Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14016
Date:	2009-06-10
Replaces:	
Document Type:	Working Draft
Document Title:	Revised text of ISO/IEC WD 29181, Future Networks : Problem Statement and Requirements
Document Source:	SC 6/WG 7 Tokyo meeting
Project Number:	
Document Status:	As per the SC 6 Tokyo resolution 6.7.10, this document is circulated to SC 6 NBs for comment.
Action ID:	COM
Due Date:	2009-09-10
No. of Pages:	32

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

6N14016

7TOK-31

Title: Revised text of Future Networks : Problem Statement and Requirements (ISO/IEC 29181)

Source: ISO/IEC JTC 1/SC 6/WG 7 Meeting (Tokyo, June 2009)

Status: This document is the revised text of ISO/IEC JTC1 WG7 (TR.FNPSR), which is an output document made in the - Tokyo meeting (June 2009).

TABLE OF CONTENTS

Technical Report 29181 TR.FNPSR

FUTURE NETWORKS : PROBLEM STATEMENT AND REQUIREMENTS

SUMMARY

This Technical Report(TR) describes the definition, general concept, problems and requirements for Future Networks (FN). Also, it discusses a milestone for standardization on Future Networks (FN).

KEYWORDS

TBD

FOREWORD

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

1. SCOPE

This Technical Report(TR) describes the definition, general concept, problems and requirements for Future Networks (FN). Also, it discusses a milestone for standardization on Future Networks (FN). The scope of this TR includes:

- Motivation of Future Networks (FN)
- Definition, general concept, and terminologies of Future Networks (FN)
- Services and applications in Future Networks (FN)
- Problem statement on current networks
- Design goals and high-level requirements for Future Networks (FN)
- Milestones for standardization on Future Networks (FN)

2. NORMATIVE REFERENCES

TBD

3. DEFINITIONS

This Technical Report (TR) uses the following terms and definitions.

EdNote : This is an initial definition for better understanding of Future Networks. Further contributions are invited.

- Future Network (FN) : A network which is able to provide revolutionary services, capabilities, and facilities that are hard to provide using existing network technologies [1].

Also, we define the following terms related to futuristic capabilities for Future Networks.

- Clean-slate design : clean-slate design means that a system (network) is re-designed from scratch. It should be based on long-term, revolutionary approach. In Clean-slate design, the backward compatibility may or may not be required [7].
- Network virtualization : the purpose of network virtualization is to de-ossify the Today's network. It could realize virtual network with programmable network elements and support the architecture of multiple architectures. Different virtual networks can provide alternate end-to-end packet delivery systems and may use different protocols and packet formats [8].
- Cross-layer communications : cross-layer communications create new interfaces between layers, redefine the layer boundaries, design protocol at a layer based on the details of how another layer is designed, joint tuning of parameters across layers, or create complete new abstraction.
- Autonomous service : It enables users or services in motion to configure autonomously and to mange networks.
- Context-awareness : It enables applications or services to adapt their behaviour based on their physical environment.
- Data-centric/content-centric : It supports contents-based applications and services.

- Service overlay: It investigates the dynamic construction of service-based overlay networks and their control and maintenance.
- Customizable QoS/QoE: It supports preference setting and service composition/re-composition accordingly
- Economic incentives: the encouragement, rewards, compensation which motivates the parties (components/participants) economically to contribute for networking and/or services and/or to provide their resources.

[EdNote] This is a basic view from Ed's contribution. Based on the contributions, the definition will be revised.

[Note] The definitions of Internet and NGN:

- Internet: A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network[4].
- The Internet: a global system of interconnected computer networks that interchange data by packet switching using the standardized Internet Protocol Suite (TCP/IP). It is a "network of networks" that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies [5].
- Next Generation Network (NGN): A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users [6].

4. ABBREVIATIONS

TBD

5. INTRODUCTION

This Technical Report(TR) describes the definition, general concept, problems and requirements for Future Networks (FN). Also, it discusses a milestone for standardization on Future Networks (FN).

EdNote : After all of section is reviewed and added based on further contributions, the section will be written up.

6. MOTIVATION

EdNote : this section should be rephrased. Further contributions are invited.

6.1 NEEDS TO RESEARCH AND STANDARDIZE THE FUTURE NETWORK

The current Internet becomes essential communication infrastructure, not only for information and communications but also for social critical infrastructures such as e-government, energy/traffic controls, finance, learning, health, etc.

Even though the current Internet is such an essential infrastructure, we see that there are many concerns on the following aspects on current Internet, including IP based networks: scalability, ubiquity, security, robustness, mobility, heterogeneity, Quality of Service (QoS), re-configurability, context-awareness, manageability, data-centric, economics, etc. Also, the advancement of mass storages, high speed computing devices and ultra broadband transport technologies (e.g. peta/exa/zeta bps) enables many emerging devices such as sensors, tiny devices, vehicles, etc. The resultant new shape of ICT architecture and huge number of new services cannot be well supported with current IP technologies.

Therefore we need to study and standardize the Future Networks (FN) which overcome the limitations of current IP, and enable new plentiful services. The Future Network, which is anticipated to provide futuristic functionalities beyond the limitations of the current network including Internet, is getting a global attention in the field of communication network and services.

The current IP technologies have significant deficiency that need to be solved before it can be become a unified global communication infrastructure. Particularly, there are problems with a large number of hosts, such as sensors, the various wireless and mobile nodes, multiple interface and multi-homed nodes, the support of the fast mobile hosts, the safe e-transaction, the quality of service guarantee at a network, the business aspect complementary, and etc., on current IP network, so various researches had been being in progress to solve these problems. Further, concerns are drastically increasing now that shortcomings would not be resolved by the conventional incremental and 'backward-compatible' style of current research and standardization efforts. That is the reason why the Future Networks research effort is called as “Clean-Slate Design for the New Internet’s Architecture”. It is assumed that the current IP’s shortcomings will not be resolved by conventional incremental and “backward-compatible” style designs. So, the Future Network designs must be discussed based on clean-slate approach.

6.2 VALUE AND VISION OF FUTURE NETWORKS

The business model of Future Networks (FN) aims for profit sharing among network providers, service providers, application providers and end users by building cooperative eco-systems between them [1].

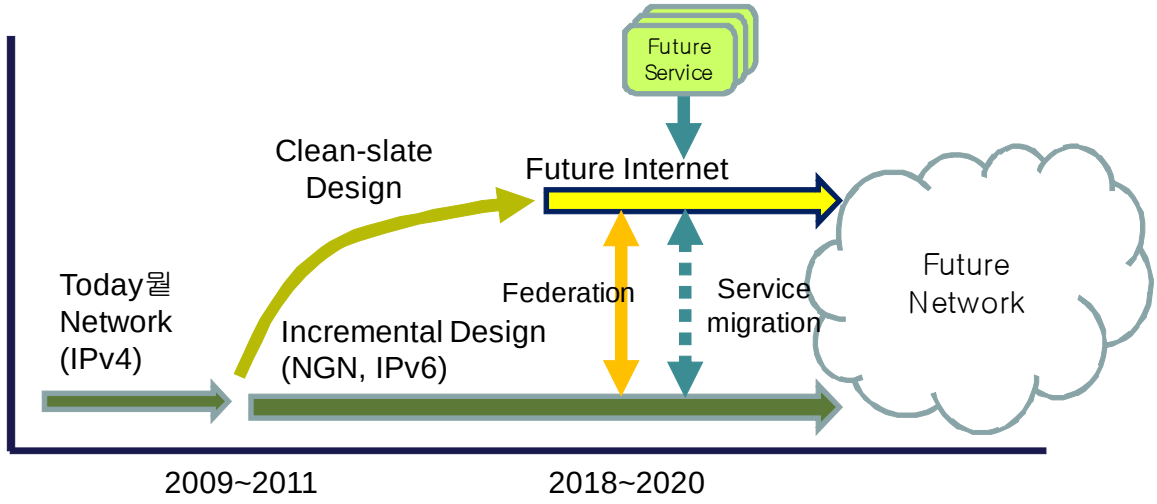
It can be accomplished by openness and accommodating various requirements of each party.

