A First Glance Comparison of Next and New Generation Network Approaches

Antonio Marcos Alberti, Tania Regina Tronco and Christian Esteve Rothenberg

Abstract— Next Generation Networks (NxGN), as pursued by international standards development organizations, represent the telecommunication operator approach to provide convergent multimedia experience for their users with improved support for mobility and unfettered service access. In contrast, research efforts in so-called New Generation Networks (NwGN), such as the Japanese project Akari and the European Future Internet initiatives, are part of an exciting trend towards re-architecting the Internet. Despite the enormous interest regarding both lines of work, few comparisons between their design approaches have been discussed in the literature. This paper provides a first glance comparison between key aspects of both proposals.

Index Terms— NGN, NwGN, Future Internet, IP networks

I. INTRODUCTION

The Next Generation Network (NGN, NxGN) is an IP - based carrier-grade telecommunications network providing QoS-enabled services via diverse types of broadband access technologies. Altogether, the NGN establishes an architectural framework in which service-related functions are independent from transport technologies, as shown in Fig. 1. Since 2001, the NGN has been studied and standardized by several international organizations such as ITU-T (International Telecommunication Union - Telecommunication Standardization Sector), 3GPP (3rd Generation Partnership), ETSI (European Telecommunications Standards Institute) and, to a less extend, the IETF (Internet Engineering Task Force). A key challenge has been releasing an overarching set of standards that enables new business opportunities while guaranteeing global interoperability. At the heart of the NGN, sits 3GPP´s original IMS (IP Multimedia Subsystem) [3], which was embraced by ETSI and ITU-T as the common control architecture.

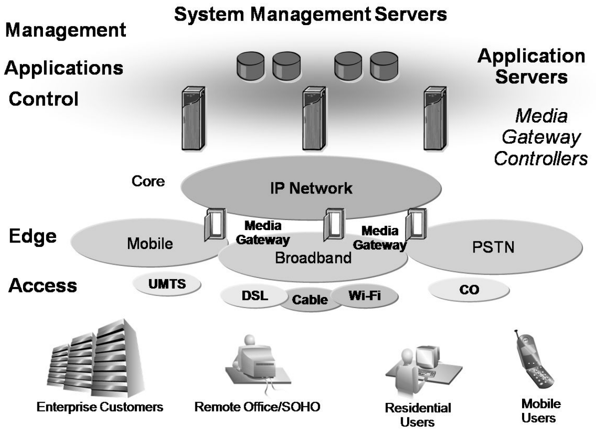

Fig.1. NGN structure.

On another research track, we can refer to New Generation Networks (NwGN)[1] as a generalization of the series of new Internet architecture proposals being pursued by research projects aiming at re-thinking the TCP/IP suite and re-engineering the Internet to address current and future requirements. There is an increasing level of concern and discussion in the networking research community as how long it will be possible to do incremental changes based on extending (i.e., patching) today´s IP-based networks and how to create a global-scale ubiquitous network foundation to solve societal and economic challenges in the future.

Being an evolutionary approach and having its original principles eroded (cf. end-to-end argument), current IP networks suffer with lack of mobility, loss of transparency, scalability issues, protocol incompatibility, security issues, and all in all, protocols taking roles for which they were not originally designed.

Future Internet research projects are popping up everywhere resulting in new architecture designs and protocols. In Europe, research activities are mainly carried under the multi-year continent-wide Framework Programme (FP), which covers a wide range of subjects, from ICT to energy, nanotechnology, health, and so on. The current programme is the seventh (FP7), started in January 2007 and will expire in 2013. In Japan, the Akari project [5] – sponsored by the National Institute of Information and Communications Technology (NICT) – has a working group for the development of a new network architecture following a clean-slate approach in what they call a NeW Generation Network (NWGN) by 2015 [1]. In the US, the National Science Foundation (NSF) has been actively funding projects within the Future Internet Design (FIND) framework, where

Manuscript received May, 15, 2010. This work was supported in part by FUNTTEL (Funding for Technological Development of the Telecommunications) - Ministry of Communications, Brazil.

Antonio Marcos Alberti is with the Instituto Nacional de Telecomunicações (INATEL), Av. João de Camargo 510, Santa Rita do Sapucaí, Minas Gerais, Brazil, CEP 37540-000 alberti@inatel.br.

