INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3001

(05/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Future networks

Future Networks: Objectives and Design Goals

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Recommendation ITU-T Y.3001

Future Networks: Objectives and Design Goals

Summary

This Recommendation describes objectives and design goals for Future Networks (FNs). In order to differentiate FNs from existing networks, four objectives were identified, which are service-, data-, environment-, and social and economic awareness. In order to realize the objectives, twelve design goals were identified, which are service diversity, functional flexibility, virtualization of resources, data access, energy consumption, service universalization, economic incentives, network management, mobility, optimization, identification, reliability and security. This Recommendation assumes that the target timeframe for FNs fall approximately between 2015 and 2020. In the appendix, this Recommendation describes technologies elaborated in recent research efforts that are likely to be used as an enabling technology of each design goal.

CONTENTS

Recommendation ITU-T Y.3001

Future Networks: Objectives and Design Goals

1 Scope

This Recommendation describes objectives and design goals for Future Networks. The scope of this Recommendation covers:

- Fundamental issues to which not enough attention was paid in designing current networks, and which are recommended to be the objective of Future Networks
- High-level capabilities and characteristics that are recommended to be supported by Future Networks
- Target timeframe for Future Networks

Ideas and research topics of Future Networks that are important and may be relevant to future ITU-T standardization are included in the Appendix of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.851] Recommendation ITU-T F.851 (1995), Universal Personal Telecommunication (UPT) – Service description (service set 1).

[ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), General overview of NGN.

[ITU-T Y.2019] Recommendation ITU-T Y.2019 (2010), Content delivery functional architecture in NGN.

[ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), Terms and definitions for Next Generation Networks.

[ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2009), Security Requirements for NGN release 1.

[ITU-T Y.2205] Recommendation ITU-T Y.2205, Next Generation Networks - Emergency telecommunications - Technical considerations.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere.

3.1.1 Identifier [Y.2091]: An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms.

3.2.1 Component network: A single homogeneous network, which, by itself, may not provide a single end-to-end global telecommunication infrastructure.

3.2.2 Future Network (FN): A network able to provide services, capabilities, and facilities difficult to provide using existing network technologies. A Future Network is either:

a) A new component network or an enhanced version of an existing one, or

b) A heterogeneous collection of new component networks or of new and existing component networks that is operated as a single network.

Notes:

1 The plural form Future Networks (FNs) is used to show that there may be more than one network that fits in the definition of Future Network.

2 A network of type b may also include networks of type a.

3 The label assigned to the final federation may or may not include the word "future," depending on its nature relative to any preceding network and similarities thereto.

4 'Difficult' does not preclude some current technologies are to be used in future networks.

5 In the context of this Recommendation, the word "new" applied to a component network means that the component network is able to provide services, capabilities, and facilities that are difficult or impossible to provide using existing network technologies.

3.2.3 Service Universalization: A process to provide telecommunication services to every individual or group of people irrespective of social, geographical, and economical status.

4 Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

CDN	Content Distribution Network
ET	Emergency Telecommunications
FN	Future Network
ICT	Information and Communication Technology
IC	Integrated Circuit
ID	Identifier
IP	Internet Protocol
P2P	Peer-to-Peer
QoE	Quality of Experience
QoS	Quality of Service
SoA	Service-oriented Architecture

5 Conventions

This Recommendation uses "is recommended" to indicate the main points to be taken into account in the standardization of FNs. Detailed requirements and their degree ("required", "recommended", "optional") need further study.

6 Introduction

While some requirements for networks do not change, a number of requirements are evolving and changing and new requirements arise, causing networks and their architecture to evolve.

For future networks, traditional requirements such as promoting fair competition [ITU-T Y.2001], which reflect our society's values, remain important.

At the same time, new requirements are emerging. Numerous research projects have proposed requirements pertaining to future society [b-NICT Vision] [b-EC FI], and though there is still a lack of consensus, it is clear that sustainability and environmental issues will be vitally important considerations over the long term. New application areas such as Internet of Things, smart grids, and cloud computing are also emerging. Also, new implementation technologies, such as advanced silicon and optical technology, enable support of requirements that were conventionally considered unrealistic, for example, by substantially reducing the production cost of an equipment. All these new factors introduce new requirements to networks.

