INVITED PAPER   *Special Section on Next Generation Network Management*

Towards Management of Next Generation Networks

Mi-Jung CHOI[†] *and* James Won-Ki HONG[†a)], *Nonmembers*

SUMMARY   Next Generation Network (NGN) is envisioned to be an inter-working environment of heterogeneous networks of wired and wireless access networks, PSTN, satellites, broadcasting, etc., all interconnected through the service provider's IP backbone and the Internet. NGN uses multiple broadband, QoS-enabled transport technologies and service-related functions independent from underlying transport-related technologies. The operations and management of such interconnected networks are expected to be much more difficult and important than the traditional network environment. In this paper, we present an overview of the current status towards the management of NGN and discuss challenges in operating and managing NGN. We also present the operations and management requirements of NGN in accordance with the challenges. We then present standardization activities of NGN management and some of the notable research and development efforts related to NGN management.
key words: NGN, BcN, NGN management

1.   Introduction

NGN is envisioned to be an answer to network operators and service providers to replace existing telephone networks as well as to introduce a new converged service platform between fixed and mobile telecommunication businesses [1]. It is generally agreed that the main difference between traditional telecommunication networks and NGN is the shift from separate and vertically integrated application-specific networks to a single network capable of carrying any services. NGN is essentially about delivering new services that are available to any place, at any time, on any device, through any customer-chosen access mechanism. NGN is expected to co-exist and inter-work among wired networks (e.g., xDSL, Metro Ethernet, FTTH, leased lines, ISDN), wireless networks (e.g., 2G, 3G, WLAN, WiMAX/WiBro) as well as satellites and broadcasting networks, all interconnected through the service provider's IP backbone networks and the Internet. In this heterogeneous networking environment, in addition to the traditional challenges such as security, QoS, and charging, new challenges such as generalized mobility, and network discovery and selection exist. Providing effective, secure and efficient operations and management of the envisioned NGN environment is a huge challenge.

In order to provide the creation, deployment, and management of all kinds of services, NGN operations are highly dependant on flexible and efficient management systems and

processes [2]. When the networks are evolving towards NGN, the scenario to support various services would become more complex. The carrying of diverse traffic such as voice, data, video or signaling would be possibly integrated onto one common platform, which would call for the corresponding network management systems.

The ITU-T Recommendation Y.2401 [5] presents the management requirements, general principles and architectural requirements for managing NGN to support business processes to plan, provision, install, maintain, operate and administer NGN resources and services [4]. This paper presents a brief overview of NGN by giving its definition and functional architecture viewed by ITU-T. Broadband Convergence Network (BcN) is an NGN equivalent terminology that has been used in Korea over the past several years. We also present a brief overview and status of BcN activities in Korea. Compared to managing the traditional telecommunication networks, managing the NGN is much more difficult and complex. Thus, we examine the challenges facing the management of NGN. The standards and research activities of NGN management are also presented.

The remainder of this paper is organized as follows. Section 2 gives an overview of NGN based on the standardization activities of ITU-T. We also provide a brief overview of BcN in Korea. Section 3 presents the challenges in managing NGN. Section 4 presents the operations and management requirements of NGN as well as some of the notable research and development activities on NGN management. Finally, we end the paper with concluding remarks in Sect. 5.

2.   Overview of NGN

In this section, we present the definition of Next Generation Network (NGN) along with its architecture and principles [3]. We also examine the development and deployment effort of BcN in Korea.

2.1   Definition of NGN

NGN is a packet-based network to support the transfer of mixed traffic types such as voice, video, and data [1]. It is expected to integrate services offered by traditional networks and new innovative IP services into a single service platform. The key foundation of the NGN is the separation of services and transport networks, which provides QoS-enabled transport technologies and service-related functions
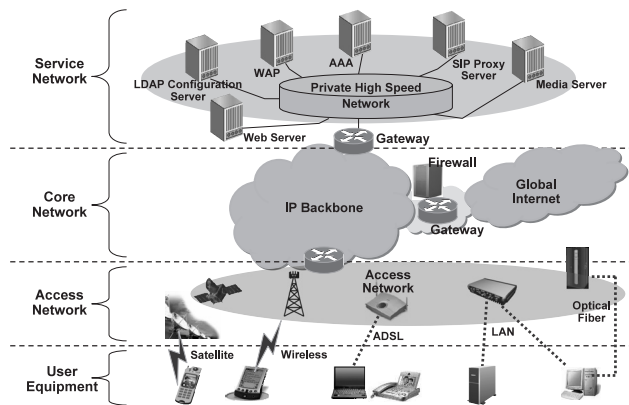
Fig. 1　NGN network components.

Fig. 2　NGN functional architecture.

independent from underlying transport technologies [36]. The transport functions provide transfer of information between peer entities; the services functions are concerned with the applications and services to be operated between peer entities [37].

Figure 1 shows typical NGN components: service network, core network, access network, and user equipment [37]. The service network is composed of various servers such as Web Server, Authentication, Authorization and Accounting (AAA), SIP Proxy Server and LDAP Server, etc. The service network is only responsible for providing services and applications for NGN users. The connection between the service network and the core network can be implemented via gateways. The core network in NGN represents the transportation backbone in traditional networks, which is concerned with the transfer of information between peer entities. Besides the transfer of packets, control and management functions are also implemented in the core network. The access network in NGN is derived from the existing access technologies. To accommodate various access media, the access network is separated from the core network of NGN, which serves as an intermediate between user equipments and core network.

2.2　NGN Functional Architecture

Figure 2 shows an overview of the NGN functional architecture [2]. The NGN architecture needs to offer the configuration flexibility to support multiple access technologies. It also needs to support a distributed and open control mechanism, which provides a separated service provisioning from transport network operation and speeds up the provision of diversified NGN services.