Tania Regina Tronco is with the CPqD Foundation, Brazil, tania@cpqd.com.br

Christian Esteve Rothenberg is with CPqD and the University of Campinas (UNICAMP), Brazil, chesteve@dca.fee.unicamp.br.

---

[1] To our best knowledgement, the acronyms NwGN and NxGN were firstly addressed by Tomonori Aoyama [1].

clean-slate thinking has been a major topic.

The main contribution of this paper is to give a first glance analysis over a potential NxGN and NwGN coexistence. To achieve this goal, we present key architectural and functional aspects of the NxGN in Section II, and those of the NwGN in Section III. In Section IV, we compare the adopted designs in NxGN and NwGN. Finally, in Section V, we outline our conclusions.

II. NEXT GENERATION NETWORKS

The main characteristic of the NGN is the separation of services and transport functions in two strata. This separation allows services being developed and offered by different players. Transport functions are based on IP packet switching as well as other technologies capable to transport IP datagrams. SIP (Session Initiation Protocol) proxies are used to control sessions at the service stratum.

Moreover, the service layer division in: control plane, management plane, and user plane enables the creation and execution of services independently from the transport delivery functions. Services can be created synergistically composed by reusing service stratum common functional entities. Service invocation depends on SIP signaling to route, negotiate capabilities, and establish communication to multimedia application servers.

Similarly, the transport layer division in: control plane, management plane, and user plane enables to establish end-to-end connections with security and QoS guarantees, following a tight control over the network resources. In addition, open interfaces between the transport layer and access layer, enable various access network technologies (e.g., xDSL) being combined with the core transport technologies (e.g., MPLS).

A. *NGN- ITU-T Standard*

NGN-ITU-T standardization work is developed under the NGN GSI (Global Standardization Initiative). Figure 2 illustrates the NGN-GSI architecture standardized in Recommendation Y.2012, “Functional Requirements and architecture of the NGN” [2]. The UNI (User-Network Interface), NNI (Network-Network Interface) and ANI (Application to Network Interface) are the main points of reference of the NGN, which can be mapped to physical interfaces depending on the technologies used in the implementation.

The “Transport Functions” provide connectivity to all components in NGN, i.e., provide the media transference as well as control and management information, controlled directly by the “Transport Control Functions” based on information from the “Transport User Profiles.” “Transport Functions” provide support not only for QoS control and traffic management, but also for security and NAPT (Network Address and Port Translation) functions. Various mechanisms are supported, such as policing, admission control, firewall control, packet filtering, network selection, MGs (Media Gateways), SGs (Signaling Gateways), etc.

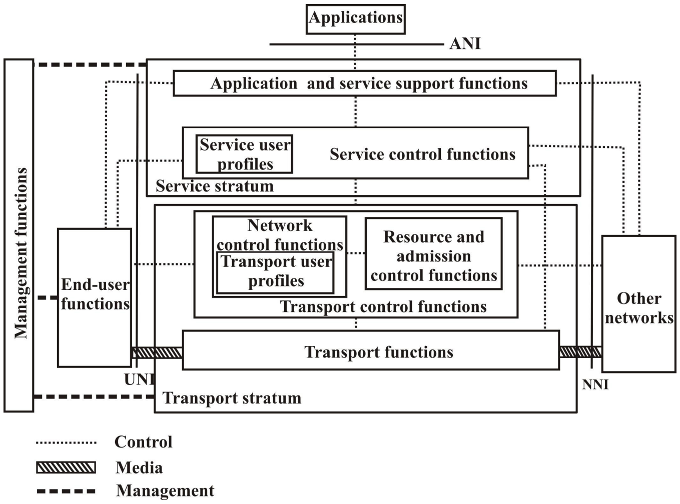

Fig. 2. NGN – ITU-T Standard. Source: [2]

The “Transport Control Functions” are divided in two blocks: RACF (Resource and Admission Control Function) and NACF (Network Attachment Control Function), as shown in Figure 2. The RACF interacts with the “Transport Functions” to control QoS, traffic and security at network elements, such as routers, switches, gateways, firewalls, etc. Admission control involves verifying authorization based on user profiles, SLA (Service Level Agreement), operator rules, service priority and resource availability in core and access segments. The RACF acts as an arbitrator in the negotiation and allocation of resources between the “Service Control Functions” and the “Transport Functions.” RACF interacts with SIP proxies at the service stratum to provide adequate transportation of traffic flows established by SIP sessions, and it interacts with NACF to access transport-related user profiles.