The basic architecture of large-scale public networks, such as telecommunication networks, is difficult to change due to the enormous amount of resources needed to build, operate, and maintain them. Their architecture is therefore carefully designed to be flexible enough to satisfy continually changing requirements. For instance, Internet Protocol (IP) absorbs and hides the different protocols and implementations of underlying layers, and with its simple addressing and other features, it has succeeded in adapting to the enormous changes in scalability as well as factors such as Quality of Service (QoS) and security.

However, it is not known if current networks can continue to fulfil changing requirements into the future, and the growing market of new application areas may have the potential to finance the enormous investment required to change the networks if the new architecture pays sufficient attention to backward compatibility and migration costs. Research communities have been working on various architectures and supporting technologies, such as network virtualization[b-Anderson][b-ITU-T FG-FN NWvir], energy-saving of networks[b-ITU-T FG-FN Energy], and content-centric networks[b-Jacobson].

It is therefore reasonable to expect that some requirements can be realized by the new network architectures and supporting technologies described by recent research activities, and that these could be the foundation of networks of the future, whose trial services and phased deployment is estimated to fall approximately between 2015 and 2020. In this Recommendation, networks based on such new architecture are named Future Networks (FNs).

This Recommendation describes objectives that may differentiate FNs from existing networks, design goals that FNs should satisfy, target dates and migration issues, and technologies for achieving the design goals.

7 Objectives

FNs are recommended to fulfil the following objectives which reflect the new requirements that are emerging. These are objectives that are not considered as primary or not realized to a satisfactory

extent in current networks. These objectives are the candidate characteristics that clearly differentiate FNs.

7.1 Service awareness

FNs are recommended to provide services whose functions are designed to be appropriate to the needs of applications and users. The number and range of services is expected to explode in the future. FNs are recommended to accommodate these services without drastic increases in, for instance, deployment and operational costs.

7.2 Data awareness

FNs are recommended to have architecture optimized to handling enormous amounts of data in a distributed environment, and are recommended to enable users to access desired data safely, easily, quickly, and accurately, regardless of their location. In the context of this Recommendation, "data" is not limited to specific data types like audio or video content, but describes all information accessible on a network.

7.3 Environmental awareness

FNs are recommended to be environmentally friendly. The architecture design, resulting implementation and operation of FNs are recommended to minimize their environmental impact, such as the consumption of materials and energy and reducing greenhouse gas emissions. FNs are recommended to also be designed and implemented so they can be used to reduce the environmental impact of other sectors.

7.4 Social and economic awareness

FNs are recommended to consider social and economic issues to reduce barriers to entry for the various actors involved in the network ecosystem. FNs are recommended to also consider the need to reduce their lifecycle costs in order for them to be deployable and sustainable. These factors will help to universalize the services and allow appropriate competition and an appropriate return for all actors.

8 Design goals

Design goals are high-level capabilities and characteristics that are recommended to be supported by FNs. FNs are recommended to support the following design goals in order to realize the objectives mentioned in clause 7. It should be noted that some of these design goals may be extremely difficult to support in a particular FN, and that each design goal will not be implemented in all FNs. Whether the support of each of these design goals in a specific FN will be required, recommended or optional is a topic for further study.

Figure 1 below shows the relationships between the four objectives as described in clause 7 and the twelve design goals described in this clause. It should be noted that some design goals, such as network management, mobility, identification, reliability and security, may relate to multiple objectives, and figure 1 only shows the relationships between a design goal and its most relevant objective.

