TECHNICAL REPORT

ISO/IEC TR 29181-1

First edition
2012-09-15

Information technology — Future Network — Problem statement and requirements —

Part 1: Overall aspects

Technologies de l'information — Réseaux du futur — Énoncé du problème et exigences —

Partie 1: Aspects généraux

Reference number
ISO/IEC TR 29181-1:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 29181-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems.*

ISO/IEC TR 29181 consists of the following parts, under the general title *Information technology — Future Network — Problem statement and requirements:*

— *Part 1: Overall aspects*

The following parts are under preparation:

— *Part 2: Naming and addressing*

— *Part 3: Switching and routing*

— *Part 4: Mobility*

— *Part 5: Security*

— *Part 6: Media distribution*

— *Part 7: Service composition*

Introduction

The current Internet has become an essential communication infrastructure, not only for data transfer but also for social applications 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 about the following technical aspects of the current Internet, including IP based networks: scalability, ubiquity, security, robustness, mobility, heterogeneity, Quality of Service (QoS), re-configurability, context-awareness, manageability, economics, etc. Also, the advancement of mass storage units, 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 network technologies.

The Future Network (FN), which is anticipated to provide functionalities and services beyond the limitations of current networking technology, has been studied by researchers in the field of communication network and services worldwide. FN technologies have now been widely and deeply studied in many research organizations and standardization bodies.

This part of ISO/IEC TR 29181 describes overall aspects for FN including definition, general concept, problems and requirements. Also, it discusses a milestone for standardization on FN.

Information technology — Future Network — Problem statement and requirements —

Part 1: Overall aspects

1 Scope

This part of ISO/IEC TR 29181 describes the definition, general concept, problems and requirements for Future Network (FN). It also discusses a milestone for standardization on FN. The scope of this part of ISO/IEC TR 29181 includes:

— motivation of FN;

— definition, general concept, and terminologies of FN;

— services and applications in FN;

— problems with current networks;

— design goals and high-level requirements for FN;

— milestones for standardization on FN.

2 Normative references

There are no normative references.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
Future Network
FN
network of the future which is made on clean-slate design approach as well as incremental design approach; it should provide futuristic capabilities and services beyond the limitations of the current network, including the Internet

3.2
clean-slate design approach
approach where a system and network are designed from scratch, based on a long-term, revolutionary approach

NOTE In clean-slate design approach, the backward compatibility may not be required [1],[2].

3.3
network virtualization
technology that enables the creation of logically isolated network partitions over shared physical network infrastructures so that multiple heterogeneous virtual networks can simultaneously coexist over the shared infrastructures

NOTE Network virtualization allows the aggregation of multiple resources and makes the aggregated resources appear as a single resource [3],[4].

3.4
cross-layer communication
technology that enables to 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

3.5
autonomous service
service that enables users or services in motion to configure autonomously and to mange networks

3.6
context-awareness service
service that enables applications or services to adapt their behaviour based on their physical environment

3.7
content-centric networking
technology that enables to support routing based on contents rather than physical location

3.8
service composition
technology that supports the composition of those activities required to combine and link existing services (atomic and, even composite services) to create new processes; i.e., the customizability of the services provided to the end users

3.9
customizable QoS/QoE
technology that enables to support preference setting and service composition/re-composition accordingly

3.10
economic incentives
encouragement, rewards and compensation which motivates the parties (components/participants) economically to contribute for networking and/or services and/or to provide their resources

3.11
Building Blocks (BB) approach
technique for development of a set of standards by creating some basic modules or elements that may be added together so as to obtain an overall architecture or entire operations

NOTE This approach may be used to develop a new challenging technology, such as Future Network, in which many of the basic associated elements have not been identified at the current stage.