The NACF provides network access initialization and boot functions for end user equipment, providing identification and authentication at the network level, and management of the IP address space among others. It also advertises NGN service and application contact points. Finally, the NACF provides functionality for location management.

The “Service Stratum” consists of “Service Control Functions”, “Application and Service Support Functions” and “Service User Profiles”. The “Service Control Functions” are componentized, i.e., new service control components can be implemented in future releases and deployed to provide new functionality. For example, NGN-GSI supports the IMS (IP Multimedia Subsystem) as a service control component. “Service Control Functions” include gateway controllers and SIP proxies (very similar to IMS – see item B), signaling interworking functions, service authentication and authorization functions, media resource control and media broker functions. The “Application and Service Support Functions” include application gateways and servers. The application gateways provide third-party applications access to exposed NGN capabilities through the ANI. Application servers implement SIP or OSA/Parlay (Open Service Access) and can invoke NGN services by means of contacting the SIP

S-CSC-FE (Serving Call Session Control Functional Entity).

The NGN-GSI approach follows a (session-based) connection-oriented service stratum (SIP and TCP are connection-oriented) over a connection-less IP routing infrastructure. Hence, SIP message routing creates an overlay over IP routing. Every service depends on SIP proxies and session establishment, even the traditional message services, such as SMS (Short Message Service). After session establishment, the RTP (Real-Time Protocol) is used to control the traffic delivery over IP (e.g., VoIP). At the transport stratum, the RACF aims at providing adequate resources for every established traffic flow. A resource reservation request is typically captured from an event at the service stratum or directly sent by a SIP proxy. The RACF translates NGN QoS requirements to technology-dependent QoS requirements and queries the involved access and core network elements regarding resource availability. The RACF then decides if a new session can be accepted or not.

The NGN-GSI enables support for dynamic QoS. The users define their needs to the network through SLA. The service provider offers a service based on the QoS specifications of the contract. The user can also evaluate the QoE (Quality of Experience) received. Adjustments are reassessed and renegotiated with the provider based on the previous results.

Management of user profile information is especially noteworthy in NGN-GSI, since such profiles are required to implement a number of capabilities, including user, service and application authentication, authorization, mobility, location and recovery. The user profile includes information related to access networks, subscribed services, identity, presence, preferences and personal information. Mobility is supported by specific functional entities enabling user and terminal mobility. NGN-GSI aims to support the so-called *generalized mobility*.

B. *NGN – IMS Standard*

IMS emerged with the goal of integrating traditional mobile services and the Internet. The IMS was originally specified by 3GPP, and like ITU-T, it does not standardize equipments or end applications but a collection of functions linked by standard interfaces. Manufacturers are free to combine multiple functions in one device or to split a function into two or more physical devices. IMS consists basically of a service control layer based on SIP and a packet network based on IP technology and IETF protocols. IMS supports a diversity of access networks, including GSM (Global System for Mobile Communications), WLAN (Wireless Local Area Networks), 3G and DSL (Digital Subscriber Line). IMS service control is exposed to third-party applications by means of application gateways, which are based on SIP or OSA/Parlay. Such approach provides an interface similar to NGN-GSI ANI.

Figure 3 shows an overview of the IMS architecture as defined by 3GPP [2]. The IMS terminal is usually called User Equipment (UE). The HSS (Home Subscriber Servers) is the central repository of information related to users, such as location, security (authentication and authorization), user profile (including the registered services) and the currently allocated S-CSCF (Serving-CSCF).

The CSCF (Call/Session Control Function) process the SIP signaling via its three functional instances:

- P-CSCF (Proxy-CSCF);
- I-CSCF (Interrogating-CSCF);
- S-CSCF (Serving-CSCF).

