Requirements For Future Internet Architecture

(draft-FIA-Requirements-r.0.6.0)

October 2011

Editor: TaeWan You, ETRI {twyou _at_ etri.re.kr}

Summary

This document describes fundamental requirements and principles for Future Internet Architecture (FIA) developed by Architecture Working Group (AWG) of Future Internet Forum (FIF). This document includes various requirements and design principles for FIA from several technical perspectives. Also, general requirements and principles are developed based on them. Finally, the document provides the recommendation for Future Internet Research.

Contributors

Name	Affiliation	Contact	Contributions
Woojik Chun	ETRI	wjchun_at_etri.re.kr	Requirements and Principles
SeokJoo Koh	KNU	sjkoh_at_knu.ac.kr	Technical Requirements – Mobile perspective
MyeongWuk Jang	SAIT	myeong.jang_at_samsung.com	Technical Requirements – Content-centric perspective
TaeKyoung Kwon	SNU	tkkwon_at_snu.ac.kr	Technical Requirements – Mapping system perspective
SangJin Jeong	ETRI	sjjeong_at_etri.re.kr	Technical Requirements – Green networking perspective
SangWoo Lee	ETRI	ttomlee_at_etri.re.kr	Technical Requirements – Security perspective
HeeYoung Jung	ETRI	hyjung_at_etri.re.kr	Overall

TABLE OF CONTENTS

[Editor's Note: the document is still in draft version, so many parts of texts are tentative. whole texts may be revised by further contributions]

1. INTRODUCTION

The Internet has been working for longer than 40 years successfully without major change of the architecture. However, the great success of the Internet has faced many challenges including technical and non-technical issues. Network links became almost a million times faster than earlier and wireless are more common technology of the Internet. Moreover, small devices including sensor are getting smarter and expected to be connected to the Internet, so that we can anticipate that the number of Internet connected nodes is growth to more than 50 billion at 2020 [1-1]. Meanwhile, new applications and services were emerged by responding to users' new demands. Also various commercial stakeholders appeared in the Internet, such as Internet Service Provider (ISP) and Content Provider (CP) as well as Telecommunication Corporation (telco). It is generally recognized that current Internet architecture cannot meet these challenges by patching solutions anymore and has faced threatened by shortcomings in terms of security, performance, reliability, and scalability. With this challenging environment, the researches on new Internet architecture are becoming world-widely popular in the name of Future Internet.

FIF AWG believes that the first step to develop Future Internet Architecture (FIA) should be the establishment of appropriate requirements and/or principles. In the context, FIF AWG develops the requirements and principles for the design of FIA by considering various technical perspectives.

This document describes the requirements and principles for the Future Internet Architecture. The document composes three parts. Firstly, the document addresses technical requirements and principles by gathering various requirements from specific technical perspectives. Secondly, general requirements and principles for FIA are drawn by extracting some common features from these technical requirements and principles. Finally the document will suggest some recommendations for the research on FIA.

1.1 Scope

The scope of this document includes the following items:

- Collect various requirements and principles from several technical perspectives.

- Identify general requirements and principles based on considering the collected requirements and principles.
- Provide the recommendation for FIA Research

2. DEFINITIONS AND ABBREVIATIONS

2.1 Terms and Definitions

2.1.1 ARCHITECTURE

It is a set of functions, states, and objects/information together with their behaviour, structure, composition, relationships and spatial-temporal distribution. The specification of the associated functional, object/informational and state models leads to an architectural model comprising a set of components (i.e. procedures, data structures, state machines) and the characterization of their interactions (i.e. messages, calls, events, etc.) [ref: FIArch 2011]

2.1.2 REQUIREMENT

It is a specific need that any stakeholders of the Future Internet wish to achieve. The terms such as Objectives and goals will be used interchangeably in this document.

2.1.3 PRINCIPLES

It suggests normative rules on how a designer/an architect can best structure the various architectural components and describes the fundamental and time invariant laws underlying the working of an engineered artefact.

2.1.4 FRAMEWORK

It provides a conceptual model of the architecture which is defined under the guideline of the principles

2.2 Abbreviation and acronyms

AWG	FIF Architecture Working Group
FIF	Future Internet Forum in Korea
FIA	Future Internet Architecture

3. REQUIREMENTS AND PRINCIPLES

[Editor's Note: The clause contains tentative contexts, the whole parts of text may be revised by further contributions]

The goal of the original Internet architecture was to develop an effective technique for multiplexed utilization of existing interconnected networks. Along with this fundamental goal several detailed requirements as follows are specified in [3-1]:

1) Internet communication must continue despite loss of networks or gateways.

2) The Internet must support multiple types of communications service.

3) The Internet architecture must accommodate variety of networks.

4) The Internet architecture must permit distributed management of its resources.

5) The Internet architecture must be cost effective.

6) The Internet architecture must permit host attachment with a low level of effort.

7) The resources used in the internet architecture must be accountable.

The list above seems to be just a wish list of general networks. Note that the requirements can be satisfied neither at the same time nor with the same significance. The selection and priority of requirements would result in totally different architecture.

Based on the requirements, the current Internet architecture was designed by principles as follows [3-2]:

1) The layering,

2) Packet switching,

3) A network of collaborating networks,

4) Intelligent end-systems as well as the end-to-end argument.

