# Requirements For Future Internet Architecture

## (draft-FIA-Requirements-r.0.5)

July 2011

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

## Summary

The document collects the requirements to be considered in the design of Future Internet Architecture from various areas. Based on the requirements, Architecture Working Group (AWG) of Future Internet Forum (FIF) aims to provide some recommendations for Future Internet Research.

*[Editor's Note: This draft is for internal discussion only]*

## Contributors

| Name | Affiliation | Contributions |
|---|---|---|
| HY Jung | ETRI | General Requirements |
| WJ Chun | ETRI | General Requirements |
| SJ Koh | KNU | Technical Requirements – Mobile perspective |
| MY Jang | SAIT | Technical Requirements – Content-centric perspective |
| TK Kwon | SNU | Technical Requirements – Resolution system perspective |
| SJ Jeong | ETRI | Technical Requirements – Green networking perspective |
| SW Lee | ETRI | Technical Requirements – Security perspective |
| YH Kim | ETRI | Testbed Requirements |

# TABLE OF CONTENTS

# 1. OVERVIEW

The Internet has been working for longer than 40 years, and now it faces many challenging technical (and non-technical) issues. There were lots of activities to address these issues for designing Future Internet over the world. However, it seems to be hard to point out principles and requirements for FIA even though there were lots of drawbacks of current Internet, due to ossifying TCP/IP architecture. The Architecture Working Group (AWG) in FIF aims to deal with these issues by collecting requirements on the FI design and providing some recommendations for Future Internet Research.

# 2. GENERAL REQUIREMENTS

## 2.1 Mandatory requirements

The clause describes mandatory requirements that FIA should be required to have capabilities among various current Internet problems.

*[Editor's Note: following requirements are proposed by editor and need further discussion]*

- **Accountability** (of resource usage and security without impeding user privacy, utility and self-arbitration)
- **Diagnosability** (root cause detection and analysis)
- **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).
- **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)
- **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.

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

- **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.

- **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

- **Simplicity and cost-effectiveness**: more data is needed but simplicity seems to be progressively decreasing see 7.3. 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.

- **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

## 2.2 Desirable requirements

This clause describes optional requirements that FIA is recommended to have capabilities among various current Internet problems.

*[Editor's Note: following requirements need to more specific description]*

- Availability or resiliency

- Evolutionary change

- Coexistence among multiple networking architectures

- Content-centric usage
- Energy efficiency
- Manageability
- Accountability
- Delivery inefficiency (or Data explosion)
- Heterogeneity (DTNs, VANETS, M2M, etc.)

## 2.3 Architectural components to revisit for key requirements

This clause describes fundamental requirements for designing FIA. Following requirements are co-related with FIA design principles.

- Naming and addressing
- Routing
- Resolution (between name or ID and address)

# 3. TECHNICAL REQUIREMENTS

This clause describes requirements to make realization of architectural components by technical point of view. Following requirements could be touched on design principles of current Internet.

## 3.1 Mobile perspective

*[Editor's Note: following requirements were proposed by KNU. Further discussion is needed, especially * marked items are still controversial]*

### 3.1.1 ID/LOC SEPARATION

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.

### 3.1.2 BACKBONE AND ACCESS NETWORK SEPARATION*

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.

### 3.1.3 CONTROL AND DATA PLANE SEPARATION*

In general, 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.

In addition, 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. However, the control information for signalling is mission-critical and thus needs to be delivered more urgently, compared to usual data traffics. Thus, the control function needs to be separated from data traffics.

### 3.1.4 DISTRIBUTED MOBILITY CONTROL*

Most of the current mobility schemes are based on a centralized mobility anchor, such as HA of MIP or LMA of PMIP. The centralized control, however, tends to inject unnecessary data traffic to Internet core, and thus the data traffic explosion problem becomes more severe. In terms of performance, the routing path through a centralized anchor tends to be longer, which results in non-optimal routes and performance degradation. Moreover, the centralized approach is vulnerable to a single point of failure or attack.

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.

### 3.1.5 SUPPORT OF WIRELESS LINKS AND HOSTS

In Internet, it is implicitly assumed that the existence of 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.

In addition, in mobile environment, we should be able to support idle/sleep-mode hosts to save their electric power. Nonetheless, in Internet we assume that most of the hosts are always on active state. This naturally requires some advanced capability, such as paging.

## 3.2 Content-centric perspective

*[Editor's Note: following requirements were proposed by SAIT. Further discussion is needed.]*

### 3.2.1 LOCATION-INDEPENDENT CONTENT ACCESS

A content file should be retrieved to a user even if the user does not know its current location(s), even though its origin server is not accessible, the user should access the content file when there is its replica in a node connected to networks.