[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 [5].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

AAA	Authentication, Authorization, and Accounting
BB	Building Blocks
DNS	Domain Name System
FA	Functional Architecture
FI	Future Internet
FIRE	Future Internet Research and Experiments
FN	Future Network
FP7	Framework Program 7
GENI	Global Environment for Network Innovations
ICT	Information Communication Technology
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
NAT	Network Address Translation
NGN	Next Generation Networks
NwGN	New Generation Network
P2P	Peer-to-Peer
PI	Provider Independent
QoE	Quality of Experience
QoS	Quality of Service
SOA	Service Oriented Architecture

5 Overview

5.1 Needs to research and standardize FN

The current IP-based technology has significant deficiencies 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 flow mobility, support of fast mobile hosts, safe e-transactions, quality of service guarantees, business aspects, etc., on current IP-based networks, so various researches have been conducted to solve these problems. Further, there are now significant concerns that shortcomings would not be completely resolved by the conventional incremental and 'backward-compatible' style of current research and standardization efforts. That is the reason why the FN research effort is called a “clean-slate design for anew network’s architecture”. It is assumed that FN design must be discussed based on a clean-slate approach as well as an incremental design approach.

In this regard, we need to study and standardize the FN which overcomes the limitations of current networks, and enable new plentiful services.

5.2 Value and vision of FN

The business model of FN aims for profit sharing among infrastructure providers, service providers, application providers and end users by building cooperative eco-systems between them. It can be accomplished by openness and accommodating various requirements of each party.

Also, FN will be able to provide millions/billions of services, therefore flexible service composition is required to achieve the FN of context-aware services. Context-aware service composition is a key functionality required to provide dynamically adapted services, and a key feature to guarantee a seamless provisioning of media services, which will allow to generate enriched and novel services for end-users.

Figure 1 illustrates vision and roadmap of FN.

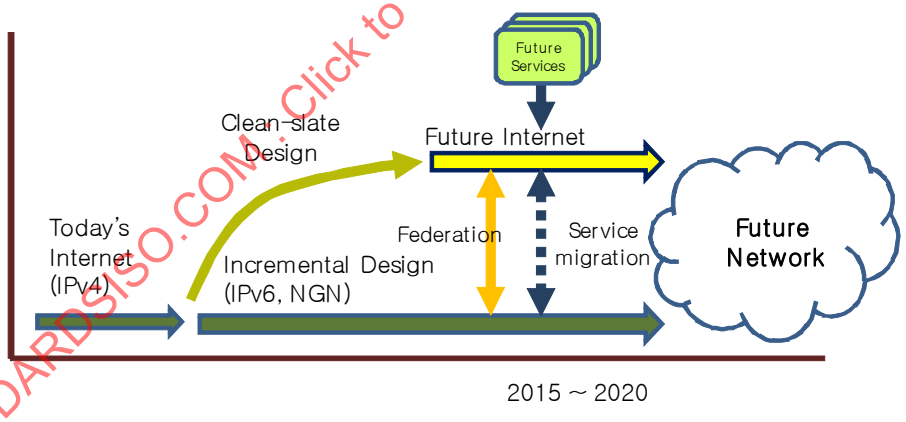

Figure 1 — Vision and Roadmap of FN

Today’s networks are mainly based on the IPv4 Internet. To enhance the Internet, there are two design approaches – clean-slate design and incremental design. Future Internet will be designed based on clean-slate approach and roughly prototyped and deployed between 2015 and 2020. At the same time, today’s networks will be evolved continuously. Thus, there will be two different network technologies and federation and service migration are required to support seamless integration. Federation is to be defined as an interconnection of multiple, heterogeneous networks (e.g, IPv4, IPv6, Future Internet, or non-IP based networks). In federation, networks would be normally be geographically dispersed and managed by different organizations/ISPs. They would however be considered as being part of single network, in so far as they are operated in a common management framework under a common management authority. So, multiple,

heterogeneous networks would be eventually seen as a single federated network – FN. The FN covers all the disruptive networks as well as existing networks. FN has a broader view than the Future Internet, and includes other non-IP networks (e.g., sensors, vehicular networks, satellite, etc.).

6 Services and applications in FN

In the clause, the following future services are envisioned and considered as benchmark services to achieve to build the FN.

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.