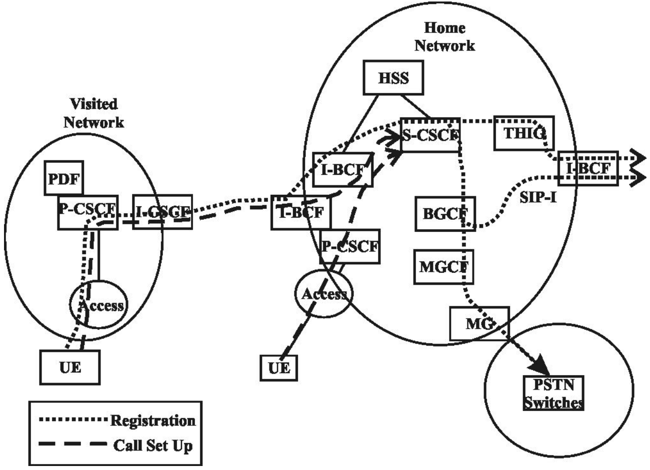

Fig.3. IMS Functions.
(Source : Funicelli, V. B. - NGN and IMS II)

Acting as a SIP proxy server, the P-CSCF is the first contact point between the IMS terminal and the network. The I-CSCF is a SIP proxy located at the edge of the network and acts as the entrance proxy for requests originated outside a local IMS network. The S-CSCF is responsible for routing SIP messages to complete the service establishment e.g., relying the messages to the Application Servers or to the session breakout gateways toward the destination IMS domain or PSTN. The S-CSCF interacts with the HSS via the Diameter protocol to authenticate and obtain the user profile. Similar to the RACF, the IMS defines a PDF (Policy Decision Function) to translate the requirements of SLA parameters to the IP network and the underlying link layer technologies. The BGCF (Breakout Gateway Control Function) is used for sessions that are initiated by an IMS terminal and terminate in the PSTN (Public Switched Telephony Network). The BGCF decides whether the translation of messages to the PSTN will occur into the existing network or if messages should be sent to other IP network. The MG (Media Gateway) provides interfaces the circuit-switched network at the data plane, allowing the IMS to handle legacy PSTN traffic. For this, it translates media TDM (Time Division Multiplexing) to RTP/UDP/IP packets based on the instructions received from the MGCF (Media Gateway Control Function).

III. NEW GENERATION NETWORK

Requirements for the global communication infrastructure known as the Internet have changed considerably since its conception in the end of the seventies. At that time, there were only hundreds of hosts connected to ARPANET (Advanced Research Projects Agency Network). Nowadays, this number has increased significantly to more than 500 million [4] and it is expected to increase even more. The notion of pervasive computing is expected to become part of people's daily lives through a myriad of sensors and mobile devices, enabling new electronic services such as e-health, remote medical care, environmental monitoring, e-government, social networking, etc. Moreover, universal access to information and communication should be provided “anywhere/anytime”.

In this sense, there are some network attributes that are being considered key features for the Future Internet (FI) architectures, including:

- Mobility and Ubiquity;
- Capacity, Reliability and Availability;
- Security and Privacy;
- Generality;
- Real-Virtual Worlds Integration;
- Content/Information-Centrism;
- Service-Centrism;
- Autonomic Networking.

Mobility and Ubiquity refer to anywhere/anytime communications wherever/whenever a person (or an object) is. Capacity, reliability, availability refer to network features to provide the services required by the users and, security and privacy refer to safety in using the network. Generality is to provide means to use generically network substrate (hardware) resources, such as transport, storage and processing capabilities. This can be implemented by means of virtualization techniques that create an abstraction layer between hardware substrate resources and software network entities yielding a flexible, resource efficient and customizable network substrate. It enables the support not only of virtual machines and distributed applications, but also virtual nodes (routers) and networks (slices). Network virtualization is a hot topic in current FI designs, whereas cloud computing today is limited to the virtualization of computing resources.

Real-virtual world integration aims at contextualizing real world information to enhance virtual world services and applications. Real world information can be obtained by NEDs (Network Enabled Devices), such as sensor nodes, RFID (Radio Frequency IDentification) tags, etc. Several authors expect a vast amount (billions) of NEDs in FI. Real world information like temperature, pressure and presence will become available to the web to contextualized use. For example, an application could help users to check if their cars have gas or not. Although each NED generates little traffic, a myriad of them can generate significant traffic. NEDs with Internet access form what is being called *Internet of Things*.