These principles are suitable for static and well-managed flat network topology. As the Internet evolved from a small research network to a worldwide information network, a growing diversity of commercial, social, ethnic, and governmental interests led to increasingly conflicting requirements among the competing stakeholders. This chapter describes general requirements and principles for the Future Internet.

3.1 General Requirements

The clause describes general requirements that FIA should be considered to have fundamental capabilities redefining from the current Internet design objectives.

Diverse requirements are arisen with respect to new applications and technologies. The requirements generally applicable to the Future Internet would be classified in 6 categories

3.1.1 SCALABLE

Many limitations of the current Internet are originated by excessive growth of the Internet in terms of bandwidth, number of hosts and users, and volume of contents. The well-known "IPv4 address deficiency problem" is a typical example of the scalability issues. As the Internet grows in the number of users and its application area, the scalability issue becomes more serious. The future Internet has to be flexible enough to cope with potential growth of the number of users, contents, services, and devices as well as explosive growth of traffic.

3.1.2 SEAMLESS

The Future Internet pursues integration of not only traditional wired and wireless networks, but also various new types of networks such as sensor, service and content aware, social networks. The Future Internet has to provide consistent access mechanism to diverse networks, communication paths on the different administration domains, mobility through even heterogeneous networks.

- **Mobility**: If an IP host is mobile, its IP address will be broken whenever it switches to a new IP subnet. The FI should support the mobility of IP hosts without breaking end-to-end connectivity.

  - Provision of mobility functionality in the built-in fashion
  - Support of Multi-homing hosts
  - Support of heterogeneous wireless networks
  - Support of unreliable wireless links
  - Support of network, service, and personal mobility

- **Distribution of processing, storage, and control functionality and autonomy** (organic deployment): Addressed by current architecture (concerning storage and processing several architectural enhancements might be required e.g. for the integration of distributed but heterogeneous data and processes).

[Editor's Note: the above description is still controversial]

- **Transparency** (the terminal/host is only concerned with the end-to-end service, in the current Internet): This service is the connectivity even if the notion of "service" is not embedded in the architectural model of the Internet

3.1.3 SENSITIVE

Since the current internet has the narrow waist model where all applications are running on the IP and IP is working on various transmission media, it provides the same functionalities regardless of requirements of specific applications. This results in the fundamental limitation on delivering real-time traffic and context sensitive contents. In the Future Internet, the services have to be differentiated according to application's requirements, communication status, and user preferences. Service differentiation means "content-aware" that discriminates traffic based on the content, "context-aware" that selects the suitable communication services based on situation and preferences, and "reality-aware" that optimizes the communication services by sensing the environments.

- **Genericity** (e.g. support multiple data traffic such as non/real-time streams, messages, etc., independently of the shared infrastructure partitioning/divisions, independently of the host/terminal): Addressed and to be reinforced (migration of mobile network to IPv6 Internet, IPTV moving to Internet TV, etc.) otherwise leading to segmentation and specialization per application/service.

[Editor's Note: More shortages of current Internet will be included, such as QoS]

3.1.4 SECURE

One of the fatal problems in the current Internet is lack of security features. For strengthening the security capability some encryption mechanisms, such as IPsec and sHTTP, are patched. However, those can only protect content privacy but cannot solve network related security issues such as DDoS (Distributed Denial of Services). Thus, security must be considered form the early stage of the Future Internet architecture design. Since how secure communications must be kept is dependent on the how much they trust peers and communication environment, security and trustworthy are two sides of the same coin in the Future Internet design.

- **Accountability** (of resource usage and security without impeding user privacy, utility and self-arbitration)

- **Reliability** refers here to the capacity of the Internet to perform in accordance to what it is expected to deliver to the end-user/hosts while coping with a growing number of users with increasing heterogeneity in applicative communication needs.

- **Robustness/stability, resiliency, and survivability**: Security and Trustworthy: The works on this requirement will be discussed in Security WG

3.1.5 SMART

[Editor's Note: Both title of sub-clause and below text is still controversial, it may be revised by further contributions]

One of the well-known principles of the current Internet is the "end-to-end" principle, where most of intelligent functions have to be deployed in end systems while keeping networks as simple and dummy as possible. This principle has contributed for graceful evolution of the Internet. However, diverge and differentiated applications of the Future Internet would require much sophisticated management over the communication infra. That is, a network itself should perform its role intelligently by classifying the traffics, prioritizing requirements, and allocating resources, and also it must be equipped with advanced management capability such as self-configure, self-healing, self-adjust, etc.

Smart network means autonomous distributed networking technology that enables the automatic construction of a network without any settings. It is capable of auto restoration in the event of a failure and adapts to changes in the surrounding network environment.

- **Manageability** (distributed, automated, and autonomic operation)

- **Autonomous**

- **Diagnosability** (root cause detection and analysis)

3.1.6 SUSTAINABLE

The primary reason why the Future Internet must be considered in the clean-slate manner is that the original principles of the current internet can no more satisfy newly arisen requirements. So the architecture for the Future Internet must be flexible enough to fulfil the requirements to be appeared as well as already identified. Also, it must be evolvable to accept new technologies and applications without interference among existing services. One step further, systems for the Future Internet must be developed by green technology for resource reuse and energy saving.