Research projects	Envisioned future services
GENI [7] (Global Environment for Network Innovations)	– Ubiquitous health care – Participatory urban sensing – Dealing with personal data – Tele-presence
NwGN [8] (New Generation Network Architecture)	– Essential services: medical care, transportation, emergency services
EU FP-7 [9] (European Union Framework Program-7)	– Personal service creation – Future home – Future of traffic – Virtual reality – Productivity tools
Korean Future Internet Development and Deployment Strategies [10]	– Smart Network services – Cloud Network services – Internet of Things services –

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 FN will encompass wide range of heterogeneous networks [11]:

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

FN (or future) services can be stated as:

- the services which emerge by the year 2020
- 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 2): 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.

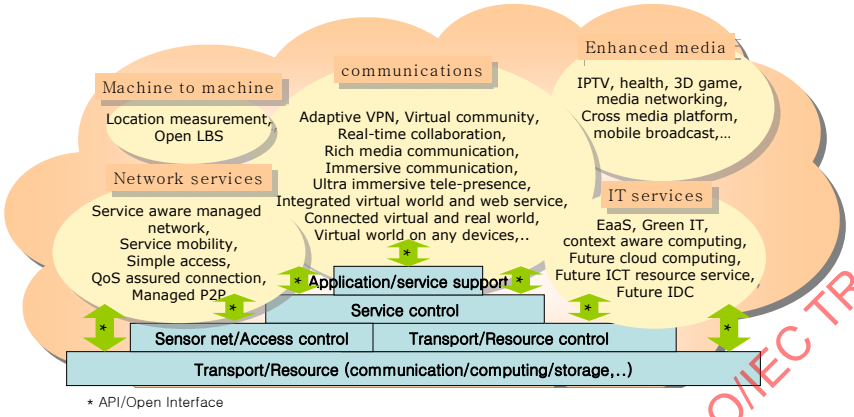

Figure 2 — Services Concept of FN

The key features the FN services should support include:

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

7 Problem statement

The problems for the FN could be classified into i) basic problems and ii) problems with fundamental design principles of current Internet. Most of them are also studied and researched in many organizations and research projects such as IETF/IRTF[12, 13], ITU-T [14], EU FIA Arch group [15].

7.1 Basic problems

7.1.1 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.

7.1.2 Insecurity

One of the main problems on the today's Internet is that it does not providesecure 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.

7.1.3 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. Moreover, multiple interfaces are recently available to user devices for the accessing of heterogeneous multiple access networks. In this case, flow level traffic control is needed in addition to host level mobility management.

7.1.4 Quality of service

Current 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.

7.1.5 Heterogeneous physical layers, applications and architecture

Current Internet 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.

7.1.6 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.

7.1.7 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.

7.1.8 Opportunistic communications

Current 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.

7.1.9 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.

7.1.10 Lack of efficient 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.

7.1.11 Customizability

The Internet has evolved to reflect changes in the way it is used. Originally, it was primarily used by scientists for networking research and for exchanging static information. However, it is now also used to carry digital media such as audio and video, which have very different requirements from the original traffic. Moreover, in the near future, this heterogeneous and dynamic context is going to rise exponentially. Additionally, it is expected that the Future Media Internet will allow to share and distribute high quality and rich (including 3D) multimedia content and services in a flexible, efficient and personalized way. This will directly impact on the improvement of quality of life, working conditions, edutainment and safety.

Broader speaking, the user will consume services that will be a composition of simple or already composited services, and these will not be limited only to media services, but also to network services and any other kind of required services.

In addition, FN will require to deal with transparent network-imposed blackboxes if they want to add intelligence to the network (opposite to end-to-end principle used for current internet design). Middleboxes or blackboxes should be natively supported by networks as they are key in order to provide future value added services and capabilities.

7.1.12 Economy and policy

There is also a question of how infrastructure providers, service providers, and end users 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.

7.2 Problems with fundamental design principles of current Internet

7.2.1 Packet switching

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

7.2.2 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.

7.2.3 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.

7.2.4 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 FN objectives.

8 General requirements for FN

In this clause, new design goals and high-level requirements for the FN are described.

8.1 Scalability

The FN should support scalable routing architecture. 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 should include following aspects:

- Routing and addressing architecture
- Multi-homing and provider independence (PI routing)

8.2 Naming and addressing scheme

The FN 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 FN 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

8.3 Security

The FN 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.

8.3.1 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 FN will require codifying legal, societal and practical considerations.