Content/Information-centrism [9,10] means the ability to handle content/information itself as a first-class citizen in the architecture. While current IP networks were designed to solve end-to-end host connectivity, i.e., host-centrism, information-centric networks offer new network primitives (e.g., publish/subscribe) to request information and service access independently from the specific network locators of the servers delivering the data. This line of thought is remarkably being pursued by Internet pioneer Van Jacobson and the Content-Centric Networking (CCN) approach [9]. Similarly, service-centrism can be referred as the capability of handling services themselves as addressable entities in the architecture, pushing the principles behind Service-Oriented Architectures (SOA) to be at the core of future inter-networking. Autonomic networking is the so-sought attribute that could minimize human activity in network operation. It is inspired in autonomic systems and computing. The idea is to design networks capable to self-manage, self-control, self-optimize, self-configure, self-heal, etc., generically speaking, networks with self-* properties.

IV. DISCUSSION

The features and approaches presented above are neither exhaustive not definitive, especially as many are still evolving and very much in its early stages. However, we belief they provide a basis to start a discussion on how they are being approached among different projects and potentially delivered by the telecom NGN proposal. The essence of this discussion can be found in Table 1, where the approaches of NxGN and NwGN are compared side by side. Considering the mobility and ubiquity aspects, we found that mobility in NxGN, specifically in IMS standard, is based on SIP mobility capabilities and by IP anchor points in the transport stratum (e.g., GGSN) and IETF Mobile IP extensions. In NwGN, there are several new proposals mostly around the identifier/locator split such as LISP [6] and Six/One [7] that provide network mobility and multi-homing, i.e., multiple attachment points to the network to provide more reliability, redundancy, load balancing, etc. Mobility in NGN-GSI is supported by T-13: TLM-FE (Transport Location Management Functional Entity) as described in ITU-T Recommendation Y.2012 [2]. This function creates a mapping table between terminal IP address and network location information at NACF. Therefore, it is well-suited to decouple the identity from location.

IMS and NGN-GSI depends on IP, SIP and other functional entities scalability to deal with a large number of NEDs. NAPT hugely decreases traceability in IP NEDs. In NwGN NEDs connectivity, traceability, security, addressing and information contextualization are being rethought.

NxGN is a managed environment with tight user ID control and relies on IPsec for data plane security while NwGN explores new paradigms. The first one is the establishment of trusted relations among users and network entities. The second one is called consented communications, where information is transferred to receiver only if it agrees. Another paradigm change is securing information itself, instead of connections, since users are ultimately interested in timely, authentic information delivery (cf. [9.10]).

With respect to generality, separation of upper layer services from transport technologies is a common (recursive) topic in any network technology. NGN follows this rationale since its conception to move beyond traditional, vertically integrated networks to modular, multi-service networks based on softswitches (i.e., CSCF) that uncouple signaling from user data transport. The NxGN transport stratum service awareness depends on SIP proxies, gateway controllers and RACF. In NwGN, separation of routing from forwarding is a common thread. Resembling NGN softswitches, software-defined networks (cf. OpenFlow [11]) represent a promising approach to pragmatically evolve the network control plane, enabling rapid innovation cycles and the emergence of virtual networks. Information-centric approaches could also take advantage of virtualization to enable new ways of content access and distribution. In NxGN, where standard IP stack protocols are used, SIP proxies create a centralized service-centric approach. In contrast, NwGN FI architectures adopt SOA (Service-Oriented Architecture) as the starting point for distributed service compose-ability solutions.

Finally, OAM in IMS and NGN-GSI depends on SNMP (Simple Network Management Protocol) and proprietary service stratum management tools. The complexity in OAM is increasing. Operational staff will be more and more stressed. Human intervention is remarkably frequent. In NwGN, autonomic approaches are being considered to create self-managed networks, reducing human intervention, increasing quality, and addressing cross-domain issues.

