement or information about the restaurant.

5.5.2.4 API Parlay is one of the telecommunication industry standard APIs (Application Programming Interface). Parlay is developed and standardized by the Parlay group formed by members from telecommunication related companies and IT companies, Parlay is also defined as part of OSA (Open Service Architecture) API in the 3GPP standard.

Parlay API is designed by abstracting the section related to the hardware, enabling the common use of the API without being conscious of the differences between fixed and mobile network, current network, and NGN. It also aims at enabling various applications to access the network resources of carriers from remote sites.

In addition to Parlay, Parlay-X is released to be used in telecommunication field. While Parlay is a set of APIs intended to be used by application developers familiar with Java and other programming technologies enabling detail control, Parlay X is designed to enable the application developers to access from external sites and make use of the functionalities, assets and resources of the carriers' network. Parlay X enables the use of communication services from the applications via Web Service messages. Parlay X can be used via SOAP making application development easier and simpler than Parlay.

Considering the recent rise of Web services in the communication market, the future prospect of Parlay X is promising as the API uses SOAP, which is highly compatible with Web services.

Parlay X APIs enable the control and management of services including but not limited to Call Control, Messaging, Presence, Location, Account, Terminal Status, etc.

5.5.3 Services Implemented on NGN

With the popularization of IP-based networks and diversification of services, the PoC (push to talk over cellular) service described in Section 5.2.1.1 has been extended from a voice-based solution to a multimedia solution (from push to talk to push to X), the development of presence and location based FMC services, and the integration of communication and broadcasting services (IPTV) are expected to significantly increase. In addition, the communication ways are also expanding from a simple communication services to a variety of services more related to the actual daily life and from person to person communication to person to machine, and then machine to machine communications.

The following sections give examples of prospective services to be implemented on NGN and discuss the relation with IMS and SDP.

5.5.3.1 Push to X PoC is a half-duplex call service that allows the user to transmit a voice by pressing a button on the terminal, similar to the transceivers and business radio equipments. By making use of the NGN and SDP features, Push to X (where X refers to "any") was developed as an enhanced solution of PoC, handling other types of multimedia.

Push to X is a communication service realized by making use of the Enablers provided in the SDP, and NGN capabilities; QoS, real-time communication, etc. Figure 5-8 shows an implementation example. Push to X includes call control (CC), presence (PR), messaging (MS), and media resource control (MR) application servers. The functions provided by these application servers are used by the Push to X application through APIs.

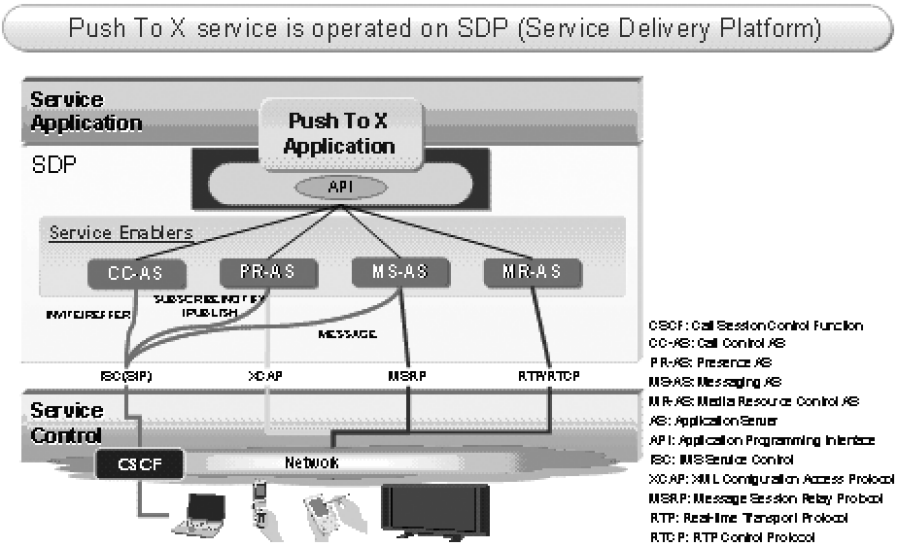


Figure 5-8. "Push to X" on SDP architecture

In addition to the transceiver-like voice solution, Push to X provides end users with more realistic and diversified ways of communication. Push to X provides, image sharing, video sharing, whiteboard sharing, Web sharing, and text chatting. Push to X solution is expected to be a rich communication tool within family or community members, or to be also used as a groupware.