The NGN functions are divided into service and transport strata. The transport stratum functions provide connectivity for all components and physically separated functions within the NGN. The service stratum functions provide session-based and non-session-based services, including subscribe/notify for presence information and a messaging method for instant message exchange [36]. End-user functions are connected to the NGN by user-to-network inter-
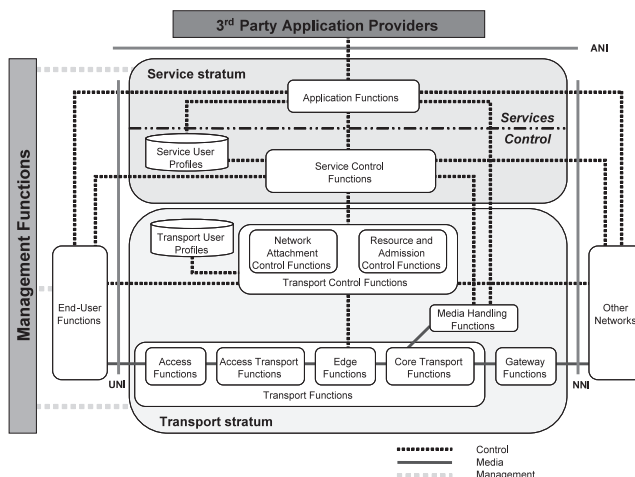
face (UNI), while other networks are interconnected through the network-to-network interface (NNI). The application-to-network interface (ANI) provides a channel for interactions and exchanges between applications and NGN elements. It also offers capabilities and resources needed for realization of applications and forms a boundary with respect to third-party application providers.

The management functions enable the NGN operator to manage the network and provide NGN services with the expected quality, security, and reliability. The management functions apply to the NGN service and transport strata, and cover fault, configuration, accounting, performance, and security management areas. The end-user functions include end-user interfaces, which provide end-user networks with capability to connect to the NGN access network. End-user equipment may be either mobile or fixed.

2.3　BcN in Korea

Korea has been leading the development of NGN-equivalent called Broadband Convergence Network (BcN) since the early 2000's. The only difference between NGN and BcN is that BcN also includes broadcasting (such as digital multimedia broadcasting, DMB). Namely, BcN is a QoS-guaranteed multimedia network that can provide integrated services of communication, broadcasting, and Internet that are ubiquitous, continuous, and secure. In BcN, various types of convergence take place such as convergence of wired and wireless networks, and convergence of telecommunications and broadcasting. For broadband end-to-end mobile networking, the broadband wired networks (such as IP/MPLS with DWDM optical networks) are interconnected with wireless networks (such as IEEE 802.11e Wireless LAN, 802.16 Wireless MAN (WiBro, WiMax) and 3G/4G wireless cellular networks).

The Korean Government finalized the 'plan for building the BcN' in February 2004 with the vision of providing the core infrastructure for broadband IT Korea by establishing the world's first BcN. The master plan for BcN construc-

tion is divided into three phases [20].

The first phase (2004–2005) is the BcN construction stage in promoting BcN establishment and facilitating its use. The objective of this phase is to build an IP-based voice and data integration network for wired and wireless networks, to provide IP-based wired and wireless interworking services. The plan in the first phrase consists of improving the performance of BcN network, and revising the strategies and roadmap of BcN to adapt to the market and technology changes. The purpose of the second phase (2006–2007) is to support the facilitation of application service models such as broadband convergence service, u-Learning, and u-Work, as well as to promote user-oriented services. The objective of the second phase is to integrate individual wired or wireless networks as the IP network, and integrate preliminarily with the broadcasting network. In the second phase, the BcN quality certification and management system are adopted together with the service level agreement (SLA) system. Strengthening the security and stability is focused during this phase. In the last completion phase (2008–2010), the objectives are to integrate the wired, wireless and broadcasting network as an IP-based network, to build an IP-based integration transport network, to complete infrastructure for quality-assured services, with the help of FTTH, 4G, etc., and to implement intelligent integrated terminals.

Currently, Korea is already regarded as the world's leading broadband nation, with 14.1 million broadband household subscribers in a population of 50 million. A full, commercial BcN deployment is scheduled for 2010, providing high quality services at a speed of 50–100 Mb/s to 20 million subscribers [21]. The telcos, ISPs and broadcasting companies have been deploying their own BcN and have been testing themselves. Recently, the interconnection and interoperability testing have been carried out between some telcos and ISPs.

3. Challenges for NGN Management

In the NGN environment, we envision and assume the co-existence of old and new networks and inter-working of heterogeneous networks provided through the cooperation of service providers around the world. This is a very ambitious goal and there are many challenges that must be overcome before this vision can be realized [22]. In this section, we examine these challenges.

3.1 Network Discovery and Selection

Since NGN consists of interconnected heterogeneous networks using heterogeneous user terminals, NGN should provide a seamless capability, independent of access method and network, and NGN also should address the identifying mechanisms [1]. That is, each terminal can use more than one type of network and possibly access multiple networks simultaneously for different applications (e.g., one for voice and another for receiving streaming media).

In such an environment, a terminal must be able to dis-

cover what networks are available for use. One of the proposed solutions for network discovery is to use software-defined radio devices that can scan the available networks. After scanning, they will load the required software and reconfigure themselves for the selected network. The software can be downloaded from the media such as a server, smart card, memory card or over the air.

3.2 Generalized Mobility

At present, mobility is used in a limited sense such as movement of user and terminal and with or without service continuity to similar public accessed networks (such as WLAN, GSM, UMTS, etc.) [6]. This means the horizontal handoff, which involves a terminal device to change cells within the same type of network to maintain service continuity. In the future, mobility will be offered in a broader sense where users may have the ability to use more access technologies, allowing movements between public wired access points and public wireless access points of various technologies. That is, in NGN environment, in addition to the horizontal handoff, the vertical handoff must also be supported. The vertical handoff mechanism allows a terminal device to change networks between different types of networks (e.g., between 3G and 4G networks) in a way that is completely transparent to end user applications. Thus, the challenge is to allow vertical handoffs between pairs of different types of networks in the presence of 2G, 3G, WLAN, WMAN, satellite, and 4G networks. The greater challenge lies when the vertical handoffs must take place with a certain set of QoS requirements still satisfied.