Figure 1 illustrates vision and roadmap of Future Networks.

[Editor's Note] Further contributions are invited.

EdNote : More explanation on the fugure is required. This is some of example of vision and roadmap.

- Terms should be defined in advanced.
- Timeline should be clearly proposed and discussed.
- Term Federation should be explained in advanced.
- Future services should be proposed.
- Future network vs. Future Internet.



[Figure 1] Vision and Roadmap of Future Network

7. GENERAL CONCEPT OF FUTURE NETWORK

General concept of Future Networks (FN) is clarified and listed as follows :

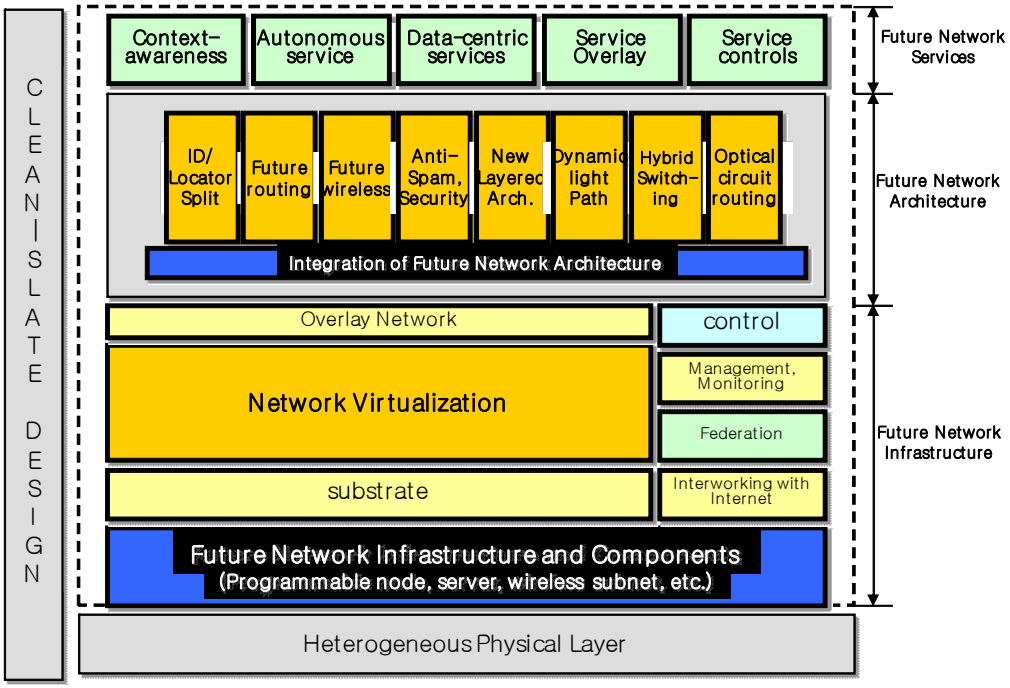
- ❍ The FN is the network of the future which is made on Clean-slate Design. Note : Clean-slate approach was understood as a design principle, not deployment aspect.
- ❍ It should provide futuristic functionalities beyond the limitations of the current network including Internet (IP).
- ❍ Revolutionary approach should be considered for the FN.
- ❍ The FN should not dependent on the current technologies and solutions.
- ❍ FN provides mechanisms that benefit every participant as much as they contribute.
- ❍ The backward compatibility may or may not be required.

The futuristic functionalities could be :

- ❍ Network virtualization
- ❍ Programmable networks
- ❍ New layered functions (e.g., cross-layer communications),
- ❍ Autonomous management and maintenance
- ❍ New control and management functions for network resource sharing and isolation
- ❍ Context-awareness services
- ❍ Data-centric or content-centric services
- ❍ Media distribution
- ❍ Customizable QoS/QoE

Future 2 illustrates a basic concept of Future Networks for research and standardization.

[Editor's Note] Further contributions are invited.



[Figure 2] Basic Concept of Future Networks

8. SERVICES AND APPLICATIONS IN FUTURE NETWORKS

EdNote: Further revision is required.

In the section, the following future services are envisioned and considered as benchmark services to achieve to build the Future Networks.

Though the listed services are shown as examples (not normative), they imply essential, societal and infrastructural services, and require considerable network resources that current Internet technology cannot support.

EdNote: References should be moved in Bibliography section.

Research projects	Envisioned future services	References
GENI [15] (Global Environment for Network Innovations)	− Ubiquitous health care − Participatory urban sensing – Dealing with personal data − Tele-presence	GENI Research Plan GDD-06-28 Version 4.5 of April 23, 2007
NwGN [16] (New Generation Network Architecture)	− Essential services: medical care, transportation, emergency services	AKARI Conceptual Design April 2007, AKARI Project
EU FP-7 [17] (European Union Framework Program-7)	− Personal service creation − Future home – Future of traffic − Virtual reality − Productivity tools	The future Internet: the operator's vision,' Eurescom P1657, EDIN 0546-1657, 2007.11

Distinguished from the traditional CT (communication technology) or IT (information technology) services, the services of the future should be reconsidered with broader concept since the Future Networks will encompass wide range of heterogeneous networks [18]:

- The problem of scope, functionality, capability, granularity, time, scale, intelligence, roles, people and their stuff, and "at your service"

Future Network (or future) services can be stated as:

- the services which emerge in the year 2010 ~ 2030

  : FN services emerge with short/mid/long term time line.

- the services which are provided and inter-work on top of both clean slate based new networks and/or existing networks

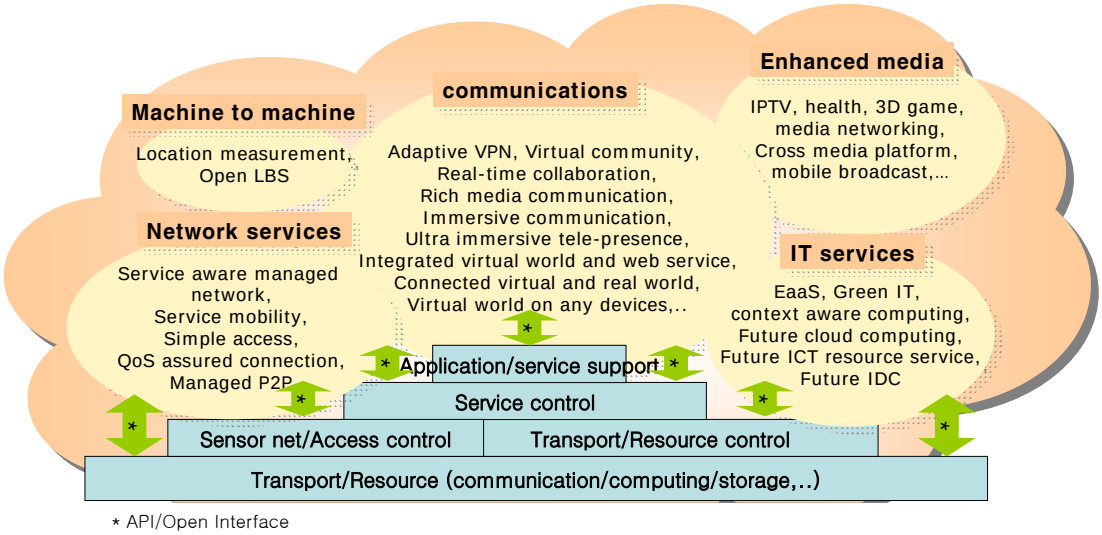
  : Since services are inherently transport /access network independent, it may span across the exiting and clean slate based infrastructures.