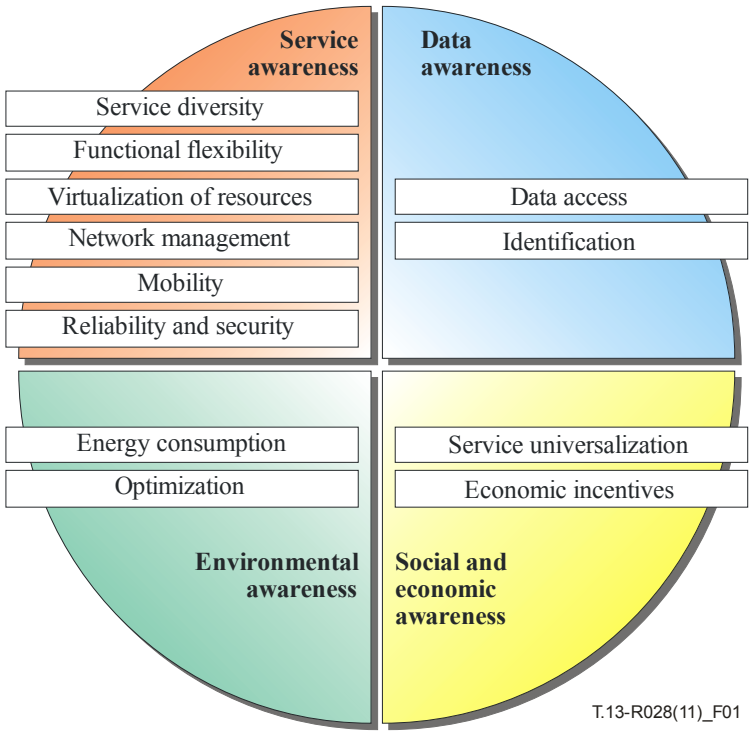

Figure 1 – Four objectives and twelve design goals of Future Networks

8.1 Service diversity

FNs are recommended to support diversified services accommodating a wide variety of traffic characteristics and behaviors. FNs are recommended to support a huge number and wide variety of communication objects such as sensors and terminal devices.

Rationale: In the future, services will become diversified with the appearance of various new services and applications that have quite different traffic characteristics such as bandwidth, latency and traffic behaviours such as security, reliability, and mobility. This requires FNs to support services that existing networks do not handle in an efficient manner. For example, FNs will have to support services that require only occasional transmission of a few bytes of data, services that require bandwidth in order of Gbps, Tbps, and beyond, or services that require end-to-end delay that is close to the speed-of-light delay, or services that allow intermittent data transmission and resulting in very large delay.

In addition, FNs will need to support a huge number and a wide variety of terminal devices to achieve an all-encompassing communication environment. On one hand, in the field of ubiquitous sensor networks, there will be a huge number of networked devices such as sensors and Integrated Circuit (IC) tag readers that will communicate using very small bandwidth. On the other hand, there will be some high-end application such as high quality videoconference application with high realistic sensation and, although the related terminal devices will not necessarily be relatively speaking, so many in number, huge bandwidths will be required for the support of these applications.

8.2 Functional flexibility

FNs are recommended to offer functional flexibility to support and sustain new services derived from user demands. FNs are recommended to support agile deployment of new services keeping pace with their rapid growth and change.

Rationale: It is extremely difficult to foresee all the user demands that may arise in the long term future. Current networks are designed to be versatile, by supporting basic functions that are expected to accompany most of the future user demands in a sufficiently efficient manner. However, the current networks' design approach sometime does not provide sufficient flexibility, e.g. when the basic functions are not optimal for the support of some new services, thus requiring changes in these same functions. Each addition or modification of functions to an already deployed network infrastructure usually results in complex deployment tasks that needs to be carefully planned, otherwise this may have impact on other services that are running on the same network infrastructure.

On the other hand, FNs are expected to enable dynamic modifications of network functions in order to operate various network services that have specific demands. For example, video trans-coding and/or aggregation of sensor data inside the network (i.e. in-network processing) should be possible. It should also be possible to implement new protocols for new type of services in FNs. Services should be laid on a single network infrastructure without interferences between each other, in order to avoid respective impact when a network function is added or modified to support a certain service. FNs should also be able to accommodate experimental services for testing and evaluation purposes, and they should also enable a graceful migration from experimental services to deployed services in order to lower the obstacles for new service deployment.