5.5.3.2 IPTV IPTV is considered one of the promising services that can be realized on top of NGN.

There are various definitions for IPTV, however, this document follows the definition given by international standardization organization, ITU-T. IPTV is defined by ITU-T as follows:

"IPTV is defined as multimedia services such as television/video/audio/text/graphics/data delivered over IP based networks managed to provide the required level of QoS/QoE, security, interactivity and reliability." Basically, IPTV is not an NGN-unique solution. Services can also be provided to users in the existing networks as long as these networks are IP-based.

5.5.3.3 IPTV Architectures Three different architectures are defined for IPTV. Figure 5-9 shows three IPTV architectures.

Non-NGN. In this case NGN is not used, services are provided by using the Internet or the operator's closed network. Since the existing network is used in this case, the initial cost is generally low. However, in many cases, vendor-unique specifications are applied. Most of these specifications are not standardized, resulting in the remaining of various issues on interoperability or interconnectivity.

Non-IMS (NGN). In this case part of NGN is used, however, IMS is not used (non-IMS). Although the NGN functions are used for the security and bandwidth control, IMS is not used for the control. For Non-IMS IPTV, in most cases

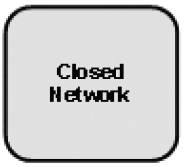
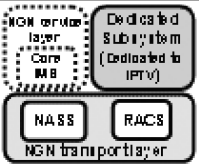
Mode		Non-NGN	NGN	
			non-IMS based IPTV (Dedicated Subsystem)	IMS-based IPTV
Network outline diagram				
Overview		Mode that provides IPTV in a closed network	Mode that installs IPTV functions in the subsystem different from Core IMS	Mode that installs IPTV functions together with Core IMS
Standard-ization group	TISPAN	X	O	O
	ITU-T	X	O	O
	ATIS	X	O	O

Figure 5-9. Comparison of IPTV architectures

special systems are required in order to integrate IPTV with the existing IMS services such as telephone, presence, and PoC.

IMS-based (NGN). This is an IMS-based case, where IMS is used for the security and bandwidth control. In this case, the interaction of IMS IPTV with the existing IMS services (e.g., telephone, presence, and PoC) can be easily performed, and the management and accounting systems of IMS can also be reused.

5.5.3.4 Advantages of NGN (IMS-based) IPTV As described in the previous section, several implementation modes are available for IPTV. This section describes the advantages to implement IPTV in NGN (IMS-based) mode.

Enhanced Video and Sound Quality. At present, key applications using the network include Web browsing and message transmission/reception. The control protocol provides the re-transmission of the data when packet loss occurs within the network, ensuring the browsing and reception of correct data by the end users. It also minimizes the delays during the network packet delays. Therefore, even in an Internet-based network where the bandwidth is not guaranteed, users do not encounter serious problems.

However, in IPTV, the end user receives the transmitted videos and sounds in real-time. Therefore, when packet loss or delay occurs within the network, the problem cannot be solved by re-transmitting the packet, causing fuzzy reception of videos and sounds troubles to the end user.

Compared with this, introducing the bandwidth guarantee mechanism of IMS, the bandwidth required by the user application is secured on demand, thus occurrence of packet loss and delay can be controlled. This enhances the quality of videos and sounds, and improves the user experience quality.

Control of CAPEX/OPEX. When IPTV is implemented in IMS, the accounting and bandwidth guarantee mechanisms can be standardized with that of the telephone service. Therefore, the providers who have already been implementing telephone services on IMS can reduce the operating cost for service maintenance and the initial investment cost during the implementation of IPTV service by sharing part of the systems of the telephone service.