- the services whose features are both user centric (I-Centric) and network centric (Net-Centric)

  : The purpose of future services is to satisfy and provide best convenience for end users with optimal usage of network resources.

And it would cover the IT, Telecom, Media and Cloud computing areas, which can be provided on any layers of network (Figure 4): for example, future ICT resource services may be provided directly on transport and resource layers, or may be provided on transport/resource control layer in case with quality controls. Likewise, immersive communication services may be provided on application/service support layer, or service control layer according to

provider's own service policy and capabilities. Capabilities of each network layer may be accessed with open standardized interfaces.



[Figure 4] Services Concept of Future Networks

The key features the Future Network services should support include:

- Context awareness
- Dynamic adaptiveness
- Self organization and Self-configuration
- Self-detection and self-healing
- Distributed control
- Mass data control
- etc

9. PROBLEM STATEMENT

The problems for the Future Networks could be classified into i) basic problems and ii) problems with original Internet design principles as follows :

9.1 BASIC PROBLEMS

9.1.1 ROUTING FAILURES AND SCALABILITY

The today's Internet is facing challenges in scalability issues on routing and addressing architecture. The problems have been examined as being caused by mobility, multi-homing, renumbering, provider independence (PI routing), IPv6 impact, etc. on the today's Internet architecture. The problem is known to be caused by current Identifier-Locator integration architecture within IP address scheme. As the Internet continues to evolve, the challenges in providing a scalable and robust global routing system will also change over time.

[Editor's Note] Further contributions are invited.

9.1.2 INSECURITY

One of the main problems on the today's Internet is not to provide secure communication. As current communication is not trusted, problems are self-evident, such as the plague of security breaches, spread of worms, and denial of service attacks. Even without attacks, service is often not available due to failures in equipment of fragile IP routing protocols.

[Editor's Note] Further contributions are invited.

9.1.3 MOBILITY

Current IP technologies are designed for hosts in fixed locations, and ill-suited to support mobile hosts. Mobile IP was designed to support host mobility, but Mobile IP has problems on update latency, signaling overhead, location privacy. Also the current Mobile IP architecture is facing challenges in fast and vertical handover.

[Editor's Note] Further contributions are invited.

9.1.4 QUALITY OF SERVICE

Internet architecture is not enough to support quality of service from user or application perspective. It is still unclear how and where to integrate different levels of quality of service in the architecture.

[Editor's Note] Further contributions are invited.

9.1.5 HETEROGENEOUS PHYSICAL LAYERS, APPLICATIONS AND ARCHITECTURE

IP architecture was known as "a narrow waist" of today's Internet hourglass. Today's IP enables a broad range of physical layers and applications. But, this physical layers and applications heterogeneity poses tremendous challenges for network architecture, resource allocation, reliable transport, context-awareness, re-configurability, and security.

[Editor's Note] Further contributions are invited.

9.1.6 NETWORK MANAGEMENT

The original Internet lacks in management plane. Instant and easy management for users is highly required, as the Future Internet can be composed of new emerging heterogeneous wireless, mobile and ad-hoc architectures. For example, the following autonomic management should be provided to future mobile networks: self-protecting, self-healing, self-configuring, self-optimizing, etc.

[Editor's Note] Further contributions are invited.

9.1.7 CONGESTIVE COLLAPSE

Current TCP is showing its limits in insufficient dynamic range to handle high-speed wide-area networks, poor performance over links with unpredictable characteristics, such as some forms of wireless link, poor latency characteristics for competing real-time flows, etc.

[Editor's Note] Further contributions are invited.

9.1.8 OPPORTUNISTIC COMMUNICATIONS

Original Internet was designed to support always-on connectivity, short delay, symmetric data rate and low error rate communications, but many evolving and challenged networks (e.g., intermittent connectivity, long or variable delay, asymmetric data rates, high error rates, etc.) do not confirm to this design philosophy.

[Editor's Note] Further contributions are invited.

9.1.9 FAST LONG-DISTANCE COMMUNICATIONS

Current Internet is based on the philosophy of 'end-to-end' packet forwarding scheme i.e., best-effort network, so that a point of bottleneck causes a delay. When the distance becomes longer, the probability of bottleneck-appearance becomes higher.

[Editor's Note] Further contributions are invited.

9.1.10 MEDIA DISTRIBUTION

Related to the media, the current problems are the lack of true interaction between the people and the media, the lack of efficient search and retrieval mechanisms, the lack of truly collaborative environments, the disembodied and non-multimodal access to the content, the gap between content (media) and senses and the lack of emotional communication among users and communities. The current network problems are its reliability aspects, its complex management, its asymmetric nature (more download than upload), relatively limited capacity of access lines, the limitation to always achieve ubiquity of access, the lack of integration of QoS and security within mobility, the lack of security mechanisms (intrusion detection, attack mitigation, quick reaction to attacks, etc.) and the difficulties for monitoring the network performance.

9.1.11 ECONOMY AND POLICY

There is also a question of how network provider and ISP continue to make profit. Some of the economic travails of the today's Internet can be traced to a failure of engineering. The today's Internet lacks explicit economic primitives.

EdNote : The scope of this section should be technical aspects, not link economic and sustainable development/energy efficiency of FN compared current network.

[Editor's Note] Further contributions are invited.

9.2 PROBLEMS WITH ORIGINAL INTERNET DESIGN PRINCIPLES

9.2.1 PACKET SWITCHING

Today's Internet technologies use packet switching making it hard to take advantage of improvements in optical. Packet switching is also known to be inappropriate for the core of networks and high capacity switching techniques (e.g., Terabit). Instead, we need to re-design dynamic circuit switching or hybrid (packet –circuit) switching for the core of networks.

[Editor's Note] Further contributions are invited.

9.2.2 MODELS OF THE END-TO-END PRINCIPLE

The models of the end-to-end principle has been progressively eroded, most notably by the use of NATs, which modify addresses, and firewalls and other middle boxes, which expect to understand the semantics behind any given port number (for instance to block or differentially handle a flow). As a result, end hosts are often not able to connect even when security policies would otherwise allow such connections. This problem will only be exacerbated with the emerging need for IPv4-IPv6 translation. Beyond this, other changes in the way the Internet is used has stressed the original unique-address:port model of transport connections.

[Editor's Note] Further contributions are invited.

9.2.3 LAYERING

Layering was one of important characteristics of today's Internet technologies, but at this phase, it has inevitable inefficiencies. One of challenging issues is how to support fast mobility in heterogeneous layered architecture. We should explore where interfaces belong, and what services each layer must provide.

[Editor's Note] Further contributions are invited.

9.2.4 NAMING AND ADDRESSING

Naming and addressing schemes are two essential and key elements in a network structure and service provisioning. How the naming and addressing are designed has a critical impact on the characteristic and performance of the networks. The fundamental structure of naming and addressing scheme in current networks especially the IP networks are mostly designed over 40 year's ago and is a major root of the problems facing existing networks. For example, the DNS to IP Address search and translation process, the centralized domain name registration, the hierarchical structure etc. limits the potential of existing networks. We should explore new naming and addressing design principles to help achieve Future Network objectives."