8.3 Virtualization of resources

FNs are recommended to support virtualization of resources associated with networks in order to support partitioning of resources, and a single resource can be shared concurrently into multiple virtual resources. FNs are recommended to support isolation of any virtual resource from all others. FNs are recommended to support abstraction in which a given virtual resource need not directly correspond to its physical characteristics.

Rationale: For virtual networks, virtualization of resources can allow networks to operate without interfering with the operation of other virtual networks while sharing the network resources among virtual networks. Since multiple virtual networks can simultaneously coexist, different virtual networks can use different network technologies without interfering each other and allowing better utilization of physical resources. The abstraction property enables to provide standard interfaces for accessing and managing the virtual network and resources and helps to support updating of virtual networks' capabilities.

8.4 Data access

FNs are recommended to be designed and implemented for optimal and efficient handling of huge amounts of data. FNs are recommended to have mechanisms for promptly retrieving data regardless of their location.

Rationale: The main purpose of existing telephone networks has been to connect two or more subscribers, enabling them to communicate. IP networks were designed for transmitting data between specified terminals. Currently, users search data on the networks using data oriented keywords, and access them without being aware of their actual location. From a user standpoint, networks evidently are used mainly as a tool for accessing the required data. Since the importance of data access will be sustained in the future, it is essential for FNs to provide users with the means to access appropriate data easily and without time-consuming procedures, while providing data accuracy and correctness.

The amount and properties of digital data in networks are changing. Consumer generated media are growing in explosive manner: social networking services are creating huge volumes of blog articles instantaneously, ubiquitous sensor networks [ITU-T Y.2221] are generating massive amounts of

digital data every second, and some applications called “micro-blogs” generate quasi-real-time communication that includes multimedia data. These data are produced, stored, and processed in networks in a distributed manner. In current IP networks, users access these data in the network via conventional procedures, i.e., identifying the address and port number of the host that provides the target data. Some data contain private information or digital assets, but there are no built-in security mechanisms. More simple, efficient, and safe networking technology dedicated for handling huge volumes of data will therefore be necessary in the future.

The traffic characteristics of such data communication are also changing. Traffic trends in FNs will mainly depend on the location of data rather than the distribution of the subscribers. Because of cloud computing, Information and Communication Technology (ICT) resources such as computing power and stored data in data centers are increasing. Combined with the proliferation of mobile devices with insufficient ICT resources, this trend is shifting data processing from user terminals to data centers. FN designers therefore need to pay close attention to these changes, e.g., the growing importance of communications in data centers, and the huge number of transactions in and between data centers to fulfill user requests.

8.5 Energy consumption

FNs are recommended to use device-, equipment-, and network-level technologies for improvement of energy efficiency and satisfaction of customers’ demands with minimum traffic. FN device-, equipment-, and network-level technologies are recommended to not work independently, but cooperate with each other as a total solution for network energy savings.

Rationale: The lifecycle of a product includes phases such as raw material production, manufacturing, use, and disposal, and these all need consideration in order to reduce the environmental impact. However, energy consumption in the use phase is usually the major issue for equipment operating 24 hours every day; this is often the case in networks. Among the various types of energy consumption, electric power consumption is usually dominant. Energy saving therefore plays a primary role in reducing the environmental impact of networks.

Energy saving is also important for network operations. Necessary bandwidth usually increases as new services and applications are added, but energy consumption and its resulting heat may work as a significant physical limitation in the future, along with other physical limitations such as the capacity of optical fibers or operation frequency of electrical devices. All this may become a major operational obstacle, and in the worst case may prevent new services and applications from being offered.

Traditionally, energy reduction has been achieved mostly by a device-level approach, i.e., by miniaturization of semiconductor processing rules and the process integration of electrical devices, but this approach is facing difficulties such as high standby power and the physical limits of operation frequency. Therefore, not only device-level approaches such as power reduction of electrical and optical devices, but also equipment- and network level approaches are essential in the future.

Switching in the optical domain uses less power than switching in the electronic domain, but packet queues are not easy to implement without electronic memory. Also, circuit switching uses less power than connectionless packet switching.