- **Flexibility** (capacity to adapt/react in a timely and cost-effective manner when internal or external events occur that affect its value delivery) and Evolutivity (of time variant components)

- **Evolvability** (of time variant components)

[Editor's Note: specific description will be needed to clarify differentiation between revolution and revolution concept for Future Internet Architecture]

- **Energy efficiency**: there is increasing demand for improving energy efficiency of network and reducing the energy consumption and greenhouse gas emissions. In order to meet the demand, Future Internet architecture should provide a way to reduce energy required to carry out a given task while maintaining the same level of performance.

3.2 Architectural Principles

[Editor's Note: The whole parts of text are still tentative, it may be revised by further contributions]

This clause describes desirable architectural principles for designing FIA based on various general requirements. Following principles are recommended to design FIA.

3.2.1 KEEP IT AS SIMPLE AS PASSIBLE

The KISP (Keep It as Simple as Possible) principle is based on the famous quote by Albert Einstein: "Make everything as simple as possible, but not simpler". Complex problems sometimes require complex solutions and the FI will be providing non-trivial functionality in many respects.

However, designers should keep in mind this principle and prefer relatively simpler and more elegant solutions over over-engineered designs. Complex systems are generally more difficult to manage and less reliable since more things can go wrong at any given time. Therefore, complexity should always be added for a good reason. Per the Ockham's razor principle, all things being equal, the simpler solution is the best. This has been one of the guiding principles of the current Internet and should continue to be taken into account when designing the FI.

- **Simplicity and cost-effectiveness**: more data is needed but simplicity seems to be progressively decreasing. Note that simplicity is explicitly added as design objective to -at least- prevent further deterioration of the complexity of current architecture (following the "Occam's razor principle" key design principle). Indeed, lowering complexity for the same level of performance and functionality at a given cost is key objective.
- **Globally Unique ID**

3.2.2 POLYMORPHIC NETWORKS

[Editor's Note: The sub-clause is still controversial, further contribution will be needed to clarify]

- **Heterogeneous networks**
- **Network virtualization**
- **Support of heterogeneous wireless networks**

3.2.3 DESIGN FOR TUSSLE

This design principle states that the Future Internet should not be engineered to favour one particular Internet stakeholder over another. The FI should be capable of supporting flexible business models where multiple stakeholders can participate in an open environment that supports and encourages innovation and participation without barriers. Open architectures and protocols will enable increased competition between providers (including network, service and application providers) increasing quality and value to the benefit of all. Individuals should be able to produce as well as consume content; innovators, both small and large, should be able to introduce new products, new technologies and even new communication paradigms without the hindrance of conformity to established or traditional business models. The FI should support a greater participation of individuals, communities and small businesses alongside larger and more established organizations and the FI should enable all providers of content, services or other forms of added value to receive appropriate compensation for their contribution.

3.2.4 MODULAR APPROACH

[Editor's Note: The sub-clause is still controversial, further contribution will be needed to clarify]

- **Decompose**
- **Recursion**
- **Vertical and/or Horizontal Layering**
- **Separation of Identifier and Locator**
- **Separation of control plane and data plane**

3.2.5 INTRINSICALLY SECURE

- **Self-certifying ID**

3.2.6 ENVIRONMENTAL AWARENESS

Future Internet architecture needs to be environmentally designed so that the architecture design, resulting implementation and operation of Future Internet can minimize their environmental impact, such as the consumption of materials and energy and reducing greenhouse gas emissions [3-3].

3.2.7 EVOLUTIONAL DEPLOYMENT

[Editor's Note: The whole parts of text are still tentative, it may be revised by further contributions]

The FI must be designed as a sustainable network being flexible enough to continuously evolve, develop and extend in response to changing societal requirements. Adopting such a sustainable design will allow for environmental and societal developments over many decades, making the FI able to support universal communication that will overcome the obstacles of language, culture, distance, or physical ability which exist in the current Internet (CI). The sustainability of the FI will rely on its ability to be scalable, available and reliable in a resource- and cost efficient manner. The latter means that the FI should be able to serve a very large number of entities (scalability), maintaining its usable operation ratio (availability) and can easily recover if faults occur (reliability). Finally, the FI should be able to provide openness to users to facilitate the creation of new applications along with the ability for multiple entities, which are implemented according to certain common rules, to communicate with each other (interoperability).

- **Network entities must be able to evolve**
  - New network entity should be supported
  - Adding new network entity incrementally

4. TECHNICAL PERSPECTIVES

This clause describes specific requirements and technical principles to make realization of Future Internet Architecture (FIA) from specific technical perspectives.

4.1 Mobile perspective

4.1.1 SPECIFIC REQUIREMENTS

To effectively support the mobility in Future Internet, the following specific requirements should be considered in the design of Future Internet architecture.

4.1.1.1 PROVISION OF MOBILITY FUNCTIONALITY IN THE BUILT-IN FASHION

It is envisioned that mobile users now become the key driver toward future Internet with explosive growth of the number of subscribers of 2G/3G cellular systems and other wireless data systems, and that there will be much more mobile/wireless users than wired ones. However, it is noted that the current Internet was originally designed for fixed hosts, rather than for mobile ones, which has enforced to develop the extensional features to Internet, in the patched-on fashion, in order to support the mobile environments, as shown in the examples of Mobile IP (MIP). However, such patched-on approach seems to be just a temporal heuristic rather than a sustainable solution to the mobility issues to future Internet.