10. GENERAL REQUIREMENTS

In this section, new design goals and general requirements for the Future Networks are described.

10.1 SCALABILITY

Scalability issue is emerging as the cultural demands for networking toward the future is growing continuously. During the next 10-15 years, it is envisioned that the telecommunication networks including internet will undergo several major transitions with respect to technologies, services, size, and so on. For example, machine-to-machine communication might be pervasive in addition to the current way of communication that human-beings are involved.

- Scalability consideration shall include following aspects:
- Routing and addressing architecture
- Multi-homing and provider independence (PI routing)

[Editor's Note] Further contributions are invited.

10.2 NAMING AND ADDRESSING SCHEME

In order to fulfill its ambitious goals, Future Networks may need new naming and addressing schemes which would require:

- The new naming and addressing schemes should take the advantage of the principle of clean slate design to explore, identify, experiment complete new architecture.
- The new architecture does not have to abide by the old network naming and addressing rules, but on the other hand, the issue of compatibility and interoperability should also be considered when technical proposals are evaluated.
- An architecture which would help Future Networks to achieve objectives such as scalability, security, mobility, robustness, heterogeneity, quality of service, customizability and economic incentive.

Ability to integrate various networks, to support new protocols, to provide bases for new applications and services, and to give support to new networking technologies

.

10.3 SECURITY

The Future Networks should be built on the premise that security must be protected from the plague of security breaches, spread of worms and spam, and denial of service attacks, and so on.

Especially, as for authentication, the following requirements are carefully investigated.

10.3.1 PRIVACY

Because of the practical considerations to prevent attacks such as spoofing, we would like to bind each user or device to a single identity. However, users value their privacy and are unlikely to adopt systems that require them to abandon their anonymity. For example, most users would resent a system such as a Mobile IP Network that allows others to know their locations. Balancing privacy concerns with authentication needs in Future Network will require codifying legal, societal and practical considerations.

10.3.2 MOBILITY

Traditional authentication mechanisms for networks frequently base on a relatively static or fixed network, and even ad hoc networks typically assume limited mobility, often focusing on handheld PDAs and laptops carried by users. The design of authentication mechanism for Future Networks should consider the case of highly mobility in a network. For example, in vehicular networks, since two vehicles may only be within communication range for a matter of seconds and many of whom it has never interacted with before and is unlikely to interact with again, we cannot rely on protocols that require significant interaction to process authentication between the sender and receiver.

10.3.3 PEER

Why the authentication and trust of ends become a challenge in current networks? One of important reasons is that many authentication mechanisms can not provide a real mutual authentication procedure. For example, we currently focus on how to identify a spoof station by the server, while a station usually does not have an effective scheme to check the identity of a server such as an AP in a network. Hence, the authentication mechanisms of peer and multi-security must be designed for Future Networks.

10.3.4 RESOURCE

With the increasing ubiquity of networks, it can be seen that size and cost constraints on nodes result in corresponding constraints on resources such as energy, memory and computational speed, resulting in the challenge of authentication for Future Networks. For example, due to the low computational and memory overhead, it is not practical to use asymmetric cryptosystems such as RSA for authentication in Wireless Sensor Networks where each node consists of a slow under-powered processor with only 4 KB of RAM space.

10.3.5 HETEROGENEITY

Authentication mechanisms for Future Networks should accommodate heterogeneous network architecture (e.g., wireless, mobile, and ad-hoc) and application. For example, original authentication mechanisms usually were designed to support host identification. However, new emerging services are more likely data-centric. The aim to authentication is not host but data. Users just want to access particular data or service (e.g., P2P) and do not care where the data or service is located and which host they are connecting to.

10.3.6 ATTACK

There are many kinds of attack against current authentication mechanisms. For example, attacks against authentication keys, authentication exchange procedure, initial enrolment process, management of authentication keys, etc., and attack methods including Eavesdropper Attacks, Man-in-the-middle Attacks, Replay Attacks, Verifier Impersonation Attacks, Password Discovery Attacks, etc. Authentication mechanisms for Future Networks should be possible to implement a range of countermeasures to the authentication attacks described above.

10.4 MOBILITY

The Future Networks should support mobility of devices, services, users and/or groups of those seamlessly. The following requirements need to be considered for efficient mobility control in Future Networks.

EdNote : The following requirements are mainly related to L3 issues. Thus more investigation including other layers is required.

- Separation of user identifier and device locator : Since the current Internet was designed mainly to support static terminals, it is difficult to provide seamless mobility for mobile users/terminals. One of the reasons for such difficulty comes from that IP address is used as user identifier and device locator both. Therefore it is required that the user identifier should be separated from device locator to effectively support mobile terminals.
- Separation of mobility control function from user data transport function : In the mobility point of view, the mobility control function needs to be separated from the user data control function, which will ensure that a mobility control scheme (or protocol) can be used with a variety of user data transport functions (e.g., data forwarding, routing protocols, etc). In addition, it is noted that the mobility control (signaling) operations may require real-time and high-reliable transmissions, whereas the user data transport operations (or application) may require different levels of reliability and timeliness.
- Location Privacy in Mobility : In Future Networks, the location privacy should be provided for mobile users. In particular, when a sender transmits some packets to a receiver, the IP address (or locator) of sender can be hidden to the receiver, when necessary. Future Internet should be able to provide this location privacy in the mobility point of view.
- Support of Network-based built-in mobility control : To provide seamless mobility for users in the effective way, the network-based mobility control functionality should be provided in the Future Networks. In particular, the mobility control functionality needs to be provided in the fashion of 'built-in' rather than add-on.'
- Route optimization : By movement, the location of a mobile terminal may change, hence the route for data delivery may change. Future Networks should be able to provide the route optimization for mobile terminals, which needs to be considered for design of the mobility control for Future Networks.
- Use of lower layer information : To provide seamless services for mobile users, the mobility control for Future Networks needs to utilize the lower layer information (e.g., link-layer triggers such as link-up, link-down, etc), if possible, as known as the cross-layer design or optimization.

Also, following features should be provided under the context of mobility in the Future Networks.

10.4.1 CONTEXT-AWARENESS

Mobility in the Future Networks is expected to support context-awareness. Section 10.7.1 describes details on context-awareness. Although location is a primary capability, location-awareness does not necessarily capture things of interest that are mobile or changing.

[Editor's Note] Further contributions are invited.

10.4.2 MULTI-HOMING AND SEAMLESS SWITCHING

Mobility in the Future Networks should support multi-homing, i.e., multiple access paths to heterogeneous /homogeneous networks. It is also expected to support seamless switching between those multiple access paths.

[Editor's Note] Further contributions are invited.

10.4.3 HETEROGENEITY

Mobility in the Future Networks is expected to support heterogeneity. Section 10.6 describes details on heterogeneity.

[Editor's Note] Further contributions are invited.

10.5 QUALITY OF SERVICE

The Future Networks should support quality of service (QoS) from user and/or application perspectives. In addition, QoS in the Future Networks is expected to support context-awareness described in section 10.7.1.

[Editor's Note] Further contributions are invited.

10.6 HETEROGENEITY AND NETWORK VIRTUALIZATION

The Future Networks should provide much better support for a broad range of applications/services and enable new applications/services. In addition, it should accommodate heterogeneous physical environments.

[Editor's Note] Further contributions are invited.

10.6.1 APPLICATION/SERVICE HETEROGENEITY

The Future Networks should be designed to support new services and/or applications, e.g., data-centric services. Original Internet was designed to support host-centric, which means users tell client to contact to another host (e.g., telnet, ftp). However, new emerging services are more likely data-centric. Users want to access particular data or service (e.g., P2P) and do not care where the data or service is located.