Networking nodes such as switches and routers should be designed considering smart sleep mode mechanisms, as with existing cell phones; this is an equipment-level approach. For network-level approaches, power-effective traffic control should be considered. A typical example is the use of routing methods that reduce the peak amount of traffic. Another example is caching and filtering, which reduce the amount of data that needs to be transmitted.

Device-, equipment-, and network-level energy saving approaches that consider both improving energy efficiency and reducing inessential traffic are key factors of energy saving in FNs.

8.6 Service universalization

FNs are recommended to facilitate and accelerate provision of facilities in differing areas such as towns or countryside, developed or developing countries, by reducing lifecycle costs of the network and through open network principles.

Rationale: Existing network environments still impose high entry barriers, both for manufacturers to develop equipment, and for operators to offer services. In this sense, FNs should enhance universalization of telecommunication services, facilitating the development and deployment of networks and provision of services.

To that purpose, FNs should support openness through global standards and simple design principles in order to reduce the lifecycle costs of the network, particularly development, deployment, operation, and management costs, and so reducing the so-called digital divide.

8.7 Economic incentives

FNs are recommended to be designed to provide a sustainable competition environment for solving tussles among the range of participants in the ICT/telecommunication ecosystem—such as users, various providers, governments, and IPR holders—by providing proper economic incentive.

Rationale: Many technologies have failed to be deployed, flourish, or be sustainable because of inadequate or inappropriate decisions of the architect, concerning intrinsic economic or social aspects (e.g., contention among participants), or because of the lack of surrounding conditions (e.g., competing technologies) or incentive (e.g., open interface). Such failures have sometimes occurred because the technologies did not provide mechanisms to stimulate fair competition.

One example of this is the lack of QoS mechanisms in the initial IP network implementation needed in real-time services such as video streaming. IP layer did not provide a means to its upper layer to know if QoS was guaranteed from end-to-end. They also lacked proper economic incentives for the network providers to implement them. Coupled with other reasons, these have provided obstacles for introduction of QoS guarantee mechanisms and streaming services in IP networks, even when telecommunications ecosystem participants have tried to customize networks or asked others to provide customized networks to start a new service and share its benefits.

Sufficient attention therefore needs to be paid to economic and social aspects such as economic incentives in designing and implementing the requirements, architecture, and protocol of FNs in order to provide a sustainable competition environment to the various participants.

Ways of resolving economic conflicts including tussles in cyberspace that include economic reward for each participant's contribution are becoming increasingly important [b-Clark]. The use of networks is considered a means of producing economic incentives in various fields as the Internet, generally speaking, grows and puts together diverse social functionalities. Different Internet participants often pursue conflicting interests, which has led to conflict over the Internet and controversy in international/domestic regulation issues.

8.8 Network management

FNs are recommended to be able to efficiently operate, maintain, and provision the increasing number of services and entities. In particular, FNs are recommended to be able to process massive amounts of management data and information efficiently and effectively transform these data to relevant information and knowledge for the operator.

Rationale: The number of service and entities that network must handle is increasing. Mobility and wireless technology have become essential aspects of networks, requirements on security and privacy to adjust to expanding applications and regulations are becoming complicated, and integration of data collecting and processing capability due to Internet of Things, smart grid, cloud computing, and other aspects introduces non-traditional network equipment into networks. This causes proliferation of network management objectives and further complicates evaluation criteria. Thus, effective support for operators is essential in the networks of the future.

One problem current networks face is that economic considerations have caused operation and management systems to be designed specific to each network component. Because the proliferation of unorganized, disorderly management functionality increases complexity and operational costs, FNs should provide highly efficient operation and management system through more integrated management interfaces.

The other problem is that current network operation and management systems largely depend on network operators' skills, so a large problem exists in how to make network management tasks easier and to inherit workers' knowledge. In the process of network management and operation, tasks will remain that require human skill, such as high-level decisions based on years of accumulated experience. For these tasks, it is important that even a novice operator without special skills can manage large-scale and complicated networks easily with the support of automation. At the same time, effective inheritance of knowledge and knowhow should also be intentionally considered.