Roaming allows a customer to automatically make and receive voice calls, send and receive data, or access other services when traveling outside the geographical coverage area of the home network. Roaming is technically supported by mobility management, authentication and billing procedures. Establishing roaming between service providers is based on roaming agreements. If the visited network is in the same country as the home network, then it is known as national roaming. If the visited network is outside the home country, then it is known as global roaming. If the visited network operates on a different technical standard than the home network, then it is known as inter-standard roaming.

In NGN, all three types of roaming should be supported to roam through different network types, operating in different cities and countries. For true global roaming, roaming agreements must be set up among service providers among countries. Today, only a few service providers in different countries provide global roaming. The challenge is to provide more roaming agreements among the service providers in different countries. The greater challenge would be to provide inter-standard roaming in different countries.

3.3 Interoperability

Considering that NGN involves a large number of protocols including various profiles at the services and network level,

there is a need in the framework of NGN to insure the interoperability among systems and networks [2]. In order to meet the interoperability among systems, the only viable approach is to provide and support open interfaces. An open interface enables the functions of one component to be readily accessible by external organizations without knowing the technical details of how these functions are implemented. That is, internetworking between NGNs of different operators and between NGN and existing legacy networks should be provided via open interfaces.

3.4 QoS Support

Over the past decade, much research has been conducted in the area of QoS, and many protocols and methods have been proposed. However, the predominant method to support QoS by the Internet service providers (ISPs) today is over-provisioning. That is, instead of implementing complex QoS algorithms and methods, ISPs typically provide enough bandwidth in their backbone trunks so that their networks are hardly overloaded and thus there exists very little delay and few packets are lost in transit. This is quite feasible since a lot of fiber trunks have been installed over the past decade and the bandwidth cost of wired Internet trunks is very cheap. In the ISP's views, it is much simpler and cheaper to provide over-provisioned networks than implementing and managing complex QoS mechanisms.

Although NGN is supposed to provide higher bandwidth and more cost-effective channels than its predecessor networks, the bandwidth cost in NGN wireless networks will remain higher than wired networks. Thus, over-provisioning in NGN will not be feasible and QoS support mechanisms will definitely be needed. Providing QoS support in NGN will be a major challenge thus much work is needed.

3.5 Charging and Billing

Internet access is widely available from ISPs by using a number of access technologies including xDSL, cable modem, FTTH, satellite, and leased lines. The charging models for these traditional Internet access networks are already established and are in use around the world. These established charging models are now being applied with limited success to the new and evolving Internet access networks including WLAN and mobile telecommunication networks offering 2G and 3G services.

In the NGN environment, multiple service providers will typically be involved during a session (e.g., a phone call and data access), which may roam from one service provider network to one or more other service provider networks. Thus, in some cases, a single session may incur a number of charges, each of which may be for a different service provider. Moreover, different charging schemes may be used for different types of services (e.g., charging can be based on data, time, or content). One challenge is to keep track of charges per each segment of a session's use of

its network, service or content. More charging agreements between the service providers are needed in order to allow roaming during a session in order to obtain a continued service as far as a customer is concerned.

3.6 Security

Over the past few years, the Internet and enterprise networks have been plagued by denial of service attacks (DoS), worms and viruses, which have caused millions of computer systems to be shutdown or infected and the stored data to be lost, ultimately causing billions of dollars in loss. The introduction of wireless LANs (e.g., IEEE 802.11) into enterprises has made network security more vulnerable since rogue base stations (i.e., unauthorized private base stations) can be easily connected to existing wired networks, potentially becoming the source of security attacks inside firewalls and intrusion detection systems. Moreover, connecting malicious PC via a base station that is not well managed is also critical.

The first mobile phone virus, Cabir, has surfaced in June 2004 on Bluetooth-enabled Nokia mobile phones running the Symbian OS. The Lasco virus in 2005 based on Cabir was a Symbian worm that used mobile malware and attached itself to executables creating unnecessary files. The Com mWarrior virus in March 2005 was a Symbian virus spread by multimedia messaging services (MMS) and Bluetooth which destroyed content on the handset. The Fontal virus in 2005 was a Symbian virus and a Trojan that spread via MMS. Once infected, the handset would no longer boot. The recent LibPing virus exploited a graphics library remote buffer overflow to compromise the system [48]. Since the first virus came out, more worms and the strains of viruses in the mobile telecommunication networks are continually discovered. In the NGN environment, we will likely see more open platforms on terminal devices and servers providing various downloadable contents, some of which may carry worms and viruses. More interconnectivity and interworking will make the vulnerability even greater. Monitoring, detecting, analyzing and preventing worms and viruses on wired networks are very difficult tasks, but the same tasks on wired, wireless, and mobile networks combined would be even more difficult and challenging.

4. NGN Management

This section presents the requirements for managing NGN to operate and administer NGN resources and services. Further, it explains the standardization activities of NGN management and recent research and development activities for providing management capabilities of NGN.

4.1 Operations and Management Requirements of NGN

NGN management (NGNM) provides management functions for NGN resources and services, and offers communications between the management planes and the NGN

resources or services and other management planes [5]. FCAPS management areas are sufficient to cover most, if not all, of the issues related to the operations and management of the wired networks in NGN. With the introduction of wireless and mobile networks, a few additional areas, which could not be easily covered by FCAPS, had to be added. They are mobility management, customer management, and terminal management [22]. In this section, we propose the requirements of NGNM based on the ITU-T specification [5] and the challenges presented in Sect. 3.

4.1.1 Fault Management

The NGN environment will consist of numerous network devices such as base stations (BSs), access points (APs), gateways (GWs), routers, and servers to be monitored and controlled. Due to the increased number of devices to cover more geographic areas and users, along with the increased number of types of devices, scalable fault management solutions are desirable. Devices are likely to generate more event (including problem) reports as they will be involved in handoffs, roaming, charging, etc., and thus there will be a lot more event reports to be processed than in the traditional networks. Logging and auditing of events will be a challenging task but will need to be provided. Hence, traditional ways of conducting fault management will not likely scale well in the NGN environment. One possible solution is to apply the concept of 'autonomic computing' [23], where devices will be more self-managed. The research in this area has recently begun and the results can hopefully be applied to the NGN environment.