[Editor's Note] Further contributions are invited.

10.6.2 DEVICE HETEROGENEITY

The Future Networks should support new devices such as sensors, RFIDs, etc.

[Editor's Note] Further contributions are invited.

10.6.3 PHYSICAL MEDIA HETEROGENEITY

The Future Networks should accommodate heterogeneous physical media, such as optical fiber, wireless access (e.g., IEEE 802.11/16/15.4 …), etc. This physical media heterogeneity poses tremendous challenges to Future Internet architecture.

[Editor's Note] Further contributions are invited.

10.6.4 NETWORK VIRTUALIZATION

The Future Networks should support network virtualization. The purpose of network virtualization is to de-ossify the Today's Internet. It could realize virtual network with programmable network elements and support multiple architectures. Different virtual networks can provide alternate end-to-end packet delivery systems and may use different protocols and packet formats. In this principle, for example, a new future service provider who doesn't have its own physical infrastructure just chooses a new particular architecture and to construct an overlay supporting the architecture that the new service provider needs to do. The new future service provider then distributes softwares or codes that let anyone, anywhere, access its overlay [13]. Also, all the resources within the infrastructure could be uniquely defined and shared.

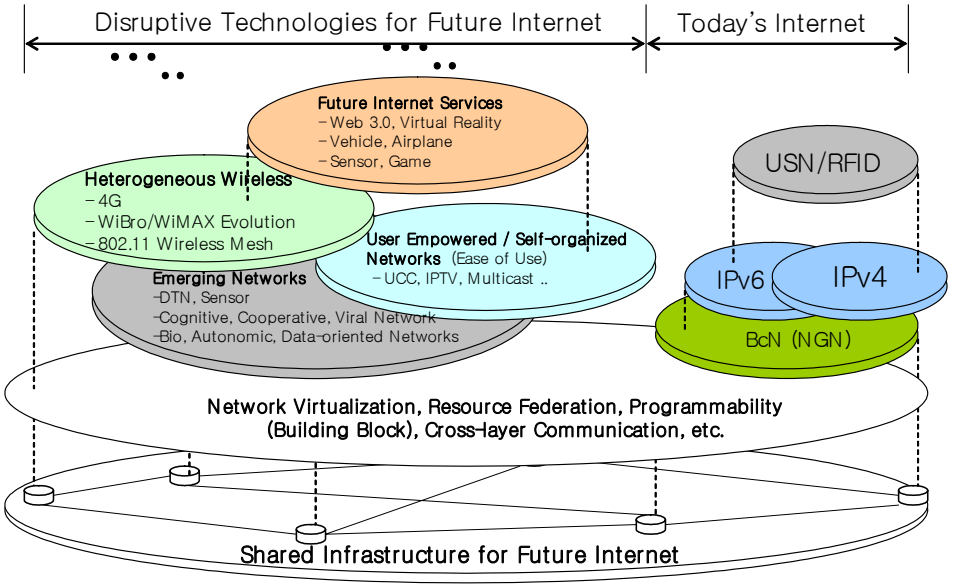
Network virtualization provides a common means to accommodate the new heterogeneous architectures and facilitate architecture revolution. Benefits from network virtualization are listed below : the conceptual benefits from network virtualization are illustrated in Figure 3.

1. Building up a single shared infrastructure for Future Networks : network virtualization can play a central role to build up a shared common infrastructure for Future Networks. The functionalities to support the network virtualization could become the architecture's core functionalities. So, in this assumption, a lot of different networks can be built on a single shared infrastructure for future experiments.

2. Deploying unconventional network architectures : New heterogeneous architectures as well as today's Internet architecture can co-exist on top of a shared infrastructure. Also, different virtual networks may provide alternate end-to-end packet delivery systems and may use different protocols and packet formats. Network virtualization has the flexibility to support a broad range of experiments, services and users. It can support various clean slate-based and disruptive technologies experiments.

3. Deploying new emerging technologies : To deploy new emerging technologies and services such as IPv6, mobile IPTV, wireless mesh (e.g., IEEE 802.11s), etc. each networks should be isolated and distinct path for new services. Meta-Architecture can easily support these kinds of new technologies and services.

4. The Advent of new generation service provider : In this network virtualization scenario, a new generation service provider will appear for Future Networks services. A new generation service provider chooses a particular new architecture, then constructs a virtual network supporting architecture [11]. The new generation service provider could easily support new architecture natively.



[Figure 3] Network virtualization concept

10.7 CUSTOMIZABILITY

The Future Networks should be customizable in accordance with various users and service requirements.

[Editor's Note] Further contributions are invited.

10.7.1 CONTEXT-AWARENESS

The Future Networks shall be aware of context. Three important aspects of context are: where you are; with whom you are; and what resources you are nearby. For example, context-awareness is applied to mobility, it refers to a general class of mobile systems that can sense their physical environment, i.e., their context of use, and adapt their behaviour accordingly. Context awareness is applied to network entities that are aware of any information (i.e. context) that can be used to sense and react based on the environment. The context includes but not limited to the user, device, service, system resources, and network context. The user context can include user characteristics, user's location, user's preference, and environmental constraint of user (e.g. public are where silence is required, working place, home, etc.). The device context can include type and capability of the device. The service context can include service availability, required QoS level, and service performance. The system resource context can include CPU, memory, processor, disk, I/O devices, and storage. The network context can include bandwidth, traffic, topology, and network performance. The Future Networks should support the context management to provide customized and context based services.

[Editor's Note] Further contributions are invited.

10.7.2 RE-CONFIGURABILITY AND SERVICE DISCOVERY

The Future Networks shall import and configure new invented technologies into its architecture. Therefore, programmable and/or re-configurable networking and computing methods need to be adopted. One of the good examples would be programmable and/or re-configurable routers/switches. The Future Internet shall discover a service based on service-specific overlay control.

[Editor's Note] Further contributions are invited.

10.7.3 CONTENT-CENTRIC SERVICES

The Future Networks shall support content-centric services. For example, numbering shall be supported in a content-centric manner.

[Editor's Note] Further contributions are invited.

10.7.4 SERVICE AWARENESS

The Future Networks shall be able to distinguish the type of the delivered service and provide delivery service accordingly to the characteristics of the service. Different service types will require different level of QoS. Thus, the network should be able to distinguish different services types and apply appropriate QoS. The Future Networks needs to provide high quality services based on the required QoS while maintaining network efficiency and low cost. The service awareness functionality can be used to provide a variety of value added services.

10.7.5 SERVICE ROUTING

The Future Networks shall provide service routing which is to provide routing according to the routing policy and the context information (e.g. user, device, service, system resources, and network context). Service routing should support to detect changes of context and adapt its behaviour, efficiently. The Future Networks needs to consider distributed service routing, since it will consists of large number of services and resources in distributed environment.

10.8 MEDIA DISTRIBUTION

In order to accomplish these requirements, some design requirements must be taken into account. Firstly, the content-centric engineering, to deliver the best possible quality within the actual context of the user. Secondly, the content-centric network design, allowing users to access information transparently and with an enhanced findability, without knowing the place or address of the host. Thirdly, design for tussle, supporting flexible business models in an open environment. Fourthly, trustworthiness, ensuring security and privacy for all the stakeholders involved. And finally, flexibility, allowing, for example, a user to fetch information divided into different locations. [29]

10.9 NEW LAYERED ARCHITECTURE

Basically, layering was one of important characteristics of Today's Internet technologies, but recently, it is also reported that it has sometimes inevitable inefficiencies. Therefore, Future Networks may provide cross-layer communication functions. To achieve this, first thing is to exploit the dependency between protocol layers to obtain performance gains and then create new interfaces between layers, redefine the layer boundaries, design protocol at a layer based on the details of how another layer is designed, joint tuning of parameters across layers, or create complete new abstraction. The purpose of cross-layer communications is to provide a way direct communication between protocols at nonadjacent layers or sharing variables between layers. We adopt this principle only within mobile, wireless, sensor sub-networks, since there is a trade-off between optimization and complexity (abstraction). Thus, measurement and monitoring should be given in advanced. Also, it is designed to support at any layer (e.g., physical layer to application layer) and implemented through network virtualization to support flexibility and programmability.