8.3.2 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 FN 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.

8.3.3 Peer

Why the authentication and trust of ends become a challenge in current networks? One of important reasons is that many authentication mechanisms cannot 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 in a network. Hence, the authentication mechanisms of peer and multi-security should be designed for FN.

8.3.4 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 FN. 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.

8.3.5 Heterogeneity

Authentication mechanisms for FN 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 carewhere the data or service is located and which host they are connecting to.

8.3.6 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, eeplay attacks, verifier impersonation attacks, password discovery attacks, etc. Authentication mechanisms for FN should be possible to implement a range of countermeasures to the authentication attacks described above.

8.4 Mobility

The FN 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 FN.

- 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 FN, 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 FN. 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. FN should be able to provide the route optimization for mobile terminals, which needs to be considered for design of the mobility control for FN.

- Use of lower layer information: To provide seamless services for mobile users, the mobility control for FN 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.

- Support of flow-level mobility: When multiple interfaces are simultaneously active on a host, a system should be able to dynamically distribute each service flow to one of diverse access networks that is most suitable and efficient for it, to provide a wide range of QoS/QoE to a user. An application should be also able to have several connections and allow each traffic to use the access network that is most suitable to its characteristics. Therefore, Future Internet should be able to provide a mechanism for supporting this multi-connectivity and flow mobility control.

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

8.4.1 Context-awareness

Mobility in the FN is expected to support context-awareness. Clause 8.7.4 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.

8.4.2 Multi-homing and seamless flow switching

Mobility in the FN should support multi-homing, i.e., multiple access paths to heterogeneous /homogeneous networks. In this case, the vertical handover should be provided to seamlessly switch the network connection when necessary. In addition to host level horizontal/vertical handover support, flow level traffic control should be supported so that traffic flows can be dynamically distributed to diverse access networks while allowing a host to use multiple interfaces simultaneously.

8.4.3 Heterogeneity

Mobility in the FN is expected to support heterogeneity. Clause 8.6 describes details on heterogeneity.

8.5 Customizable quality of service

The FN should support quality of service (QoS) from user and/or application perspectives. In addition, QoS in the FN is expected to support service composition and context-awareness described in clause 8.7.2 and 8.7.4, respectively.

8.6 Heterogeneity and network virtualization

The FN 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. Also, following features should be provided under the context of heterogeneity support in the FN.

8.6.1 Application/service heterogeneity

The FN 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.

8.6.2 Device heterogeneity

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

8.6.3 Physical media heterogeneity

The FN 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.

8.6.4 Network virtualization

The FN should provide much better support for a broad range of applications, services, and network architectures. In the FN, multiple isolated logical networks each with different applications, services, and architectures should share the physical infrastructure and resources. Network virtualization is the key features to support them, and federation, and network programmability should be also tightly coupled with it.

The virtual networks are completed isolated each other, so different virtual networks may use different protocols and packet formats. When combined with programmability in network elements, users of virtual networks can program the network elements on any layers from physical layer to application layer. They can even define new layering architecture without interfering the operation of other virtual networks. In other words, each virtual network can provide the corresponding user group with full network services similar to those provided by a traditional non-virtualized network. The users of virtual networks may not be limited to the users of services or applications, but may include service providers. For example, a service provider can lease a virtual network and can provide emerging services or technologies such as cloud computing service, and so on. The service providers can realize the emerging services as if they own dedicated physical network infrastructures. In order to facilitate the deployment of network virtualization, it may be necessary to provide control procedures such as creating virtual networks, monitoring the status of virtual network, measuring the performance, and so on.

The FN is also recommended to support federation and programmability with network virtualization technology. Federation enables the networks to be operated as being part of a single network with sharing network resources, even though the networks are geographically dispersed and managed by different providers. Programmability enables users to dynamically import and re-configure new invented technologies into virtualized equipments (e.g., routers/switches) in networks.

8.7 Service awareness

The FN should provide services efficiently taking into consideration the requirements posed by each communication. Thus, service provisioning should consider the needs in terms of QoE and preferences of the communication requester. Consequently, the service requester will improve its service experience if requirements are considered.