4.1.2 Configuration Management

Device configuration management is one of the most difficult management functional areas even in the wired networks. IETF has recently formed a working group called Netconf [24], whose goal is to provide a standard mechanism for transferring configuration data to and from a device, and for examining device state information which may impact the configuration. This standard method can be easily extended to the devices in the wireless and mobile networks, which is absolutely desirable as the terminal devices in the NGN environment will be multi-mode and multi-access capable. Devices can be automatically or manually configured to access a certain type of network and their capabilities and status can be automatically registered or notified to the configuration management system in the networks.

To provide seamless services in the converged network environment, a terminal device must be able to discover what networks are available for use and select which network to use. This must be also possible when a handoff is necessary. The device must also be able to select the one, if available, that satisfies the current session's QoS requirement. Thus, a network discovery and selection mechanism must be provided. Ideally, the selection is done intelligently

and automatically based on the most economical choice out of the available ones for the user. Since the handoffs must take place very quickly in order to provide continued service without the user's intervention or even the user knowing that a handoff is taking place, the discovery and selection mechanism must be conducted in real-time within the given time constraint.

When a customer subscribes for a network access service, appropriate network resources must be allocated so that the service can be provided. Similarly, when a customer subscribes for one or more application services, the subscription must be registered and appropriate resources must be allocated. These aspects are closely coupled with resource management and planning. It is currently an intense area for research even in the wired networks. Intelligent resource management and service brokering is even more important in the wireless and mobile networks as the resources are typically more scarce and expensive. Some research of configuration management has started for wireless and mobile networks [25] but much more research is needed in this area.

4.1.3 Accounting Management

Accounting management largely entails Authentication, Authorization and Accounting (AAA), Charging, and Billing. Accounting management in the NGN environment is also very important and robust, thus precise and inter-working accounting systems are required.

Users wishing to use one or more services provided by the service providers must be authenticated (i.e., validate who the user is) and authorized (i.e., validate whether the user is allowed to use the service or not). Then, the user can enjoy the service and be charged accordingly. One of the most difficult challenges in the NGN is in providing authentication and authorization service in real-time so that when roaming is required, the user can be authenticated and authorized to change the network on the fly. It becomes even more challenging when the roaming combined with vertical handoff and QoS requirement satisfaction checking is required on the fly. IETF AAA Working Group has standardized AAA based on RADIUS and is currently working on AAA based on DIAMETER [26]. It will be interesting to see whether DIAMETER will be sufficient for AAA in the NGN environment or not.

A single user session may involve one or more service providers' networks in the NGN. Also, within the same service provider, a session may involve multiple types of networks which may have different charging schemes. Billing needs to consider various ratings due to service bundling (e.g., mobile phone, Internet access, satellite TV, etc.) A session manager would keep track of the user's activities during a session. A charging system needs to exist in each service provider's network that keeps track of the individual customer's usage. Service providers in turn would periodically settle charges with other service providers based on the settlement agreements' setup between the service providers. A

billing system keeps track of customers' charges and generates monthly bills. It also keeps track of overdue payments, credits, etc.

4.1.4 Performance Management

Performance management is another essential management area for the NGN environment. This is especially true as most of the service providers today consider performance assurance as a key part of SLA that they make with the customers when they subscribe. At a lower level, network performance monitoring is required while at an upper level, service quality management is required.

For network performance monitoring, an active monitoring method is typically used, where packets are sent in to the network to obtain performance metrics such as delay, jitter, packet loss, and throughput [27]. These performance figures are either provided to the customers as requested (or via a network weather website), or used for service quality management to verify that their networks are performing according to the agreements they made with the customers via SLAs.

SLA is a formal negotiated agreement between a service provider and a customer. The service quality management is the integrated management of all functionalities in the SLA life cycle. When a customer orders a service from a service provider, an SLA is negotiated and then a contract is made. In the SLA contract, QoS parameters that specify the service quality that the service provider will guarantee are included. The service provider must perform SLA monitoring to verify whether the offered service meets the QoS parameters specified in the SLA or not. In order for the service quality management system to verify whether the specified QoS parameters are being met or not, the system must gather performance data from the underlying network performance monitoring system and map such data to the QoS parameters [28]–[30].

4.1.5 Security Management

In addition to the AAA requirement described above, information security and network security are two important aspects of security in the NGN environment. Both aspects are important to the integrity of the communication or data being transferred and for the health of the network resources including the networks and servers providing the services.

Cryptography can be used to encrypt and decrypt packet data while in transit to provide secure communication. A lot of research has been done in this area with results such as AES [31]. A disadvantage of using cryptography is the degradation in the performance. Secure communication may not always be necessary. Thus, service providers must determine where cryptic communication would be necessary and may apply only when and where needed.

Firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) will be needed in key places in the network to protect resources from potential

hackers and worms. Anti-virus software must also be installed in key servers in order to detect and cure viruses. It is always a good idea to constantly keep them up to date and replace to new systems when patching and updating will no longer be effective. Again, these protective measures may degrade the performance of networks and servers but it is well advised to invest and deploy those measures wherever necessary.

4.1.6 Mobility Management

Mobility management in the NGN entails horizontal and vertical handoffs, and roaming [32]. As explained in Sect. 3.2, both horizontal and vertical handoff functionalities must be provided in the NGN and a mobility management system is required to support them. A key challenge will be when changing a network for a session with certain QoS requirements. If the QoS requirement can be satisfied in the new network, then there will be no problem. The problem arises if the new network cannot satisfy the QoS requirement. Should we terminate the session or continue it with lower quality? Although the latter will likely be chosen by most users, such decision can be preset by the user in his or her personal profile.