[Editor's Note] Further contributions are invited.

10.10 MANAGEABILITY

The Future Networks will become more and more complex with emerging services and architectural diversity. Therefore, Instant and easy management is desired in the Future Networks.

[Editor's Note] Further contributions are invited.

10.10.1 ROBUSTNESS

The Future Networks should be robust, fault-tolerant and available as the wire-line telephone network is today. Robustness shall be considered from the following aspects.

[Editor's Note] Further contributions are invited.

10.10.2 AUTONOMY

Autonomic management might be provided to future mobile networks: self-protecting, self-healing, self-configuring, self-optimizing, etc.

[Editor's Note] Further contributions are invited.

10.11 ECONOMIC INCENTIVES

The Future Networks shall provide economic incentives to the components/participants that contribute to the networking. For example, network providers and/or ISPs contribute to construct the infrastructure of network. The users of GRID computing contribute to provide resources. Therefore it is desired that the Future Network provides with explicit economic primitives.

[EdNote] Further discussion is required. The following text is not fully discussed yet.

10.11.1 QUALITY OF SERVICE/EXPERIENCE

Future Networks should support quality of service (QoS) and/or quality of experience (QoE) from user and/or application perspectives. In addition, QoS/QoE in the Future Networks is expected to be aware of context, e.g., location.

10.11.2 MANAGEABILITY

The Future Networks will become more and more complex with emerging services and architectural diversity. Therefore, Instant and easy management is desired in the Future Networks. Resource availability is one of the important things to be managed in terms of economic incentives in Future Networks.

10.11.3 CUSTOMIZABILITY

Future Networks should be customizable along with diverse requirements and/or preferences of each user.

10.11.4 AAA AND SECURITY

Future Networks should be built on the premise of AAA (Authentication, Authorization, and Accounting) and security to provide economic incentives.

11. MILESTONE FOR STANDARDIZATION ON FUTURE NETWORKS

This clause describes a set of promising work items of standardization on Future Networks.

EdNote : The details are not fully discussed yet. Further discussion and revision are required based on this initial input.

11.1 OVERALL WORK PLAN

This Technical Report has described the problem statement and requirements for Future Networks (FN). From the discussion on FN, a set of requirements and design considerations have been derived for further progressing of standardization on FN.

Based on these results, the design of FN architecture and the development of specific protocols need to be progressed as the future work items, as shown in the following figure.

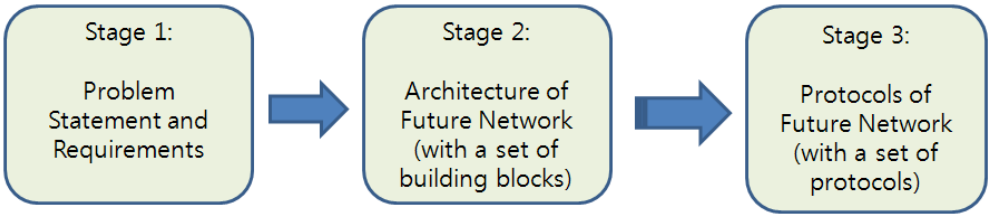


Figure – Overall milestone of standardization on FN

In Stage 1, in this TR, a set of requirements and considerations are identified for design of the FN architecture. In Stag 2, the FN architecture will be designed. The design of FN architecture can be done with a set of architectural building block (BB) components for overall FN architecture. This is because the FN architecture contains a wide variety of technical issues to be considered such as services/application, identification, naming/addressing, mobility control, QoS, security, and network virtualization, migration from the current network to FN. With this building block approach, a set of the BB architectures will result in the overall FN architecture. From the FN architecture, in Stage 3, one or more specific protocols of FN might be developed. Details of the protocols for FN to be developed are still for further study.

11.2 ARCHITECTURES OF FUTURE NETWORK

The FN architecture will be design with a set of component architectures as building blocks (BBs). These BBs may include the following architectural components, but not enumerative:

- ✧ Services/Network Model, including the Identification issues such as Naming and Addressing
- ✧ Functional Reference Architecture
- ✧ Mobility Control
- ✧ Security
- ✧ QoS
- ✧ Network virtualization
- ✧ New layered architecture (e.g., cross-layer communication architecture)
- ✧ Migration to FN

Some more additional BBs could be considered, if necessary. These architectural BBs will construct the overall FN architecture, as illustrated in the following figure.

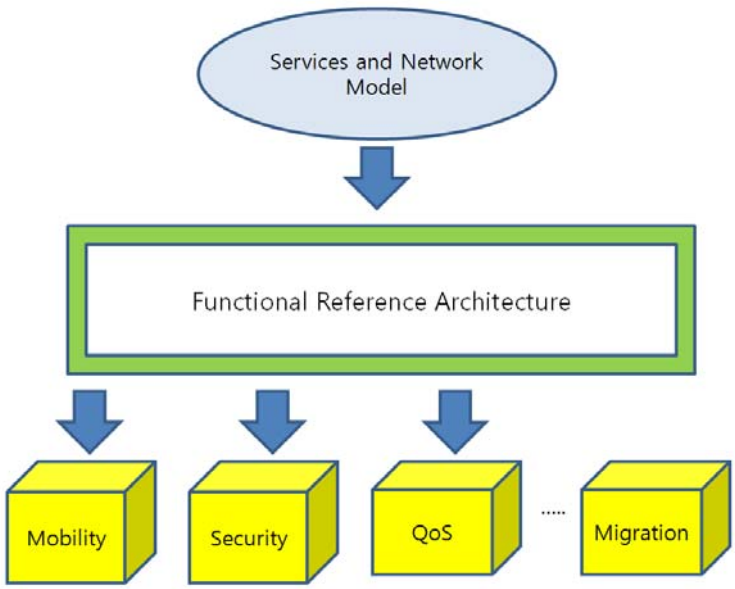


Figure 4 – Building blocks components for FN architecture

As shown in the figure, the Services and Identification BBs will be used as substantial inputs to design the generic Functional Reference Architecture (FRA) BB. Based on the FRA BB, the following specific functional BBs could be designed: mobility, security, QoS, and migration to FN, and more additional BBs. For the standardization process, each of the BBs will be made as a part of the overall FN architecture as follows:

- ✧ Services and Network Model;
- ✧ Functional Reference Architecture;
- ✧ Mobility Control;
- ✧ Security;
- ✧ Quality of Services;
- ✧ Network virtualization;
- ✧ New Layered Architecture
- ✧ Naming and addressing
- ✧ Routing
- ✧ Migration to Future Network

Some more parts (BBs) may be added to the above list, depending on further progress.