Accordingly, the mobility functionality should be provided in the design of Future Internet in the built-in fashion rather than in the patched-on way.

4.1.1.2 Provision of Location Management and Handover Control

To support the mobility functionality, the Future Internet should be designed to provide the location management and handover control.

The location management function is used to keep track of the movement of a user in the network and to locate the user for data delivery. It is noted that the location management function is used for supporting the prospective 'incoming' call to the mobile user. The LM functionality includes the location registration/update and location query (for user data transport). The location registration/update function is to keep track of the current location of a user. The location query function is to locate the user for data communication.

The handover control function is used to provide the 'service continuity' for the 'on-going' session of the moving user by minimizing data loss and handover delay during handover. With the help of the handover control function, a mobile user can seamlessly continue the data communication during the session, even though it changes its location (or IP address) in the network.

4.1.1.3 Provision of Scalability to Mobility Control

Most of the mobility schemes in current Internet are based on a centralized mobility anchor, such as Home Agent (HA) of Mobile IP (MIP) or Local Mobility Anchor (LMA) of Proxy MIP (PMIP). The centralized control, however, tends to inject unnecessary data traffic to Internet core, and thus the data traffic explosion problem becomes more severe. Moreover, the centralized approach is vulnerable to a single point of failure or attack.

Accordingly, the scalability to mobility control should be provided in the design of Future Internet for effective mobility support and for avoiding the traffic explosions.

4.1.1.4 Support of Route Optimization

In the centralized mobility control of current Internet, the routing path through a centralized anchor tends to be longer, which results in non-optimal routes and performance degradation.

Accordingly, the route optimization in the mobility control should be provided in the design of Future Internet.

4.1.1.5 Support of Multi-homing Hosts

In the future Internet environment, it is expected that a host with multiple interfaces will be very common, in which the host may be connected to two or more wireless networks (e.g. wireless LAN or 3G wireless network, etc).

Accordingly, the Future Internet should be designed to effectively support the multi-homing hosts with multiple network interfaces.

4.1.1.6 Support of Heterogeneous Wireless Networks

The current Internet assumes a common IP protocol stack over all Internet nodes according to the famous hourglass model. However, networks environment will become more heterogeneous, which are ranged from simple lightweight networks to highly reliable networks. For instance, wireless networks are likely to have quite diverse characteristics from sensor networks to cellular networks. In the meantime, the backbone network is evolving to full optical network with very high bandwidth.

Accordingly, the future Internet should be designed to effectively support the network heterogeneity and diversity.

4.1.1.7 Support of Opportunistic Wireless Links

The current Internet was designed based on a stable connection between host and network. However, in mobile environment, the connection is subject to dynamics of the network, in particular, due to high error rates and intermittent connections, depending on characteristics of wireless links.

Accordingly, special considerations should be taken for lossless and reliable communications in such wireless network environments, as shown in the example of the Delay Tolerant Network (DTN).

4.1.1.8 Support of Idle/Sleep-mode Hosts

In current Internet, it is implicitly assumed that a host is always active so that it can receive the incoming packets at any time. However, it may not be true in a certain mobile/wireless environment. For instance, mobile hosts such as smart phone may be in idle, dormant or sleep mode frequently where they may not response immediately for incoming packets. This inactive condition of mobile hosts brings unacceptable packet loss. In addition, the power saving is the most essential requirement for mobile hosts. However, we note that the current Internet protocols have been designed without any special consideration on this issue.

Accordingly, the Future Internet should be designed to effectively support the idle/sleep mode hosts.

4.1.1.9 Support of Network Mobility

Future Internet is envisioned to include moving networks as well as moving terminals. Some of typical example platforms for moving networks could be bus, train, ship, air plane and so on. Such moving networks may require the seamless services.

Accordingly, the Future Internet should be designed to effectively support the network mobility, which is called 'network mobility'. This network mobility may require the different features from the host mobility.

4.1.1.10 Support of Service/Personal Mobility

In addition to the host and network mobility issues, the services mobility and the personal mobility need to be supported in the Future Internet environments. The services mobility can be applied for a specific service, i.e., the ability of a moving object to use the particular (subscribed) service irrespective of the location of the user and the terminal. The personal mobility represents the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

Accordingly, the Future Internet should be designed to effectively support the services mobility and the personal mobility.

4.1.2 **Technical Principles**

4.1.2.1 Separation of Identifier and Locator

In current Internet, an IP address has overloaded semantics as Identifier (ID) and Locator (LOC). In mobile environment, however, the location of mobile host is likely to continue to change by movement. This means that the static allocation of LOC (IP address) to a host may become problematic in mobile networks. In the meantime, the ID needs to be kept persistently (without change) to maintain an on-going sessions against movement of a host.

Accordingly, ID and LOC should be separated to support the mobility in future Internet. That is, an identifier should be used only to identify an object in the viewpoint of service provisioning, whereas a locator should be used so as to effectively locate the object and to deliver packets in the network.