Mobility agreements must exist in advance between the service providers in order to provide service continuity. The goal of mobility is to have a customer receive the same service (or as close to the same service) when traveling in an area supported by another network as the customer receives when in their home service provider's area. Authentication of the user in the home network and registration in the session manager must be done on a fly. Otherwise, the transition from one network to another will not be smooth and may lose a connection or experience a short outage in communication.

4.1.7 Customer Management

Customers have become very important in recent years as the telecom world has become very competitive with more service providers in business than ever before. A customer is a 'king' these days in most of the developed countries in the world. Two subareas of customer management are required as a part of customer management, namely subscription management and profile management.

Subscription management is a feature that permits service providers to provision services for a specific subscriber [33]. This feature is necessary to allow service providers to provision, control, and monitor and bill the configuration of services that they offer to their subscribers. It focuses on the operations and management processes to manage subscription information, which is concerned with provisioning the subscription profile throughout all the systems and trading partners needed to realize the customer service. The NGN subscription management is no longer simply an internal matter for a single operator but a capability that is achieved by linking features together across multiple service

providers' operation support systems.

A customer profile is customized preference information that allows a personalized service by the service providers. The NGN environment needs to focus more on customer profile management as a customer may access with different terminals depending on where they are and what they are doing. The goal of profile management is to provide a ubiquitous, single look-and-feel access environment even in the presence of customers' multiple, heterogeneous terminals (e.g., mobile phone, PDA, laptop) and different operator networks. Customers must be able to change their profile from their terminal or from the Web for setting profiles for multiple terminal types. The customized or updated profile information must be propagated to all the systems in the network that maintain the information.

4.1.8 Terminal Management

Terminal management entails two subareas, namely terminal location management and terminal trace management [34]. The terminal location information can be used to make the QoS related decisions by the operations and management system when a user wishes to use a particular service, and a certain set of QoS has been requested. It can also be used when a handoff is needed, and to provide a value-added service such as for locating a missing or an overdue child as well as locating a 'mis-behaving' spouse.

Terminal trace management is important for detecting and tracing stolen terminals or frauds, which are currently one of the biggest headaches experienced by the service providers today. There are many missing or stolen terminals in the world. When these terminals are illegally used by someone other than the owner, the terminal trace management feature can be used to trace the terminal. Terminals may not be stolen but the terminal IDs may have been copied and embedded into another terminal illegally. This feature can be used to trace such illegal use as well. Traces information can also play a key role in activities such as determining the root cause of a malfunctioning terminal, advanced trouble shooting, optimization of resource usage and quality, RF coverage control and capacity improvement, and dropped call analysis.

4.2 Standard Activities on NGN Management

ITU-T has been operating a special expert group called FGNGN to provide the architecture of NGN, and is currently working on the network operations and management issues actively in Study Groups (SG) 13 and SG 11. The NGN Management Focus Group (NGNMFG) [7] is acting as a coordinator and as an information broker on work directions, plans and progress in the various standard bodies. The NGN Management Specification Roadmap [7] is an output of the NGNMFG and identifies various existing, or work-in-progress specifications relevant to NGN management. It also identifies the gaps which have to be filled and the candidate bodies to undertake this work.

European Telecommunications Standards Institute (ETSI) [8] focuses on defining the NGN OSS architecture structured in three views (business, functional/information and implementation), and in particular on the management of IP-based services in the NGN network environment [9]. ETIS also defines the NGN OSS requirements, structures the requirements into a hierarchy (level 0, 1 or 2 requirements) and categorizes them on how they fulfill the NGN management [10], [11].

The TeleManagement Forum (TMF) NGN Management (NGN-M) team was formed in early 2005 to provide strategic planning and recommendations to the TMF in order to lead the industry activities in NGN management [18]. The NGN-M team identifies how NGOSS frameworks such as enhanced Telecom Operations Map (eTOM) [14], shared information data (SID) [15], technology-neutral architecture (TNA) [16] may be applied to support NGN management, but also identifies any necessary modifications and/or additions that will be required. In particular, the integrated nature of the various NGOSS frameworks could provide a significant amount of infrastructure required for NGN management. The eTOM is used as a common business process framework of NGN, and the SID can be the concept of factoring out and sharing information across a number of management areas. Usage of the component-based systems architecture for realization of OSS/BSS solutions with many other related concepts of contract interface definition, namely TNA, can be applied to distributed systems' design principles of NGN management. Multi-technology network management (MTNM) [17] is used as a common approach and service interface applied to the management of multiple core and access network technologies. Multi-technology operations systems interface (MTOSI) [19] can be applicable to agreed service abstractions and interface between peer OSS/BSS components.

There are four harmonization efforts amongst standardization organizations of NGN management specification [7]. The first one is to define the NGNM architecture. ETSI 188 001 document [10] describes the NGN management architecture, which is based on Service Oriented Architecture (SOA) principles. The document provides a mapping of the NGN OSS functional/information view, which is based on TMF's eTOM, to service interface groups. The architecture specified by ITU-T recommendation Y.2401 [5] is based on a number of concepts from the Telecommunication Management Network (TMN) Logical Layered Architecture. It also refers to SOA principles.

The second one is on the management information. There are two generic information models included in the NGN Roadmap, the TMF SID and Distributed Management Task Force (DMTF) Common Information Model (CIM). Traditionally, the CIM and SID models have focused on different operational domains. Currently, CIM's primary focus is on the IT resource management (Systems, Storage) and IP Networks, and SID provides a description of the telecom service provider's total technical and business systems. However, both models have many similarities and overlap in

the domain they cover and are currently used by the number of different management solutions. Harmonization between CIM and SID needs to occur within operational domains where these models need to coexist in order to provide interoperability between different management solutions used for NGN. The CIM-SID harmonization activity is a joint effort between the DMTF and the TMF. The final objective, however, is to develop an approach applicable to other domains as well.