11.2.1 FN ARCHITECTURE: SERVICES AND NETWORK MODEL

As a basic architecture, the services and network model for FN should be identified. This work needs to address the following issues:

- ✧ Services, including some set of target services and killer applications, to be provided in the FN environment;
- ✧ Network model to be considered for design of FN architecture, which will include the fixe/wireless access network, core/backbone network, interworking between access networks and core networks;
- ✧ Abstract protocol stack in the layered architecture, as shown in the TCP/IP Internet protocol stack;
- ✧ Identification of users, devices, services in the FN, in which a variety of naming, addressing and numbering schemes will be investigated in the viewpoint of FN;

11.2.2 FN ARCHITECTURE: FUNCTIONAL REFERENCE ARCHITECTURE

The FRA BB will be the core part of the FN architecture. The details of functionality required for FN should be identified, and the relationship or interworking between the FN functions should be described. The routing/switching schemes or principles for FN should also be examined. This work needs to address the following issues:

- ✧ Functionality required for FN, such as routing, mobility control, QoS, security, etc;
- ✧ Concrete Protocol Stack that contains the protocols of FN in the layered architecture, as illustrated in the TCP/IP protocol stack;
- ✧ FN Routing principles and schemes, which include the routing between FN routers, the relationship between optical switching and routing, and the end-to-end data delivery model using the routing and switching, and so on;
- ✧ Relationship between user data transport plane and control plane.

11.2.3 FN ARCHITECTURE: MOBILITY CONTROL

This BB should provide the architecture of mobility control for FN. This work needs to address the following issues:

- ✧ Mobility control framework in FN;
- ✧ Location management of mobile users;
- ✧ Seamless handover support for mobile users;
- ✧ Separation of user identifier from network locator;
- ✧ Separation of user data transport function from mobility control function;
- ✧ Context-awareness;
- ✧ Multi-homing and vertical handover support;
- ✧ Heterogeneity of wireless and fixed access networks.

11.2.4 FN ARCHITECTURE: SECURITY

This BB should address how to provide the security for FN users, which may include the investigation of a wide variety of legacy security schemes to FN.

11.2.5 FN ARCHITECTURE: QUALITY OF SERVICES

This BB should address how to provide the QoS for FN services and users, which may contain the investigation of a wide variety of legacy QoS provisioning schemes to FN, including the QoS signalling and network resource reservation schemes.

11.2.6 FN ARCHITECTURE: NETWORK VIRTUALIZATION

TBD

11.2.7 FN ARCHITECTURE: NEW LAYERED ARCHITECTURE

TBD

11.2.8 FN ARCHITECTURE: (FUTURE) ROUTING

TBD

11.2.9 FN ARCHITECTURE: MIGRATION TO FUTURE NETWORK

This BB should describe the issues on how to migrate to the FN from the current network in the service and network point of view. This work needs to address the following issues:

- ✧ Issue on transition to FN services and networks;
- ✧ Building up a single shared infrastructure for FN;

- ✧ Deploying unconventional network architectures;
- ✧ Deploying new emerging technologies.

11.3 PROTOCOLS FOR FUTURE NETWORKS

As the next phase, a set of specific protocols should be developed based on the designed architecture of FN. This work should be done as a new project in the JTC1/SC6.

The final list of the FN protocols required may depend on the FN architecture, but, at this moment the promising set of protocols include the followings:

- ✧ Protocols for routing and switching the data and control packets in the FN (c.f., IP);
- ✧ Interworking of the routing/switching protocols with the heterogeneous underlying access technologies;
- ✧ End-to-end transmission protocols for user data processing and control (c.f., TCP and UDP);
- ✧ Application-specific protocols.

ANNEX A. GAP ANALYSIS

EdNote : Revision is required. The details are not reviewed yet. For improvement, ITU-T, IETF expert review is also required.

This Annex A discusses a gap between design goals and main characteristics for existing standards and/or proposals for next-generation or new generation and the Future Networks [19,20].

Corresponding technologies and architecture for gap analysis :

- ITU-T NGN (Next Generation Network)
- IETF IPv6 (Internet Protocol version 6, Next generation Internet)

2.1 NGN vs. Future Networks (FN)

As universal high speed Internet access has spurred the growth of e-life applications, it has raised the necessary of NGN (Next Generation Network) which will lead the world all-IP based.

The concept of an NGN has been introduced to take into consideration the new realities in the telecommunications industry, characterized by factors such as: competition among operators due to ongoing deregulation of markets, explosion of digital traffic, e.g., increasing use of "the Internet", increasing demand for new multimedia services, increasing demand for a general mobility, convergence of networks and services, etc.

ITU-T has been making effort to develop NGN, and it published quite important deliverables on NGN which describe requirements and necessary functions. NGN Release 1 and the ongoing Release 2 work cover broad area of technologies including inter-network, inter-operate with non-NGN networks, transport connectivity, media resource management, Quality of Service, security, network management, open service environment, multimedia subsystem, account and billing, etc. It will be provided to connect all legacy networks into NGN and support seamless services for e-life applications.

The NGN can be further defined by the following fundamental characteristics. The characteristics could be compared to design goals of Future Networks.

- Packet-based transfer
- Separation of control functions among bearer capabilities, call/session, and application/ service;
- Decoupling of service provision from transport, and provision of open interfaces;
- Support for a wide range of services, applications and mechanisms based on service building blocks (including real time/ streaming/ non-real time and multimedia services)
- Broadband capabilities with end-to-end QoS (Quality of Service)
- Inter-working with legacy networks via open interfaces
- Generalized mobility
- Unrestricted access by users to different service providers
- A variety of identification schemes
- Unified service characteristics for the same service as perceived by the user;
- Converged services between fixed/mobile
- Independence of service-related functions from underlying transport technologies;
- Support of multiple last mile technologies;

- Compliant with all regulatory requirements, for example concerning emergency communications, security, privacy, lawful interception, etc.

If we compare the list of Future Networks design goals (and general requirements) with NGN characteristics, we note that these are very similar with each other, and these can be considered as those of major futuristic challenges on the network of the future.

The major differences are that any IP-based network architecture or packet switching technology is not assumed for Future Networks, whereas NGN is based on all-IP networks and packet-based transfer. Also, NGN research is based on short/mid term evolutionary approach, so NGN technologies could be evolved from the current IP-based network. But Future Networks is based on clean-slate designs and long-term revolutionary approach.

A major goal of the NGN is to facilitate convergence of networks and convergence of services. Thus, NGN is not totally a new network, but all-IP converged networks. Instead, Future Networks researchers believe that it is impossible to resolve the new characteristics (or requirements) facing today's IP technology without re-design the fundamental assumptions.

Table 1 shows the review results on gap analysis of NGN and Future Networks from perspective on design method, fundamental characteristics, and deployment aspect.

Table 1. NGN vs. Future Networks

		NGN	Future Networks
Design Methods		Incremental (backward-compatible) design	Clean-slate design
Fundamental Characteristics	Transport Method	Packet-based transfer	Not assume any packet or circuit transfer
	Layering and API	Concrete layered architecture and open interface	Cross-layered architecture
	Control Plane	Separation of control functions	New control plane (separated from data)
	End-to-end principle	Not strict	New principle required e.g., End-Middle-End principle
	Scalability	A variety of ID schemes support including IPv4 and IPv6	New ID, ID/locator split and multi-level locator
	Security	Layered security (e.g., L2 security, L3-IPsec, etc.)	Not clear yet
	Mobility	Generalized mobility (e.g., MIP)	Cross-layer design based mobility management
	QoS	Broadband capabilities with end-to-end QoS	Not clear yet
	Heterogeneity	Support for a wide range of medium, and services	Application/Service, Heterogeneity, Physical Media Heterogeneity
	Robustness	Management plane	Manageability, Autonomic management
	Network Virtualization	None	Re-configurability Programmable Network
	New Services and technologies Support	Support of multiple last mile technologies	Easy support of new service e.g., Data-centric, Context-awareness
	Economics	Limited	New parameters
Deployment Aspect		Incremental migration, Integration	New testbed and infrastructure required

In the meantime, some questions about the current network have been issued. It has started from the agony of today's Internet, which shows some of unintended consequences;

- Is it right way to keep the current role of Internet address which delivers who you are, where you are, and how the packets should be delivered?;
- Is the current address mechanism bringing the big challenge of mobility support?
- Is spam a necessary outcome of the Internet mail delivery?;
- Why the identification and trust of end peers become a challenge?
- Why has Quality of Service proved to be a commercial failure?;
- Is the host-oriented internet able to smoothly cover data-oriented usage of current Internet?;
- etc.