Another critical concern is that IP address, as an ID, is allocated to a network interface of a host, rather the host itself. Accordingly, if a host has multiple interfaces, multiple IP addresses must be allocated to a single host. This may give serious inefficiency to a multi-homing host, since the same host has to use different IDs for communication. Therefore, ID needs to be allocated to a host itself rather than its network interface.

As for the allocation of LOC or IP address, it does not make sense to allocate IP address to a mobile host, since it may continue to move on. Accordingly, in mobile environments, it is suggested that an address or LOC should be allocated to a certain fixed node in the network, rather than the host itself.

4.1.2.2 ID-BASED GLOBAL COMMUNICATION AND LOC-BASED LOCAL DELIVERY

With host ID and network LOC, the ID-based global communication and LOC-based local delivery is considered for effective mobility control. That is, the end-to-end communication between two hosts will be performed only with their host IDs, whereas data packets will be delivered to an end host by using the associated network LOCs, possibly through one or more transit networks. Such LOCs may be local or private IP addresses, and each of transit networks may use different routing schemes within its domain.

For this purpose, each host has a globally unique ID, by which global communication is accomplished. In the meantime, various LOCs can be used for packet delivery in each network. Each LOC is used locally in the networks, without any assumption on global uniqueness of LOC.

In addition, in Future Internet, the protocols used for data delivery in access and backbone networks need to be separated. In future Internet environment, each access network and the backbone network may have quite different characteristics. For example, access networks might consist of the wireless links with relatively low bandwidth and unreliable transmissions, whereas the backbone network will be the optical network with high bandwidth to provide reliable transmissions. Accordingly, the protocol requirements for the access and backbone networks may be quite different. This implies that the protocols used in the access network need to be designed by considering the wireless link characteristics, whereas the protocols used in the backbone network may be designed to be as simple as possible by considering the optical networks.

The access networks should be able to guarantee easy access of users, whereas the backbone network is primarily purposed to provide effective delivery of packets. In this context, we need to separate the protocols used for access and backbone networks in the design of Future Internet. In particular, we also note that the current IPv4/v6 protocols may be used in the backbone network, as an incremental approach (or a tentative solution) to deployment of future Internet. This is because the backbone network is quite difficult to replace with a completely new protocol at a stretch, compared to the access network. This approach will also be helpful for migration from the current Internet to the clean-slate future Internet.

4.1.2.3 SEPARATION OF CONTROL PLANE AND DATA PLANE

In most of current Internet protocols, data delivery and control function are integrated and implemented at the same devices, and the data and control traffics are routed along the same path, as shown in the IP and ICMP protocols. The control information for signalling is mission-critical and thus needs to be delivered more urgently and more reliably, compared to normal user data. In this context, it is desired that the control functionality should be separated from the data transport functionality, as seen in the 3G or 4G wireless mobile communication systems.

4.1.2.4 DISTRIBUTED MOBILITY CONTROL

To effectively distribute the data traffic in the network, the future Internet shall be designed to provide a distributed mobility control. In the distributed mobility control, the route optimization will be intrinsically supported, and this can also mitigate the problem of a single point of failure to a local network. For this purpose, a centralized mobility anchor needs to be distributed to two or more locally distributed mobility anchors.

4.2 Content-centric perspective

4.2.1 SPECIFIC REQUIREMENTS

4.2.1.1 PROVISION OF USER-ORIENTED CONTENT NAMING SCHEME

Host addresses, such as IP addresses and MAC addresses, were introduced to connect devices and were used by computer experts, but the current Internet is mainly used by general users to access content. While a host address represents the location of a device, users are interested in content. Therefore, the addressing/naming scheme in networking should be changed from host addressing to content naming. Also, the content name should be easy to use by general users. Domain names are currently used for the similar purpose.

While a name in content-centric networking usually identifies a piece of content, a name can also represent multiple pieces of content (e.g., movies directed by Steven Spielberg), a person (e.g., talk with Steven Spielberg), or a group of people (e.g., chat with actors of Jurassic Park). etc. Multiple different names may represent the same content (e.g., the Jurassic Park movie, the Jurassic Park movie directed by Steven Spielberg, the dinosaur movie directed by Steven Spielberg, etc.). Therefore, a name or names in the future Internet should be able to identify any entity or a group of entities.

4.2.1.2 SUPPORT OF EFFICIENT CONTENT ACCESS

While the host address-based networking is an efficient way to send a packet to a device, it causes inefficiency when retrieving content. When the same content exists on multiple devices, the addressed host may not be the best device to access the content. If general users can access what content they want, it is not important for them where the content comes. Therefore, content should be transferred from the nearest host in the communication space. Also, when a device has multiple connectivities, such as WiFi, cellular, and Bluetooth, the best connectivity should be used to get content quickly. Network traffic is changing from time to time, and thus, networking path should also be changed to escape traffic congestion. That is, networking should dynamically adopt the given environment and its change to support efficient content access.