The third harmonization effort is related to defining management functionalities such as accounting and charging, alarm management, and QoS management. The 3rd Generation Partnership Project (3GPP) [13] and Alliance for Telecommunications Industry Solutions (ATIS) [12] have reached an initial agreement regarding the harmonization of their specifications for charging, billing and accounting management and have indicated their willingness to work with the ITU-T NGNMFG. TMF MTNM, 3GPP and ITU-T SG4 support alarm management, which involves at a minimum alarm reporting with multiple severity levels. ITU-T SG, 3GPP, ATIS and ETSI define dynamic QoS controls, performance measurement and monitoring, and performance assessment to provide end-to-end QoS services.

The last harmonization effort is the work for specifying management interfaces. Implementable interfaces are defined in most management standards' organizations by a similar methodology resulting in the following set of specification types: interface requirements, a protocol-neutral information model formatted using UML notation, and one or more protocol-specific data models. ITU-T SG4 and 3GPP try to define common management interfaces [7]. Currently, the harmonization efforts are in process, while standardization in the area of NGN management is still fragmented at many different standards' bodies.

4.3   Research Activities on NGN Management

In the past several years, some research and developments have been conducted in the area of NGN management. One work has been completed in the area of defining the NGN management requirements. Some other work has focused on NGN network and service management. The management functionalities of NGN (e.g., mobility management, QoS management, security management), have also been performed.

4.3.1   NGN Management Requirements

M. Li and K. Sandrasegaran [37] introduced the current network management approaches and described some deficiencies of current solutions. Current network management solutions have followed two general technical directions: ITU-T's TMN for telecommunication networks and IETF's Simple Network Management Protocol (SNMP) [39] for IP networks. SNMP approach is simple and cost-effective compared to TMN approach, but the complexity and completeness of TMN are most suitable for some critical applica-

tions such as the management of transportation backbones. Moreover, they presented and discussed the network management challenges in NGN, and explained why it is difficult to solve them by traditional network management methods. The challenges were dynamic topology configuration, interoperability among heterogeneous networks, and QoS-guaranteed services, etc. They also illustrated some emerging approaches towards network management in NGN. One was Web services management which applies Web services technologies such as XML, SOAP, and WSDL to NGN management in order to improve system interconnections through ubiquitous availability of HTTP and the simplicity of SOAP messages. The other was policy-based management which defines policies, and distributes and enforces them to network devices.

4.3.2   NGN Network and Services Management

I.G. Yahia., et al. [41] described the service management aspects and their challenges during the evolution towards next generation services (NGS). They set up a common service architecture for NGS and its management. NGS are basically an advanced telecommunication services. Service management is an iteration of management functions that handle the service from its creation to its delivery to the customer and its maintenance. Management functions include service design/assign, service configuration, service provisioning, service performance, service quality monitoring and impact analysis, service problem resolution, service assurance management, and service introduction. The challenges for NGN service management are the complex and heterogeneous management operations, insufficient information model for service management, and no standard management interfaces for various services. In 2006, I.G. Yahia., et al. also proposed autonomic management for NGS to avoid complexity of existing service management systems [46].

Managing services on the NGN is becoming more and more complex and time consuming for service providers since services are increasing both in number and complexity and the number of users per service is going up. A solution to this problem is to allow the service users themselves to partly manage the services they are using. This is called Customer Service Management (CSM). X. Jiang, et al. [42] presented an architecture for CSM in NGN. The SLA and SLS play a key role in CSM as they can determine in detail the possible user service management actions. The CSM will both increase the perceived value of the services to the users and lower the operational costs of service management for the service provider.

4.3.3   NGN Management Functionalities

In NGN, identity management is a critical factor in providing seamless ubiquitous support to various services in a larger service provider environment. It involves consolidation, management and exchange of identity information

of users to ensure that the users have a fast, reliable and secure access to distributed network resources across multiple service providers. Identity management is applied to support mobility management and accounting management. S. Subenthiran, et al. [43] analyzed the requirements for identity management in an NGN to meet the needs of end users, network operators, network roaming, application service providers, regulatory and legal bodies in terms of some of NGNs key functions such as operation, security, personalization, charging, etc.

To provide mobility capability, J.M. Kang, et al. [40] proposed an Autonomic Handover Manager (AHM). It is based on the autonomic computing concept to decide on the best network interface to handover in 4G networks. The manager chooses the appropriate policy for the specific service or application without the user's intervention using the context information from the mobile terminal, the network, and the user. They presented the context information and the context evaluation function to decide on the handover based on the user preferences. They then described the scenario to validate its feasibility by using multimedia conferencing service on the mobile terminal.

W. Jia, et al. [45] discussed some important design issues for the NGN architecture and different layers for end-to-end QoS control. They illustrated five functional layers of NGN architecture to support end-to-end QoS services. The five functional layers are: (1) Application Layer that supports SIP protocol; (2) Network Control Layer that aims at overcoming the bottleneck problems at edge nodes or servers for end-to-end admission control; (3) Adaptation Layer that supports different network configurations and network mobility; (4) Network Transmission Layer that provides end-to-end QoS control for real-time communications through integrating Differentiated Service (DiffServ) and Multi-Protocol Label Switching (MPLS) and (5) Management Layer that provides Web-based GUI browser for data presentation, monitoring, modification and decision making in NGN.

O. Alanen, et al. [38] studied and presented the performance requirements for a future real time 3/4G management system. They also implemented a 3/4G network visualization and control system, and the name of the visualization tool is VizTool [47]. The VizTool tool provides a hierarchical, color-coded presentation of the network with performance and alarm information. They included a preliminary study and full functional visualization tool demonstration results to show what the future tools and methods would look like in reality. In the near future, the development of the visualization tool and the control model will continue, keeping the goal into developing a full scale real time control and management model and solution for 4G networks.