It is believed that the NGN is being designed to support seamless mobility, strong security, QoS, etc., which includes those issues. It is, however, not clear yet if they were unavoidable, and if NGN do not hand over the problems. Thus, it is necessary to study to find the answers and gives the input to design beyond NGN or other futures.

At this phase, current various IP based networks including Internet have significant deficiencies that need to be solved before it can become a unified global communication infrastructure. Further, concerns are drastically increasing now that shortcomings would not be resolved by the conventional incremental and 'backward-compatible' style of current research and standardization efforts. That is why the Future Network research effort is called as "Clean-Slate Design for the Internet's Architecture".

[Editor's Note] Further contributions are invited.

2.2 IPv6 (Next generation Internet) vs. Future Networks

IPv6 is the next generation Internet Protocol (IP) proposed as a successor of current IPv4. One important key to a successful IPv6 transition is the compatibility with the large installed base of IPv4 hosts and routers.

The requirements and design goals for IPv6 was as follows

- Number of addresses
- Efficiency in routers low and very high bandwidth (100G/bytes++)
- Security
- Mobility
- Auto-configuration
- Seamless transition
  - Don't require a day X for switching to IPv6
  - No need to change hardware

As seen above, IPv6 was designed to supplement the current IP, IPv4, so, main goal of IPv4 was to inherit the current IP characteristics. Thus, when we consider deployment and migration from current IPv4, IPv6 might be better approach for the network of the future. Some researcher is considering IPv6 as one of proposed solutions for the Future Networks. However, IPv6 has the same limitation like IPv4, IPv6 cannot fulfil all the requirements for the Future Networks.

If we compare the list of Future Network design goals (and general requirements) with IPv6 characteristics, we note that these are very similar in some point, but many other new requirements are still missed in IPv6, for examples,

Heterogeneity, Re-configurability, Context-awareness, Data-centric, Virtualization, Economics. Actually, these kinds of new requirement cannot be resolved without any new trial of re-design.

Table 2 shows the review on gap analysis of IPv6 (Next generation Internet) and Future Networks from perspective on design method, Fundamental Characteristics, and deployment aspect.

Table 2. IPv6 vs. Future Networks

		IPv6	Future Networks
Design Methods		Incremental (backward-compatible) design	Clean-slate design
Fundamental Characteristics	Transport Method	Packet-based transfer	Not assume any packet or circuit transfer
	Layering and API	Concrete layered architecture and open interface	Cross-layered architecture
	Control Plane	Not separated from data	New control plane (separated from data)
	End-to-end principle	Strict principle	New principle required e.g., End-Middle-End principle
	Scalability	Problems with scalable routing and addressing	New ID, ID/locator split and multi-level locatord
	Security	IPsec for IPv6	Not clear yet
	Mobility	MIPv6	Cross-layer design based mobility management
	QoS	Not support within IP	Not clear yet
	Heterogeneity	Problems with support for a wide range of medium, and services	Application/Service, Heterogeneity, Physical Media Heterogeneity
	Robustness	Fault-tolerant	Manageability, Autonomic management
	Network Virtualization	None	Re-configurability, Programmable Network
	New Services and technologies Support	Not easy support of new service	Easy support of new service e.g., Data-centric, Context-awareness
	Economics	None	New parameters
Deployment Aspect		Incremental migration, Integration	New testbed and infrastructure required

[Editor's Note] Further contributions are invited.

BIBLIOGRAPHY

[1] J. Hwang, M. Shin, S. Jeong, “Definition of Future Network” in Proc. ITU-T SG13 Geneva Meeting, January 2009.

[2] A. Feldmann, “Internet Clean-Slate Design : What and Why ?,” ACM SIGCOMM Computer Communication Review, Vol. 37, No. 3., pp 59-64, 2007.

[3] Standford Univ, “Clean Slate Designs for the Internet, “http://cleanslate.stanford.edu.

[4] ITU-T sancho (ITU-T Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented database), http://www.itu.int/sancho/

[5] Wikipedia, http://www.wikipedia.com

[6] ITU-T recommendation Y.2001 (12/2004), General overview of NGN

[7] Stanford Univ., The Clean-slate Design for the Internet, http://cleanslate.stanford.edu/

[8] Network Virtualization : a strategy for de-ossifying the internet, http://www.arl.wustl.edu/netv/main.html

[9] M-K. Shin et al., “Future Network : Problem Statement,” in Proc. ITU-T NGN-GSI Seoul Meeting, January 2008.

[10] M-K. Shin et al., “Problem Statement for Future Network :,” in Proc. ISO/IEC JTC1 SC6 Geneva Meeting, 2008.

[11] E. Paik et al., “Future Network : General Requirements and Design Goals,”, ” in Proc. ITU-T NGN-GSI Seoul Meeting, January 2008.

[12] E. Paik et al., General Requirements and Design Goals for Future Network in Proc. ISO/IEC JTC1 SC6 Geneva Meeting, 2008.

[13] T. Anderson et al, “Overcoming the Internet Impasse through Virtualization,” IEEE Computer, 2005.

[14] J. Hwang, “Future Network services,” in Proc. ITU-T SG13 Geneva Meeting, January 2009.

[15] GENI Research Plan GDD-06-28 Version 4.5 of April 23, 2007

[16] New Generation Network Architecture AKARI Conceptual Design (ver1.1), http://akari-project.nict.go.jp/eng/index2.htm, October 2008

[17] The future Internet: the operator’s vision,’ Eurescom P1657, EDIN 0546-1657, 2007.11

[18] Man-Sze Li, ‘Internet of Services,’ Korea-EU Forum, 2008

[19] M-K. Shin et al., “Future Network : Gap Analysis,” in Proc. ITU-T NGN-GSI Seoul Meeting, 2008.

[20] M-K. Shin et al., “Gap Analysis for Future Network :,” in Proc. ISO/IEC JTC1 SC6 Geneva Meeting, 2008,

[21] ITU-T Recommendation Y.2011 (2004), General principles and general reference model for Next Generation Networks.

[22] ITU-T Recommendation Y.2601 (2006), Fundamental characteristics and requirements of future packet-based networks.

[23] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, December 1998.

[24] Internet Engineering Task Force (IETF), http://www.ietf.org

[25] Internet Research Task Force (IRTF), http://www.irtf.org.

[26] T. Koponen et al., “A data-oriented (and beyond) network architecture,” In Proc. of ACM SIGCOMM 07, 2007.

[27] MIT Media Lab, Viral Communications, http://dl.media.mit.edu/viral/.

[28] Future Internet of Creative Media. Report of a workshop organized by the Networked Media Systems Unit of the Information Society and Media , Directorate General of the European Commission. January, 2008.

[29] Future Internet and NGN Design requirements and principles for a Future Media and 3D Internet. Created by "Future Media and 3D Internet Task Force". Coordinated and supported by the Networked Media Unit of the DG Information Society and Media of the European Commission. Feb 2009.