V. CONCLUSION

This paper provides a first impression on design approaches taken for IMS, NGN-GSI and FI. While both developments have different timing scopes, understanding their core divergences and their potential synergies seems to be required in steering networking research agendas. Towards this end, we have provided a preliminary comparison. Apparently, NxGN (i) will suffer with the impact of NEDs; (ii) will have more complex OAM, increasing OPEX; (iii) traceability and other IP/TCP/UDP/SIP security limitations will continue causing trouble. NwGN constitute a never-ending set of promissory solutions for these limitations and others, but currently lacks on integrated proposals. Overarching and pragmatic research steps seem necessary to convey the requirements and incentives of the multiple parties.

REFERENCES

[1] Tomonori, A, “A New Generation Network - Beyond NGN”, ITU-T Kaleidoscope Academic Conference, May 2008.

[2] ITU-T Recommendation Y.2012, “Functional Requirements and architecture of the NGN”, release 1, 2006.

[3] http://www.3gpp.org/.

[4] Roberts, J., “The clean-slate approach to future Internet Design: a survey of research initiatives”, Ann. telecommun. 64:271-276, 2009.

[5] Akari, “New Generation Network Architecture AKARI Conceptual Design”, Project Description v1.1. http://akari-project.nict.go.jp/eng/conceptdesign.htm. Accessed 20 April 2010.

[6] Farinacci, D., et al. Draft-ietf-lisp-06.txt- Locator/ID Separation Protocol (LISP), 2010.

[7] Vogt, C., Draft-vogt-rrg-six-one-02 - Six/One: A Solution for Routing and Addressing in IPv6, 2009.

[8] The Future of the Internet, “A Compendium of European Projects on ICT Research Supported by the EU 7th Framework Programme for RTD”, 2008.

[9] Jacobson, V., Smetters. D., Thornton, J., Plass, M., Briggs, N. and Braynard, R.. “Networking Named Content”, CoNEXT 2009, December 2009, Rome.

[10] Trossen, D., Särelä, M., and Sollins, K., “Arguments for an Information-Centric Internetworking Architecture”, ACM CCR, April 2010.

[11] OpenFlow, http://www.openflowswitch.org/. Accessed 29 June 2010.

TABLE I
COMPARISON BETWEEN NXGN AND NWGN.

	NGN-GSI and IMS	NwGN (Future Internet)
Mobility	SIP-based. Suffers with IP limitations regarding mobility. IMS also relays on cellular networks mobility support. NGN-GSI uses an ID/Loc decoupling.	Mobility support based on ID/Loc and Information/Loc splitting. Protocol examples are LISP, Six/One, PSIRP [10].
Ubiquity	Traceability is limited due to the IP address space depletion. IP ubiquity depends on NAPT and other entities scalability.	Ubiquitous connectivity is considered as a tendency. New approaches to deal with traceability, context, addressing and localization.
Security	IPSec-based. Suffers with traditional IP security limitations as well as new ones related to SIP.	New approaches, such as trust relations, publish/subscribe paradigm, securing information objects and self-security mechanisms.
Generality	Transport resources are decoupled of service stratum. Limited network customization is provided by RACF.	Transport, processing and storage virtualization. Coexistence of different service aware virtual networks. E.g. FIA MANA, AutoI [8], Software-defined networks (e.g., OpenFlow [11]).
RVWI	Support for NEDs is virtually nonexistent. Moreover, it is unclear to what extent the IP network can scale in order to support the phenomenal growth predicted for NED.	NEDs' requirements are being considered. Information contextualization, privacy and security are being redesigned. E.g. FIA RWI [8].
Information-centrism	Information exchange supported by traditional protocols, such as HTTP, RTP, SMTP, etc. OSA/Parlay and SIP gateways and servers.	New paradigm to redesign network architectures from the information point of view, e.g. CCN and PSIRP [9, 10].
Service-centrism	SIP and its proxies are used to orchestrate services. Highly centralized approach. SOA-based Service Delivery Platforms (SDP) approach. App-store paradigm.	SOA is considered in some approaches to provide service compose-ability and orchestration. Distributed approach. E.g. SOA4ALL, S-Cube [8].
Autonomy	Virtually all operation depends on proprietary management software, which requires human interference in a daily basis.	Autonomic networking could provide self-emergent behavior. Network operation emerges as a result of distributed autonomous nodes (cf. MANA, AutoI, 4WARD, Akari [5, 8]).