The growing threats and risks by changes in the overall regulatory and technological environments have highlighted the need for additional security requirements. Alcatel identified that security in NGN needs to be addressed as an important management issue [44]. An important challenge for NGN IP systems is the way in which security is realized in many different kinds of applications. From the beginning, the NGN architecture was developed considering security issues, based on a threat analysis and the use of cost-effective countermeasures, thanks to IPsec from IETF. Flexibility ensures that security can be customized to meet the needs of real environments. Alcatel first defined threat analysis in NGN such as denial of service, eavesdropping, masquerade, unauthorized, modification of information, and repudiation. Then, Alcatel provided security requirements and countermeasures. Still, more work is needed in order to safeguard the network against future attacks from unknown sources.

4.3.4 BcN NMS

As the BcN emerges, efficient NMS needs to be designed and implemented to manage various network equipments and services. That is, for efficient service provisioning on the BcN, well-designed and implemented network operations and management functions are essential. KT has developed an BcN NMS using several technologies such as OSS through Java (OSS/J), TMF SID, and Web services [49].

Current OSS technology cannot cope with the rapidly increasing scale of BcN network with the diversity of communications technology, availability, and reliability. Therefore, service providers need proper OSS solutions and a new approach to provide OSS solutions. The OSS/J APIs support a full OSS solution that provides service fulfillment, assurance, and billing. KT used QoS API and common API of OSS/J, as well as XML as defining management interfaces and SOAP as a management protocol in order to take advantage of the compatibility reduced development period, easy maintenance, and low development costs of BcN NMS applications. In addition, KT defined the management information model of BcN NMS by using the TMF SID model.

Over the past two years, KT has been operating the BcN-NMS for their BcN network without much problem. One thing that they have noticed is that the response time of BcN-NMS operations takes longer than their other NMS systems. They suspect that this is due to the use of Java (in OSS/J) for the implementation.

Current research activities of NGN operations and management are performed only in defining the requirements of NGN management and in the area of resource and service management, mobility management, performance management and security management. These research activities are mostly in early stages. Also, the KT's implementation of BcN-NMS is not much different than the existing network management system from the perspective of management functions and operations. Thus, it is difficult to find new aspects of NGN management based on KT's implementation experience. More efforts are required to devise an NGN management system to meet the challenges and requirements of NGN management.

5. Concluding Remarks

This paper presented an overview of NGN and the status towards the management of NGN. Standardization and research activities on NGN and NGN management have been taking place quite actively in the past several years but much more work is needed before NGN can be fully realized and OSSs for NGN can be deployed and used.

We will undoubtedly see more work on developing and using operations and management systems for NGN in the near future. Much of these systems will likely employ one or more of the latest approaches such as autonomic management where self-configuring, self-optimizing, and self-managing will be critical in overcoming complex NGN network environments.

Acknowledgments

References

[1] ITU-T, "General overview of NGN," Recommendation Y.2001, Dec. 2004.

[2] ITU-T, "General principles and general reference model for next generation networks," Recommendation Y.2011, Oct. 2004.

[3] ITU-T, "Functional requirements and architecture of the NGN," Recommendation Y.2012, Sept. 2006.

[4] ITU-T, "Resource and admission control functions in next generation networks," Recommendation Y.2111, Sept. 2006.

[5] ITU-T, "Principles for the management of the next generation networks," Recommendation Y.2401, March 2006.

[6] ITU-T, "Mobility management requirements for NGN," Recommendation Y.2801, Nov. 2006.

[7] ITU-T NGN Management Focus Group, "NGN management specification roadmap v3.1," Jan. 2007.

[8] European Telecommunications Standards Institute (ETSI), http://www.etsi.org

[9] ETSI, "NGN management: OSS architecture," ETSI TS 188 001, March 2006.

[10] ETSI, "NGN management: OSS requirements," ETSI TS 188 003, March 2006.

[11] ETSI, "NGN management: OSS vision," ETSI TS 188 004, March 2006.

[12] Alliance for Telecommunications Industry Solutions (ATIS), http://www.atis.org

[13] 3rd Generation Partnership Project (3GPP), http://www.3gpp.org

[14] TMF, "enhanced Telecom Operations Map^{TM}(eTOM) version 3.0," GB 921, Release 6.0, Nov. 2005.

[15] TMF, "Shared information/data (SID) model," GB 922, Release 6.0, Nov. 2005.

[16] TMF, "NGOSS technology neutral architecture (TNA)," - TMF053 Version 5.3, Release 6.0, Nov. 2005.

[17] TMF, "MTNM solution suit v3.0," TMF 814 Version 3.0, April 2004.

[18] TMF, "NGN management strategy: Policy paper," TR133-Req Version 1.2, Release 1.0, June 2006.

[19] TMF, "Multi-technology operations systems interface (MTOSI)—XML solution set," TMF 854, Version 1.1, Dec. 2005.

[20] ETRI, "Broadband convergence network (BcN) for ubiquitous Korea vision," 7th International Conference on Advanced Communication Technology (ICACT 2005), pp.168–181, Feb. 2005.

[21] D.J. Chin and M.W. Rim, "IT839 STRATEGY: The Korean challenges toward a ubiquitous world," IEEE Commun. Mag., vol., pp.32–38, April 2006.

[22] J.W. Hong and A. Leon-Garcia, "Requirements for the operations and management for 4G networks," Proc. 19th International Telegraffic Congress (ITC 19), pp.981–990, Beijing, China, Aug. 2005.

[23] IBM, Autonomic Computing, http://www.research.ibm.com/autonomic

[24] IETF, Network Configuration (netconf), http://www.ietf.org/html.charters/netconf-charter.html

[25] S. Karlich, T. Zahariadis, N. Zervos, N. Nikolaou, B. Jennings, V. Kollias, and T. Magedanz, "A self-adaptive service provisioning framework for 3G+/4G mobile applications," IEEE Wireless Commun., vol.11, no.5, pp.48–56, Oct. 2004.

[26] IETF, Authentication, Authorization and Accounting (aaa), http://www.ietf.org/html.charters/aaa-charter.html

[27] J.W.-K. Hong, "Internet traffic monitoring and analysis: Methods and applications," Tutorial, Globecom 2004, Dallas, TX, Dec. 2004.