4.2.1.3 FAIR SUPPORT OF MASSIVE CONTENT DISTRIBUTION

A video on demand service, such as YouTube and NetFlix, and a real-time video transferring service, such as IPTV, are significantly increasing the traffic of the Internet. Especially, an explosive increase of users to access certain content, such as a big match in the World Cup game, during the short time period causes serious traffic congestion in networks closed to its content server. The CDN (Content Delivery Network) service can reduce the number of same packets over the same physical link using local servers. However, the CDN service does support personal content which is not located on servers registered to the service, even though the content is required by numerous users at the same time. Also, the shared links between a local server and multiple client devices deliver the same packets. Therefore, massive content distribution should be supported by networking nodes without external servers to reduce network traffic for any content either on a server or a personal device.

4.2.1.4 SECURE NETWORKING

Major requirements of secure networking have been described in Section 3.1.4 Secure.

In content-centric networking, a name is given to access content. This name does not mean the location of the content. The content may exist on multiple devices and/or routing nodes; the content is delivered from any device holding the content. In such a networking environment, sever protection and channel protection mechanisms cannot be enough to guarantee that the content is correct and secure. Therefore, the integrity of content should be provided with the signature of the content creator. Also, in order to allow only authorized/authenticated users to access content, the content should be encrypted with a security key.

4.2.2 TECHNICAL PRINCIPLES

4.2.2.1 HIERARCHICAL CONTENT NAMING

The size of a routing table in content-centric networking may be proportional to the number of content prefixes which are used to forward packets; as the number of content prefixes increases the size of the routing table also increases. It is assumed that the number of content prefixes will be larger than the number of devices. Thus, the size of FIB(Forwarding Information Base) table in content-centric networking will be larger than that of FIB in the current Internet. To effectively reduce the size of FIB, aggregation of names is necessary. Therefore, names should be hierarchically structured to support aggregation of content names.

4.2.2.2 DIRECT NAME-BASED PACKET FORWARDING

A domain name is easier for general users to identify a host than a host address. However, it introduces inefficiency in networking. Because the current packet forwarding nodes cannot directly handle domain names, a given domain name should be changed to an IP address through an external DNS (Domain Name System) server before delivering a packet to a destination device. Networks should directly process a name of content without the support of such external servers.

4.2.2.3 TIME-SHIFTED MULTICAST

To avoid transferring same packets over the same physical link, a packet forwarding node should know what packets the node delivers. By knowing the history of content requesting packets, the node can avoid to send the same content requesting packets to other devices. When the node receives the corresponding content, it will duplicate and send the content to the requesting devices. Also, if the node stores content being delivered on its cache, the node will send the stored content to devices that request the same content. It is called time-shifted multicast.

4.2.2.4 STRATEGY-BASED PACKET FORWARDING

When there are multiple candidates for networking, some of them may be used (e.g., multiple connectivities of a device, multiple paths from a content requesting device to a content providing device, multiple sources for same content, etc.). To select a candidate, various networking strategies may be applied: Select-All, Best-Fit, Round-Robin, etc. The future Internet should support various strategies to fit well user intention.

4.3 Mapping system perspective

The mapping system in the Future Internet may have to support a variety of mapping services. That is, when a user (or a host) sends a query with a key to the mapping system, it should reply with the value that corresponds to the given key. The current mapping system in the Internet is the DNS, which is host-oriented, and mainly used for mapping between domain names and their corresponding IP addresses. The DNS requires individual hosts to be connected to the global Internet, and potentially has the scalability issue. For instance, the popularity of .com implies that its registry operator (i.e. VeriSign) should handle a large amount of query traffic. Also, if it is used to provide the mapping between identifiers and locators of mobile hosts, it should be provisioned for dynamic updates of the entries.

4.3.1 SPECIFIC REQUIREMENTS

4.3.1.1 FLEXIBILITY

The mapping system may have to support a wide variety of key-value mapping. One of the crucial key-value mapping is the locator update of mobile hosts for mobility support. Also, to mitigate the routing scalability, the mapping of endpoint identifiers to their routing locators can be supported by the mapping system. Another potentially important usage is the mapping from content names (or content identifiers) to their locators, which is similar to trackers in BitTorrent systems. There may be other usages or requirements of the mapping system in the Future Internet. It should be able to be extended to support other naming or mapping functionality.

4.3.1.2 Availability/Resiliency

It should not have a single point of failure/bottleneck. According to some DNS measurements, a substantial portion of the DNS traffic is often lost. The workload on the servers in the mapping system should be balanced and distributed. Also, a failure of a single server or component in the mapping system may have to be recovered without noticeable disruption.

4.3.1.3 Response time

The mapping of key-value pairs may be replicated globally or locally. In this way the response from the mapping system may be returned to potential solicitors timely, so that the delay of resolution does not affect the applications and services.

4.3.1.4 Authenticity/Integrity

The mapping information of the key should be trustworthy. We may leverage the DNSSEC or Resource PKI. Whether this issue is handled in the AWG or security WG needs further discussions.

4.3.1.5 Absence of Global Connectivity

The mapping system may have to be able to operate even without its global connectivity. For instance, sensor networks, ad hoc networks, and delay tolerant network may operate individually without connectivity to the global Internet. The mapping system may need to support operations locally in an autonomic manner.