8.9 Mobility

FNs are recommended to provide mobility that facilitates high-speed and large-scale network in an environment where a huge number of nodes can dynamically move across heterogeneous networks. FNs are recommended to support mobile services irrespective of node's mobility capability.

Rationale: Mobile networks are continuously evolving by incorporating new technologies. Future mobile networks therefore are expected to include various heterogeneous networks, ranging from macro to micro, pico, and even femtocell, and diverse types of nodes equipped with a variety of access technology, because a single-access network cannot provide ubiquitous coverage and a continuously high quality of service-level communications for a huge number of nodes. On the other hand, existing mobile networks such as cellular networks have been designed from a centralized perspective and main signaling functionalities regarding mobility are located at the core network. However, this approach may limit the operational efficiency because signaling of all traffic is handled by centralized systems so that scalability and performance issues arise. From this perspective, highly scalable architecture for distributed access nodes, mechanisms for operators to manage distributed mobile networks, and optimized route for application data and signalling data should be supported for the Future Networks.

Since, the distributed mobile network architecture facilitates deployment ease of new access technologies by flexibly locating mobility functionalities at the access levels, and optimized mobility by short-distance backhauling and high-speed networks, it is the key for providing mobility in future networks.

Even though some technologies that provide mobility service irrespective of a node's capability exist, it is not easy to do so when the node has limited capability, such as sensor. Therefore, how to universally provide mobility should be considered in FNs.

8.10 Optimization

FNs are recommended to provide sufficient performance by optimizing network equipment capacity based on service requirement and user demand. FNs are recommended to perform various optimizations within the network with consideration of various physical limitations of network equipments.

Rationale: The spread of broadband access will encourage the appearance of various services with different characteristics and will further widen the variety of requirements among each service, such as bandwidth, delay, etc. Current networks have been designed to meet the highest level of requirement for the services with maximum number of users, and the transmission capacity of the equipment that is provisioned for the services is usually over-specified for most users and services. If this model is sustained while the user demand increases in the future, the network equipments in the future will face various physical limitations such as transmission capacity of optical fiber, operation frequency of electrical devices, etc.

For this reason, FNs should optimize capacity of network equipments, and also perform optimizations within the network with consideration to various physical limitations of network equipments.

8.11 Identification

FNs are recommended to provide a new identification structure that can effectively support mobility and data access in a scalable manner.

Rationale: Mobility and data access are design goals of FNs. Both features require a provision for efficient and scalable identification (and naming) [ITU-T F.851] of a great number of network communication objects (hosts and data). Current IP networks uses IP addresses for host identification. These are in fact host locators that depend on the points of attachment with the network. As the host moves its Identifier (ID) [ITU-T Y.2091] changes, resulting in broken communication sessions. Cell phones conceal this problem by managing the mobility issues in lower layers, but when the lower layer fails to handle this, e.g., because of the access networks' heterogeneity, this problem reemerges. Similarly, there are no widely used IDs that can be used in the identification of data. FNs therefore should solve these issues by defining a new identification structure for efficiently networking among hosts and data. They should provide dynamic mapping between data and host IDs, as well as dynamic mapping of these IDs with host locators.

8.12 Reliability and security

FNs are recommended to be designed, operated, and evolved with reliability and resilience considering challenging conditions. FNs are recommended to be designed for safety and privacy of their users.

Rationale: Since FNs should serve as essential infrastructures supporting human social activity, they should also support any type of mission critical services such as intelligent traffic management (road-, rail-, air-, marine- and space traffic), smart-grids, e-health e-security, and Emergency Telecommunications (ET) [Y.2205] with integrity and reliability. Communication devices are used to ensure human safety and support automation of human activities (driving, flying, office-home control, medical inspection and supervision, etc). This becomes extremely important in disaster situations (natural disasters, e.g. earthquake, tsunamis, hurricanes, military or other confrontations, large traffic accidents, etc.). Certain emergency response services (e.g., individual-to-authority) may also require priority access to authorized users, priority treatment to emergency traffic, network device identification, and time and location stamping including the associated accuracy information which would dramatically improve the Quality of Service.