### 3.2.2 NEAREST CONTENT ACCESS (ANYCAST)

It is desirable to bring the content from the place that can deliver the content as fast as possible

### 3.2.3 MULTICAST & TIME-SHIFTED MULTICAST

It is desirable to minimize the number of transmitting the same content over the same physical link

### 3.2.4 COST EFFICIENT DATA DISSEMINATION/DISTRIBUTION

Networks should be suitable to support user generated data dissemination as well as commercial data dissemination.

### 3.2.5 ID/LOCATOR SEPARATION

The locator of a node can be changed, but it is better to keep the node's identifier fixed. A single ID can refer to multiple nodes. Multiple IDs can refer to the same node.

### 3.2.6 CONNECTIVITY-INDEPENDENT NETWORK LAYER

Network API should be independent of the physical wireless communication technologies such as WiFi, Cellular, BlueTooth, etc.

### 3.2.7 MULTIPATH SUPPORT

Sender and receiver nodes may be connected by more than one communication interface at the same time.

### 3.2.8 MULTISOURCE SUPPORT

A node may request the same content file from multiple nodes.

### 3.2.9 CONTENT SECURITY

The authentication and the data integrity of content received should be verified (e.g. by signature). It is better to have confidentiality only to authorized user(s)

### 3.2.10 NETWORK SECURITY

The performance of networks should not be affected by DDoS attacks.

### 3.2.11 NODE PRIVACY

It is desirable to have anonymity among nodes

### 3.2.12 SERVER-LESS NETWORKING

It is desirable to retrieve a content file without contacting resolution servers (e.g. DNS). It is better to ensure authentication and data integrity without contacting key management servers.

### 3.2.13 STRATEGY-BASED PACKET FORWARDING

Networks support various strategies to download a content file from a static node over a mobile node, a high throughput node over a low throughput node, or a near located node over a far located node.

### 3.2.14 SCALABILITY

The overhead of control traffic that exchange routing information between nodes is less than O(n)

(n = # of nodes or # of major content prefixes)

### 3.2.15 MOBILITY SUPPORT

It is desirable to support mobile node

### 3.2.16 MANAGEABILITY

It is desirable to diagnose, pinpoint, and troubleshoot the network anomalies

### 3.2.17 INCREMENTAL DEPLOYMENT

The deployment of new Internet architectures and/or protocols should not disrupt operations of the current Internet.

### 3.2.18 CONTEXT/NETWORK-AWARENESS

Content delivery path should be adjusted according to the status of network traffic.

## 3.3 Resolution system perspective

*[Editor's Note: following requirements were proposed by SNU. Further discussion is needed.]*

The resolution system in the Future Internet may have to support key mapping. That is, when a user (or a host) sends a query for a key to the resolution system, it should reply with the value that corresponds to the given key. The current resolution system is the DNS, which is host-oriented, and mainly used for mapping between domain names and their corresponding IP addresses. The DNS requires the connectivity 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.

### 3.3.1 FLEXIBILITY

The resolution 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 resolution 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 can be other usages of the resolution system in the Future Internet. It should be able to be extended to support other naming or resolution functionality.

### 3.3.2 AVAILABILITY/RESILIENCY

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

### 3.3.3 SPEED

The mapping of key-value pairs may be replicated worldwide or to some places close enough to potential solicitors, so that the delay of resolution does not affect the Internet applications and services.

#### 3.3.4 AUTHENTICITY/DATA 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.

#### 3.3.5 ABSENCE OF GLOBAL CONNECTIVITY

The resolution system may have to be able to operate even without its global connectivity. For instance, sensor networks, ad hoc networks may operate individually without connectivity to the global Internet. The resolution system need operate in a local network in an autonomic manner.

## 3.4 Green networking perspective

*[Editor's Note: following requirements were proposed by ETRI. Further discussion is needed.]*

#### 3.4.1 GENERAL REQUIREMENT

Green networking should provide a way to reduce energy required to carry out a given task while maintaining the same level of performance.