Taking the above into consideration, contrarily to the Non-IMS which requires special systems for bandwidth guarantee and accounting, the IMS-based system has better advantages and can be easily realized as a business model.

Improvement of Usability. The standardization of the existing services such as telephone, presence, and PoC in IMS, facilitates the interoperability among multiple vendor equipments. When IPTV is implemented on IMS, other IMS services can be easily integrated with IPTV. For example, the caller's phone number and name can be displayed on the IPTV terminal screen when the user receives a call while watching TV. It is also possible to record the IPTV program while talking on the phone. The mash-up of multiple services improves the convenience and user-friendliness of solutions.

Quicker Service Delivery. The IPTV services are not limited to the videos and sound transmission. The IPTV service includes distribution of advertisements according to the users' preferences and also control of the contents addressed to children. By implementing such services on SDP as described above, multiple types of advertisement distribution engines can be selected and new services can be created easily and quickly.

As described above, implementing IPTV on top of IMS has better advantages compared to the other modes of implementation. IMS-based IPTV is regarded as one of the most important items by the NGN standardization organizations (ITU-T, TISPAN etc.), and is formulated as part of the NGN Release 2 (NGN Release 1 mainly handles the telephone service). In addition, the IMS-based IPTV interoperability tests between multiple vendor equipments in GMI (Global MSF Interoperability) clearly indicate that IMS-based IPTV is attracting a lot of attention. From these reasons, the IMS-based IPTV service is expected to be one of the promising key services that utilize the features of NGN.

5.6 REFERENCES

1. ITU-T Recommendation Y. 1901. Requirements for the Support of IPTV services, 2008. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
2. ITU-T Recommendation Y. 1910. IPTV Functional Architecture, 2008. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
3. ITU-T Y. 1900 Series, Supplement 5. IPTV Service Use Cases, 2008. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
4. ITU-T Recommendation Y. 2012. Functional requirements and architecture of the NGN release 1, 2006. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
5. ITU-T Recommendation Y. 2234. Open service environment capabilities for NGN, 2008. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
6. ITU-T Recommendation M. 3400. TMN management functions, 2000. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
7. 3GPP. 2008. IP Multimedia Subsystem (IMS); Stage 2 (Release 8). 3GPP TS 23.228 V8.7.0. Sophia-Antipolis, France: 3GPP Mobile Competence Centre.

5.7 SUGGESTED FURTHER READING

1. ITU-T Recommendation M. 3060. Principles for the Management of Next Generation Networks, 2006. Geneva, Switzerland: International Telecommunication Union Telecommunication Standardization Bureau.
2. TM Forum. 2008. NGN Management Strategy. TR133. Morristown, NJ: TM Forum.
3. ETSI. 2005. ETSI TR 188 004 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; OSS vision. Sophia Antipolis, France: European Telecommunications Standards Institute (ETSI).
4. ETSI. "TISPAN." http://www.etsi.org/tispan/ (accessed October 1, 2009).
5. ETSI. "ETSI Standards." http://www.etsi.org/WebSite/Standards/Standard.aspx (accessed October 1, 2009).
6. 3GPP. 2003. Open Service Access (OSA). Sophia-Antipolis, France: 3GPP Mobile Competence Centre.

7. Open Mobile Alliance. “Presence and Availability Working Group.” http://www.openmobilealliance.org/technical/PAG.aspx (accessed October 1, 2009).
8. Open Mobile Alliance. “Messaging Working Group.” http://www.openmobilealliance.org/Technical/MWG.aspx (accessed October 1, 2009).
9. Open Mobile Alliance. “Location Working Group.” http://www.openmobilealliance.org/Technical/LOC.aspx (accessed October 1, 2009).
10. Open Mobile Alliance. “Device Management Working Group.” http://www.openmobilealliance.org/Technical/DM.aspx (accessed October 1, 2009).
11. Open Mobile Alliance. “OMA Push to talk over Cellular V1.0.2” http://www.openmobilealliance.org/technical/release_program/poc_v1_0.aspx (accessed October 1, 2009).