All users have to place justifiable trust onto FNs to provide an acceptable level of service even in the face of various faults and challenges to normal operation. This ability of a FN is called resilience which is characterized by its two features trustworthiness (how readily trust can be placed on a system) and challenge tolerance. Trust can be gained from the assurance that the FNs will perform as expected with respect to dependability and security. The trustworthiness of a system is threatened by a large set of challenges, including natural faults (e.g., aging of hardware), large-scale disasters (natural or man-made), attacks (real-world or cyber-based), mis-configurations, unusual but legitimate traffic, and environmental challenges (especially in wireless networks). Challenge Tolerance disciplines deal with the design and engineering of FNs that can continue to provide service in the face of challenges. Its sub-disciplines are survivability, disruption tolerance and traffic tolerance, which enact the capability of a system to fulfil its mission, in a timely manner, in the presence of these mentioned challenges respectively.

FNs are characterized by virtualization and mobility, and also by extensive data and services. Security for networks with these characteristics requires multi-level access control (assurance of user identification, authentication, authorization). This is an addition to existing security requirements such as [ITU-T Y.2701]. This includes protecting the online identity, reputation as well as providing users ability to control unsolicited communications. FNs should provide safe online environment for everyone, in particular for children, disabled people, and minority groups.

9 Target date and migration

In this Recommendation, description of FNs is to meet the assumption that trial services and phased deployment of Future Networks supporting the above objectives and design goals falls approximately between 2015 and 2020. This estimation is based on two factors: the first is the status of current and evolving technologies that would be employed in the experimentation and development of FNs; second is that any novel development that might take place well beyond that estimated date is speculative.

This target date does not mean a network will change by that estimated timeframe, but parts of a network are expected to evolve. Evolution and migration strategies may be employed to accommodate emerging and future network technologies. Such evolution and migration scenarios are topics for further study.

Appendix I

Technologies for achieving the design goals

This appendix describes some of the technologies emerging in recent research efforts. These technologies are likely to be used as an enabling technology for FNs and may play an important role in their development. The title of each clause shows the technology name and the design goal that is most relevant to the technology to show the relevance to the main body of this Recommendation. It should be noted that a technology may relate to multiple design goals. For example, network virtualization deeply relates not only to virtualization of resources, but also to service diversity, functional flexibility, network management, reliability and security. The clause title shows the most relevant design goal.

I.1 Network virtualization (Virtualization of resources)

FNs should provide a broad range of applications, services, and network architectures. Network virtualization is a key technology supporting this. Network virtualization enables creation of logically isolated network partitions over shared physical network infrastructure so that multiple heterogeneous virtual networks can simultaneously coexist over the infrastructure. It also allows aggregation of multiple resources and makes the aggregated resources appear as a single resource. The detailed definition and framework of network virtualization are described in [b-ITU-T FG-FN NWvir].

Users of logically isolated network partitions can program network elements by leveraging programmability that enables users to dynamically import and reconfigure newly invented technologies into virtualized equipment (e.g., routers/switches) in the network. Network virtualization also has federation of networks so that multiple network infrastructures can be operated as part of a single network, even though they are geographically dispersed and managed by different providers. Supporting programmability and federation requires support of the dynamic movement of logical network elements, services, and capabilities among the logically isolated network partitions. In other words, it is possible to remove a service or element from one network partition and re-offer it in a different, logically isolated partition in order to provide a continued service or connection to the end users or other providers. By doing so, the end users or other providers can locate and access such remote services and elements.

I.2 Data/content-oriented networking (Data access)

The explosive growth of the World Wide Web in the Internet has caused a large volume of distribution of digital content such as texts, pictures, audio data, and video data. A large portion of Internet traffic is derived from this content. Therefore, several networking methods focusing on contents distribution have been proposed. These include so-called Content Distribution Networks (CDNs) [ITU-T Y.2019] and Peer-to-Peer (P2P) networking for content sharing.