[28] H.-J. Lee, M.-S. Kim, J.W. Hong, and G.-H. Lee, "Mapping between QoS parameters and network performance metrics for SLA monitoring," Proc. 2002 Asia-Pacific Network Operations and Management Symposium (APNOMS 2002), pp.97–108, Jeju, Korea, Sept. 2002.

[29] H. Jiang and W. Zhuang, "Quality-of-service provisioning in future 4G CDMA cellular networks," IEEE Wireless Commun., vol.11, no.2, pp.48–54, April 2004.

[30] X. Gao, G. Wu, and T. Miki, "End-to-end QoS provisioning in mobile heterogeneous networks," IEEE Wireless Commun., vol.11, no.3, pp.24–34, June 2004.

[31] NIST, Advanced Encryption Standard, http://csrc.nist.gov/CryptoToolkit/aes/

[32] I.F. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," IEEE Wireless Commun., vol.11, no.4, pp.16–28, Aug. 2004.

[33] 3GPP, "Telecommunication management: Subscription Management (SuM) Architecture," 3GPP TS 32.141, V6.1.0, March 2004.

[34] F. Ayazi and M. Mirzabaghi, "NGN management requirements in a multi vendor pilot platform," 2nd Information and Communication Technologies (ICTTA'06), pp.3613–3615, April 2006.

[35] C.S. Lee and D. Knight, "Realization of next generation network," IEEE Commun. Mag., vol.43, no.10, pp.34–41, Oct. 2005.

[36] K. Knight, T. Towle, and N. Morita, "NGN architecture: Generic principle, functional architecture, and its realization," IEEE Commun. Mag., vol.43, no.10, pp.49–56, Oct. 2005.

[37] M. Li and K. Sandrasegaran, "Network management challenges for next generation networks," IEEE Conference on Local Computer Networks, pp.593–598, Nov. 2005.

[38] O. Alanen, T. Hamalainen, and E. Wallenius, "Network and system performance management for next generation networks," Proc. 20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06), pp.689–692, 2006.

[39] W. Stallings, SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards, Addison-Wesley, Reading, MA, 1993.

[40] J.-M. Kang, H.-T. Ju, and J.W.-K. Hong, "Towards autonomic handover decision management in 4G networks," 9th IFIP/IEEE International Conference on Management of Multimedia and Mobile Networks and Services (MMNS 2006), LNCS 4267, pp.145–157, Dublin, Ireland, Oct. 2006.

[41] I.G. Yahia and E. Bertin, "Next/new generation networks services and management," International Conference on Networking and Services (ICNS'06), pp.15–19, July 2006.

[42] X. Jiang, F. Yang, and H. Zou, "A novel architecture to customer

service management for the NGN," International Conference on Communication Technology Proceedings (ICCT 2003), pp.123–126, April 2003.

[43] S. Subenthiran, K. Sandrasegaran, and R. Shalak, "Requirements for identity management in next generation networks," 6th International Conference on Advanced Communication Technology, pp.138–142, 2004.

[44] B. Gamm, B. Howard, and O. Paridaens, "Security features required in an NGN," Alcatel Telecommunications Review, 2001.

[45] W. Jia, B. Han, J. Shen, and H. Fu, "Next generation networks architecture and layered end-to-end QoS control," ISPA 2005, LNCS 3758, pp.1055–1064, 2005.

[46] Imen Grida Ben Yahia and E. Bertin, "Towards autonomic management for next generation services," International Conference on Networking and Services (ICNS'06), pp.38–41, July 2006.

[47] E. Wallenius, H. Helanter, T. Hamalainen, O. Alanen, and O. Karppinen, "Performance management in 3/4G mobile networks," IEEE 62nd Vehicular Technology Conference, pp.2144–2148, Sept. 2005.

[48] D. Krishnaswamy, R.N. Hasbun, and J.P. Brizek, "Secure manageable mobile handset platform architectures," IEEE Commun. Mag., vol.44, no.9, pp.158–165, Sept. 2006.

[49] S.H. Park, S.H. Suk, and J.H. Yoo, "Design and implementation of BcN-NMS," 2005 Asia-Pacific Network Management Operations, pp.493–504, Sept. 2005.

James Won-Ki Hong is a professor in the Dept. of Computer Science and Engineering, POSTECH, Pohang, Korea. He received a Ph.D. degree from the University of Waterloo, Canada in 1991 and an M.S. degree from the University of Western Ontario in 1985. His research interests include network and systems management, distributed computing, and network monitoring and analysis, and network planning. James has served as Technical Chair (1998–2000), Vice Chair (2003–2005) and Chair (2005–present) for IEEE Comsoc Committee on Network Operations and Management (CNOM). He has also served as Director of Online Content for the IEEE Comsoc (Jan. 2004–Dec. 2005). He is a NOMS/IM Steering Committee Member and a Steering Committee Member of APNOMS. He was technical co-chair of NOMS 2000 and APNOMS'99. He was Finance Chair for NOMS 2006, IM 2005 and Finance Chair and Chair of Local Planning Committee for NOMS 2004. He was the General Chair for APNOMS 2006. He is an editorial advisory board member of JNSM, IJNM, JTM and TNSM. He is also editor-in-chief of KNOM Review Journal. He is a member of IEEE, KICS, KNOM, and KISS.

Mi-Jung Choi received her B.S. degree in computer science from Ewha Womans University in 1998, M.S. and Ph.D. degrees in the Dept. of Computer Science and Engineering (CSE) from Pohang University of Science and Technology (POSTECH) in 2000, 2004 respectively. She was a Post-doc fellow at INRIA, France from Oct. 2004 to Sept. 2005 and at School of Computer Science, University of Waterloo, Canada from Nov. 2005 to Oct. 2006. Currently, she works in POSTECH, Korea as a research professor from Nov. 2006. Her research interests include XML-based network management and NGN management. She is a member of IEEE and KNOM.