#### 3.4.2 CORE NETWORK

- Protocols used in core network should be designed in order to establish a reliable connection but at the same time be power efficient.
- Energy management functions should be deployed in core networks
- Electronic networks may need to be replaced by optical networks as much as possible in order to reduce the power consumption for data transfer

#### 3.4.3 ACCESS NETWORK

- Energy efficiency should be considered during network planning and dimensioning

- Power management techniques should be deployed in access network equipments
- Energy-aware network protocols should be used in access networks
- Optimized transmission and access techniques should be supported in wireless access networks
- Advanced techniques for wireless channel management should be supported in wireless access networks
- Optical fibers (FTTH PONS, FTTCab, etc.) need to be deployed in order to reduce energy consumption

### 3.4.4 NETWORK EDGE

- Low power electronics may be used for reduce energy consumption
- Efficient battery technology should be deployed in nodes
- Nodes should support energy saving mode i.e., sleep mode, in order to reduce power consumption
- Network interfaces should support power management techniques such as adaptive link rate and sleeping mode
-

### 3.4.5 DATA CENTERS

- Server and network virtualization should be supported in order to increase the number of virtual machines per resources
- Server and network consolidation should be considered in order to decommission underutilized physical resources
- Rack space consolidation should be considered in order to relocate underutilized racks
- Data center consolidation should be considered in order to shut down underutilized facilities

## 3.5 Security perspective

*[Editor's Note: following requirements were proposed by ETRI. Further discussion is needed.]*

### 3.5.1 BUILT-IN SECURITY

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.

### 3.5.2 MALICIOUS-PACKET-FREE NETWORK ARCHITECTURE

Future Internet should support network architecture which guarantees that there are no malicious packets such as the data from a spoofed host in the network.

### 3.5.3 TRACEABILITY OF MALICIOUS HACKER

Future Internet should support traceability of a malicious hacker. It means that the network should have the functionality on achieving location information or identifier of the malicious hacker.

### 3.5.4 AUTHENTICATION OF NETWORK ENTITY

Future Internet should support mutual authentication of the respective host.

### 3.5.5 CONTENT INTEGRITY

Future Internet should support integrity and validity of the content that a user requests.

#### 3.5.6 USER PRIVACY

Future Internet should support user privacy. It means that service providers cannot achieve normal user's private information without the prior consent.

# 4. REQUIREMENTS ON TESTBED TO EVALUATE A NEW FI ARCHITECTURE

*[Editor's Note: following requirements were proposed by ETRI. Further discussion is needed.]*

## 4.1 Testbed architecture perspective

#### 4.1.1 VIRTUALIZATION

The testbed should hide hardware characteristics about substrates of the testbed to users (M) and it should provide severe resource isolation between slices and slivers (D).

#### 4.1.2 PROGRAMMABILITY

The testbed should provide dynamic downloading of virtual machines (M) and it provide easy programming environment of virtual machines (D).

#### 4.1.3 FEDERATION

The testbed should provide federation between multiple domains (M).

## 4.2 Experiment support perspective

#### 4.2.1 RESOURCE DISCOVERY

The testbed should support tools for discovering resources available to slices (M).

### 4.2.2 SLICE MANAGEMENT TOOLS

The testbed should support tools for configuring, managing, and monitoring slices (M).

### 4.2.3 SOFTWARE DEVELOPMENT TOOLS

The testbed should support tools for programming and debugging virtual machines (D).

### 4.2.4 RANGE OF EXPERIMENT LIFETIMES

The testbed should support a wide range of lifetime, i.e., ranging from minutes, days, weeks, months, to years as the running duration of a slice (M).

### 4.2.5 REPEATABILITY

The testbed should support repeatable behaviour of slices (D).

### 4.2.6 INTENTIONAL FAILURE AND DEGRADATION

The testbed should support intentional failure and degradation in virtual nodes on command (D).

### 4.2.7 ADDITION OR REDUCTION OF RESOURCES

The testbed should support addition and reduction of resources used in a slice to grow or shrink the slice (M).

### 4.2.8 OAM

The testbed should provide OAM functions to users (D).

#### 4.2.9 BIBLIOGRAPHY

The testbed should support a bibliography site by which users can access research results performed on the testbed (D).

## 4.3 Instrumentation and measurement perspective

#### 4.3.1 MEASUREMENT DATA

The testbed should provide the on-line collection, storage, and access of the data measured in slices (M).

#### 4.3.2 NODE LOCATIONS

The testbed should provide the location information of physical nodes available to users (M).

#### 4.3.3 POWER USAGE

The testbed should provide the information of power usage consumed in slices (D).

## 4.4 User opt-in perspective

#### 4.4.1 USER ACCESS

The testbed should provide easy and secure user access environment to the testbed (M) and it should permit the user access via the current Internet (D).

## 4.5 Testbed sizing perspective

### 4.5.1 NUMBERS OF CONCURRENT EXPERIMENTS

The testbed should support at least 10 continuous, concurrent experiments (M).

### 4.5.2 INFRASTRUCTURE SCALE

The tested should support at least 3 physical nodes within a domain (M).

# 5. RECOMMENDATIONS

TBD

# 6. REFERENCES

TBD

---

*[Editor's Note: Requirements are not limited to above items. Additional requirements will be added according to contributions]*

---