Furthermore, context data is essential in order to provide adapted services, create and enrich value-added services and to adapt them if context conditions change during service execution.

The FN should be able to discover and compose services considering QoE parameters, preferences and context conditions.

The following features are fundamental to be adopted by the FN:

- Service Discovery
- Service Composition
- Self-organizing service Context-awareness, and
- Service QoE

8.7.1 Service discovery

The FN should provide service discovery which is to provide services according to the specific node policies and the context information (e.g. user, device, service, system resources, and network context). The FN needs to consider distributed service discovery, since it will consists of large number of services and resources in distributed environment.

In specific, service discovery is how to find and select the best service out of a number of discovered services for a service request. On the request of a service type by a user or a composite service, candidate services are discovered based on the requested service type. Then the FN selects one of them considering the context and their properties such as activity status, performance, charge, and load.

8.7.2 Service composition

The FN should support efficient methods of service composition for composite services. The FN should support static and dynamic service composition where static composition is accomplished at design time and dynamic composition is accomplished at run time.

The FN should support context aware service composition using different types of context in the service composition process. It means that the FN should be able to adapt its operations to the context changes during the service execution phase (i.e. dynamic adaptation).

For service composition, the FN should 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 covers how to discover atomic services across heterogeneous network environments and select the best service out of a number of discovered services for a service request. On the request of a service type by a user or a composite service, candidate services are discovered based on the requested service type. Then the service composition component selects one of them considering the context and their properties such as activity status, performance, charge, network status and load.

8.7.3 Self-organizing service

The FN should provide support for self-organization of services that are spread across the network. Services may be autonomously distributed, replicated and migrated within FN to optimize the availability, performance,response times, and network usage.

In FN, it is required to provide efficient mechanisms for the self-organized placement and coordination of services within a network, since they allow for autonomous configuration and adaptations to dynamic changes in terms of service availability, overload or failure.

In specific, the feature of self-organization of services includes self-configuration, self-optimization and self-recovery of services.

8.7.4 Context-awareness

The FN should 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.

Applications or services may use this context information for their own purpose. Instead of those applications and services who have difficulties in obtaining the context from various sources of context, the Future Network should take charge of collecting raw information from the sources and modelling/reasoning of the context.

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 context can be handled in composite manners as well as solely with each of user, device, service, and network context. For example, a composite context can be constructed with considering user and network context together. This composite context can be exploited at service composition or external use by services so that they do not have to further collect or reason different types of context.

The FN should support the context management to provide customized and context based services.

8.7.5 Service QoE

The FN should be able to provide customized services according to context or preferences of users) in order to maximize QoE requested for a service.

Service QoE is a subjective measure of user's experiences when using a specific service. The metrics needed to estimate the level of QoE depend on the specific service that is being requested by a user. In addition, QoE is closely related with QoS, which attempts to objectively measure the service delivered by a provider.

8.8 Media transport

The FN should support efficient methods to deliver media. 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.

8.9 New layered architecture

The FN may need a 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, FN 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.

8.10 Management

The FN should support Instant and easy management. The FN will become more and more complex with emerging services and architectural diversity. The following features should be provided under the context of management in the FN.

8.10.1 Robustness

The FN should be as robust, fault-tolerant and available as the wire-line telephone network is today. Robustness should be considered from the following aspects: automatic reporting of link and equipment failures automatic and immediate re-routing around failures; resilience to equipment malfunction; and resistance to denial-of-service and similar attacks.

8.10.2 Autonomy

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

8.11 Energy efficiency

The FN should provide energy saving capabilities to support green ICT environments. Energy-saving of networks means a network capability where total power consumption of network equipment such as routers and switches is systematically used thus reduced of energy consumption comparing with current networks.

8.12 Economic incentives

The FN should provide economic incentives to the infrastructure providers, service providers, and end users that contribute to the networking. For example, infrastructure providers and service providers contribute to construct the infrastructure of network. The end users of GRID computing contribute to provide resources. Therefore it is desired that the FN provides with explicit economic primitives. The following features should be provided under the context of economic incentives in the FN.

8.12.1 Quality of service/experience

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

8.12.2 Manageability

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

8.12.3 Customizability

The FN should be customizable along with diverse requirements and/or preferences of each user.