4.3.2 Technical Principles

4.3.2.1 Hierarchical or Flat Structures

One of the main principles that should be considered in designing a mapping system is that whether the main structure is hierarchical or flat. The DNS has the tree structure, which has the problem of a single point of failure/bottleneck. The weakness is augmented by adding redundant nodes (and links) to enhance resiliency (e.g. 100+ root server machines) and has been extended with high availability. If the mapping system has a tree structure, the lessons from the DNS operations should be taken into account. A flat structure, like distributed hash table (DHT) is also possible for a mapping system. Even though it is more resilient by nature, its performance issue (e.g. delay) should be solved. Some combination of tree and flat structures may be possible.

4.3.2.2 Caching Friendliness

The mapping system may have to be designed in the anticipation of caching the mapping data. That is, in-network nodes (say routers) or end-hosts may cache the value that corresponds to a key. The workload on the mapping system will be significantly mitigated, and the lookup delay will also be reduced.

4.3.2.3 Locality or Popularity

Not all the data in the mapping table will be equally accessed. For instance, in the cases of mobility, there is often the locality between the corresponding host and mobile host. If the mapping system provides the location of content files, there will be popular files and unpopular files. The mapping system can be efficiently or cost-effectively designed and operated if the disparity among the mapping data is exploited.

4.4 Green networking perspective

This subsection investigates Future Internet architectural requirements from the perspective of green networking or energy-efficient networking [4-1].

4.4.1 Specific Requirements

4.4.1.1 Improved Energy Efficiency in Network

Improving energy efficiency and reducing the greenhouse gas (GHG) emissions have become a global agenda recently. European Union (EU) has announced that EU will reduce the GHG emissions by 20 percent until 2020. Korean government also has declared the reduction of GHG emissions by 4 percent in compared with those of 2005 until 2020. It has been investigated that ICT industry emitted 2 percent of man-made GHG and consumed 4% of global electricity consumption in 2008, so efficient operations become important for reducing energy consumption in ICT industry. Therefore, Future Internet should be designed by considering the energy efficiency and energy consumption in network.

4.4.2 Technical Principles

4.4.2.1 Increased Energy Efficiency in Network Equipments

In order to increase the energy efficiency of network, the energy efficiency of network equipments should be initially considered. There are several methods to increase the energy efficiency of equipments, including network interface proxying, rate adaptive link control, etc. More specifically, network equipments need to support energy saving mode i.e., sleep mode, in order to reduce energy consumption and network interfaces should support energy management mechanisms such as adaptive link rate and sleeping mode. In addition to that, network equipments should have mechanisms allowing single pieces of equipment to go idle for some time, as transparently as possible for the rest of the networked devices. And, network equipments should have different energy consumption (or cost) profiles that a device may exhibit as a function of its utilization level. Also, from the hardware's point of view, network equipments need to utilize low power electronics for reduce energy consumption and efficient battery technology should be deployed in nodes in case of battery-powered equipments. Finally, in order to effectively control and manage the energy consumption in equipments, energy management functions should be deployed in network and equipments.

4.4.2.2 Increased Energy Efficiency in Networks

In order to achieve more improvement in energy efficiency, it is necessary to consider energy efficiency in network. First of all, energy efficiency should be considered during network planning and dimensioning. The planning includes how to replace electronic networks with more energy efficient networks such as optical networks and accomplish more reduction in energy consumption for data transfer. Also, network protocols used in network should be designed in order to establish a reliable connection but at the same time be energy efficient and these energy-aware network protocols should be used in not only core networks, but also access networks. Finally, optimized transmission and access methods such as advanced wireless channel management methods should be supported in wireless access networks.

4.5 Security perspective

4.5.1 Specific Requirements

To effectively support the security in Future Internet, the following specific requirements should be considered in the design of Future Internet architecture.

4.5.1.1 Malicious-Packet-Free Architecture

The various forms of malware such as botnets are emerging as the most serious threat against network security as they provide a distributed platform for several illegal activities such as launching distributed denial of service attacks against critical targets.

Accordingly, the Future Internet should be designed to effectively support that there are no malicious packets such as the data from a spoofed host in the network.

4.5.1.2 Built-In Security

The current Internet was originally designed for open and scalable network. This feature makes it possible to deploy the Internet very successfully. In particular, the Internet Protocol (IP) was designed to support ease of attachment of hosts to networks. However, this feature results in the lack of security. In particular, there is no inherent support in the IP layer to check whether a source is authorized or not. Therefore, security function was added into the original Internet as an additional or optional layer such as IPSec. However, this add-on solution cannot solve the problem fundamentally.

Accordingly, the Future Internet should be designed to support the security function intrinsically.

4.5.1.3 Traceability of Malicious Activity

When network security accident such as DDoS happens, the traceability of original attacker is required to cope with next accident and to claim responsibility for the attacks. Traceability of malicious activity means that the network should have the functionality on achieving location information or identifier of the malicious host or hacker.

Accordingly, the Future Internet should be designed to support traceability of a malicious activity.

4.5.1.4 User Privacy

User privacy is hot issue in today’s network environment. The privacy information includes personal identification data such as social security number and e-mail ID. In addition, it includes location data of an user such as GPS information of a smart phone. The customer’s personal information on service provider should be handled confidentially by adopting cryptographic encryption and secure audit technology. Also, service providers cannot achieve normal user’s private information including location data without the prior consent.

Accordingly, the Future Internet should be designed to support user privacy.