8.12.4 AAA and security

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

8.12.5 Operational aspect

The FN should provide network providers and/or ISPs an operational platform (infrastructure and architecture) in terms of economic activities.

9 Milestone for standardization on FN

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

9.1 Overall work plan

This TR has described the problem statement and requirements for 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 3.

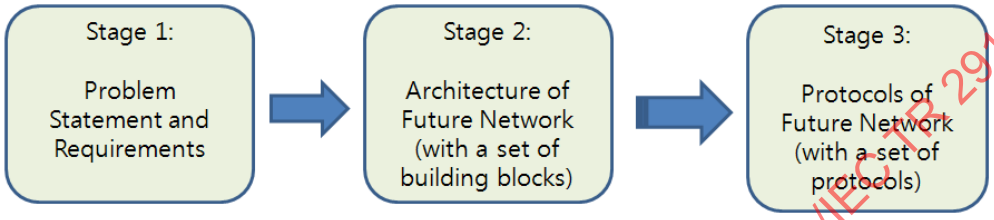

Figure 3 — Overall Milestone of Standardization on FN

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. The BB approach is a technique for development of a set of standards by creating some basic modules or elements that may be added together so as to obtain an overall architecture or entire operations. 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.

9.2 Architectures of FN

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 and Functional Architecture (FA)
- Naming and addressing
- Switching and routing
- Mobility
- Security
- Media transport
- Service composition
- Fedration

Some more additional BBs could be considered, if necessary. These architectural BBs will construct the overall FN architecture, as illustrated in the following Figure 4.

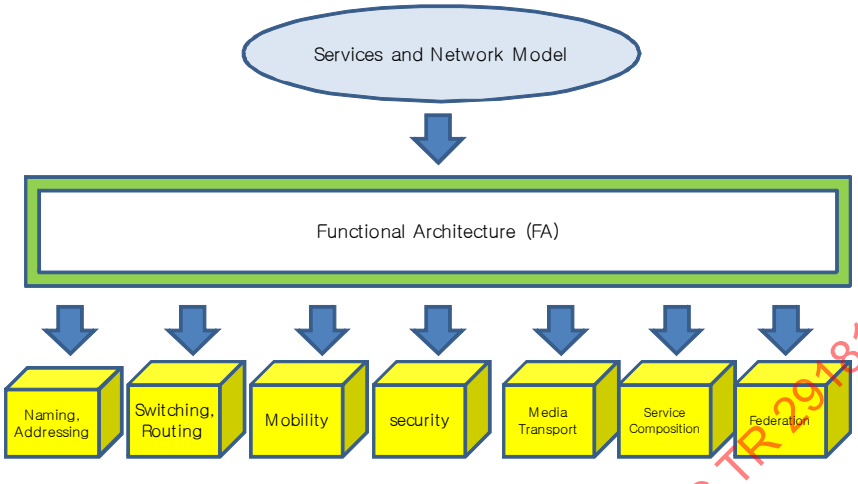

Figure 4 — Building blocks components for FN architecture

As shown in the Figure 4, the Services and Network BBs will be used as substantial inputs to design the generic Functional Architecture (FA) BB. Based on the FA BB, the following specific functional BBs could be designed: Switching/routing, Service composition, Media distribution, Security, Mobility, and more additional BBs. For the standardization process, each of the BBs will be made as a part of the overall FN architecture.

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

9.2.1 FN architecture: services/network model and functional architecture

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;
- 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.

The FA 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 architecture,
- Relationship between user data transport plane and control plane.

9.2.2 FN architecture: naming and addressing

This BB should provide the architecture of naming and addressing for FN. This work needs to address the following issues:

- Identification and Identifier;
- Separation of user identifier from network locator;
- Scalable naming and addressing.

9.2.3 FN architecture : switching and routing

This BB should provide the architecture of switching/routing for FN. This work needs to address the following issues:

- Model of control plane and data plane;
- Functional architecture for switching and routing;
- Requirements for control plane protocols;
- Compatibility and migration.

9.2.4 FN architecture: mobility

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.

9.2.5 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. This work needs to address the following issues:

- Plague of security breaches;
- Spread of worms;
- Denial of service attacks.

9.2.6 FN architecture : media transport

This BB should address how to provide media distribution for FN users. This work need to address the following issues:

- Media discovery;
- Media session management;
- Media distribution mechanism;
- QoS/QoE management;
- Privacy and Security.

9.2.7 FN architecture : service composition

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

- Service Oriented Architecture (SOA);
- Decomposition and re-composition of services;
- Re-configurability and service discovery;
- Service routing;
- Dynamic adaptation.

9.2.8 FN architecture : federation

This BB should address how to incorporate multiple heterogenous networks into a single FN. This work needs to address the following issues:

- Global name space;
- Metadata services;
- Site autonomy;
- Collection and exchange of resources;
- Separation of authentication and authorization.

9.2.9 Protocols for FN

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 JTC 1/SC 6.

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;
- Interworking of the routing/switching protocols with the heterogeneous underlying access technologies;
- End-to-end transmission protocols for user data processing and control;
- Application-specific protocols.

Annex A
(informative)

General concept of FN

General concept of FN could be described as follows:

- The FN is the network of the future which is made on clean-slate design approach as well as incremental design approach. Note that clean-slate design approach was understood as a design principle, not deployment aspect.
- It should provide futuristic functionalities and services beyond the limitations of the current network including Internet.
- The FN should not dependent on the current technologies and solutions.
- The FN provides mechanisms that benefit every participant as much as they contribute.

Figure A.1 illustrates a general conceptual model of FN. Conceptual model of FN is described with two apsects: network architecture and sevice architecture.

Network architecture is the design of a communications network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation. Network architecture of the FN is expressed by its use of a set of component architectures suite as BBs, rather than tranditional TCP/IP Internet suite. These BBs may include the following architectural components, but not enumerative:

- Naming and addressing
- Routing
- Mobility
- Wireless optimization
- Anti-Spam, Security
- Cross-layer communication
- QoS/QoE
- Energy-efficiency
- Management

Also, network virtualization provides capabilities to accommodate a set of heterogeneous architecture components within a single integrated FN architecture.

Service architecture is the design of a communications service. Service architecture of FN is also essentially a collection of services and appllications, as BBs. These services communicate with each other. These BBs may include the following service components, but not enumerative:

- Context-awareness
- Data-centric services

- Service composition
- Internet of Things
- Broadcasting and Media
- Semantic Web

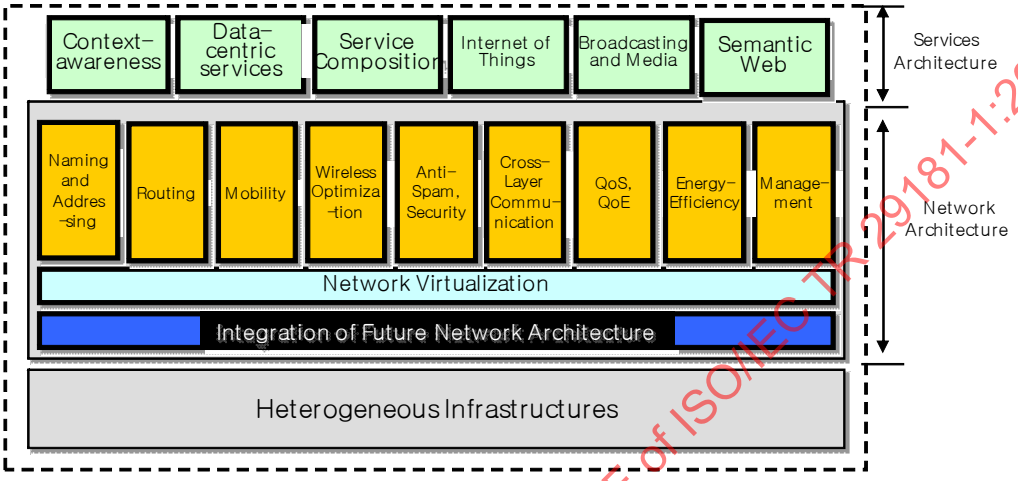

Figure A.1 — General Concept of FN