4.5.1.5 Consideration of System Availability

The security function should be developed in consideration with system availability. Security problem is big issue nowadays because the security features has been developed without taking into account the availability. For example, the system with security function such as firewall and IDS shows lower performance compared to the system without security function. This makes it hard to deploy the security function in the whole network.

Accordingly, the Future Internet should be designed to develop security function in consideration with system availability.

4.5.2 Technical Principles

4.5.2.1 Self-Certifying Identification

Future Internet should support the built-in security which allows an entity to validate that it is communicating with the correct entity without needing access to external databases information, or configuration. The use of self-certifying identifiers for network entities can provide intrinsic security. The self-certifying identifier can be defined as an identifier which is proved without relying on any global trusted authority. One example for the self-certifying identifier of the network entity is the public key of the network entity or the hash of the public key. With the self-certifying identifier the Future internet should support mutual authentication of the respective host. In addition, the Future Internet should support integrity and validity of the content that a user requests.

4.5.2.2 User-Centric Identity Management

Future Internet should support user-centric identification management which allows users to have control over their identity information as it's collected and stored. In addition, users should be able to know and restrict who might use the data for what purposes.

4.5.2.3 Trust Domain Management

The Future Internet should support trust domain management. The domain can be defined as logical or physical communication group in the whole network. The trust domain can be defined as the domain which is composed of the entities trust each other. Entities outside of the trust domain should have high level of security policies to communicate each other. However, entities inside of the trust domain can have low level of security policies. Future Internet should support the built-in security which allows an entity to validate that it is communicating with the correct entity without needing access to external databases information, or configuration. The use of self-certifying identifiers for network entities can provide intrinsic security.

5. RECOMMENDATIONS

[Editor's Note: The section will be described after maturing the draft document]

6. REFERENCES

[1-1] Infographic, Cisco, http://www.ditii.com/2011/08/23/infographic-cisco-50-billion-things-on-the-internet-by-2020/

[3-1] D.D. Clark, The Design Philosophy of the DARPA Internet Protocols, ACM SIGCOMM Computer Communications Review, Vol. 18, No. 4, Aug. 1988, pp. 106-114

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

[3-3] ITU-T Recommendation Y.3001 (2011), Future Networks: Objectives and Design Goals.

[4-1] George Koutitas and Panagiotis Demestichas, "A Review of Energy Efficiency in Telecommunication Networks," Telfor Journal, Vol. 2, No. 1, 2010.

[Editor's Note: Requirements are not limited to above items. Additional requirements will be added according to contributions. Any contribution to FIF AWG is welcome: architecture@fif.kr or twyou@etri.re.kr]

APPENDIX

[Editor's Note: The appendix gives background information about world-wide research activities relevant requirements and principles for FIA]

1. SUGGESTED DESIGN PRINCIPLES

[Ref: Keith Howker, Jim Clarke, Frances Cleary, Waterford Institute of Technology, Nick Wainwright, Nick Papanikolaou,HP Labs Bristol]

- **The FIArch Call for Position Papers on Internet Design Principles includes a short initial list:**
  - modularization by relaxed layering
  - connectionless datagram forwarding
  - network of collaborating networks
  - end-to-end principle/fate sharing principle combined with intelligent end-systems
  - simplicity principle
  - loose coupling principle
  - locality principle

- **Some suggested additional baseline design principles**
  - service composition/federation* (cf network of collaborating networks)
  - interoperability of services and entities*
  - dynamics and mobility*
  - heterogeneity*
  - gateway(ing) services – across

- cross-layer needs – up and down
- modularity – reusable/replaceable (service-, etc.-) components
- compartmentalisation (cf loose coupling and localisation)
- simplicity and understandability – allowing manageability

2. FUTURE INTERNET DESIGN PRINCIPLES

[Ref: "Future Internet Architecture (FIArch) Group]

- **Principles that should be preserved**
  - Inherent backwards compatibility principle
  - Heterogeneity support principle
  - Scalability & the Amplification Principle
- **Principles that should be adapted (modification of existing description)**
  - Keep it simple, but not stupid principle
  - Minimum Intervention Principle
  - Security, confidentiality and authentication principles
- **Principles that should be augmented (addition to the existing description)**
  - Polymorphism principle
  - Unambiguous naming data & services principle
- **Seeds for New Design Principles**
  - Networking is IPC and only IPC
  - Trusted IPC –to –Trusted IPC principle

3. XIA: EXPRESSIVE INTERNET ARCHITECTURE

- **P1: Evolvable Set of Principals**
  - Identifying the intended communicating entities reduces complexity and overhead
  - No need to force all communication at a lower level (hosts), as in today’s Internet
  - Allows the network to evolve
- **P2: Security as Intrinsic as Possible**
  - Security properties are a direct result of the design of the system
  - Do not rely on correctness of external configurations, actions, data bases
  - Malicious actions can be easily identified
- **Narrow waist for trust management**
  - Ensure that the inputs to the intrinsically secure system match the trust assumptions and intensions of the user
  - Narrow waist allows leveraging diverse mechanisms for trust management: CAs, reputation, personal, …
- **Narrow waist for all principals**
  - Defines the API between the principals and the network protocol mechanisms
- **All other network functions are explicit services**
  - XIA provides a principal type for services (visible)
  - Keeps the architecture simple and easy to reason about