In addition, some novel approaches specializing in data content handling have been proposed from the perspective of network usage [b-CCNX] [b-Jacobson] [b-NAMED DATA]. They are distinguished from existing networks in the concepts of addressing, routing, security mechanism and so on. While the routing mechanism of current networks depends on ‘location’ (IP address or host name), the new routing method is based on the name of data/content and the data/content may be stored in multiple physical locations with a network-wide caching mechanism. As for security issues, there has been proposals where all data/contents has a public-key signature and can prove

their authenticity. Another research emphasizes naming and name resolution of data in the network [b-Koponen]. Some approaches assume overlay implementation using existing IP networks, and others assume a new implementation base in a clean-slate manner.

There are a couple of research projects that propose a new paradigm called "publish/subscribe (pub/sub) networking" [b-Sarela] [b-PSIRP]. In pub/sub networking, data senders "publish" what they want to send and receivers "subscribe" to the publications that they want to receive. There are other research activities which are trying to create new network architectures based on contents/data new information and information management model. [b-NETINF] [b-Dannewitz].

I.3 Energy-saving of networks (Energy consumption)

Reduction of energy consumption is extremely important with regard to environmental awareness and network operation. This includes variety of device-, equipment-, and network-level technologies [ITU Climate Change] [b-Gupa]. Each technology, whether at the same or different levels, should not work independently, but should cooperate with the others and provide a total solution that minimizes total energy consumption.

Energy-saving of networks has the following three promising areas:

- Forward traffic with less power
  Existing data transmission is usually carried out with power-consuming devices and equipment, and their energy consumption depends mainly on their transmission rate. Energy-saving technologies enables to achieve the same rate with less power using low-power devices/equipment, photonic switching, lightweight protocols, and so on [b-Baliga2007], thus reduce W/bps.
- Control device/equipment operation for traffic dynamics
  Existing network devices or systems continually operate at full specification and full speed. On the contrary, networks with energy-saving technologies will control operation based on the traffic, using methods such as sleep mode control, dynamic voltage scaling, and dynamic clock operation technique [b-Chabarek]. This reduces the total energy consumption needed.
- Satisfy customer requests with minimum traffic
  Existing networks typically have not paid attention to the total amount of traffic to satisfy customer requests. Networks with energy-saving technologies, however, will satisfy requests with minimum traffic. That is, they can reduce inessential or invalid traffic such as excessive keep-alive messages or duplicated user messages, by using multicasting, filtering, caching, redirect, and so on. They reduce traffic and hence reduce the total energy consumption needed.

Based on these characteristics, energy-saving of networks can reduce total power consumption, and serve as a solution to environmental issues from a network perspective. A newly implemented service may increase energy consumption, but networks with energy-saving technologies can mitigate this increase. Compared with cases having no energy-saving technologies, overall energy consumption may even be able to be reduced.

I.4 In-system network management (Network management)

Due to limitations of today's network management operations a new decentralized network management approach, called In-system Management is being developed.[b-MANA][b-UniverSELF] In-System Management employs decentralization, self-organization, autonomy, and autonomicity as its basic enabling concepts. The idea is that, contrary to the legacy approach, the management tasks are embedded in the network and as such it empowering the network to control

complexity. The FN as a managed system now executes management functions on its own. The following are features of the in-system management for FN.

In the future, networks will be large-scale and complicated for supporting various services with different characteristics, such as bandwidth and QoS, so network infrastructure and network service management will become more complicated and difficult tasks. Various approaches have previously been proposed for standardizing the network management system by defining the common interface for the operation system, such as the service-oriented architecture (SOA) concept, but have not been operated due to problems such as cost. This will grow worse in the future due to the proliferation of different management systems caused by increasing services, so high-efficiency operation and management technologies are needed. Also, because current network operation and management depends mainly on the skills of the network manager, making easy network management tasks and inheriting workers' knowledge are significant problems.

There are two candidate functions to achieve these goals.

First is a unified operation and management system from the perspective of highly efficient management, the other is sophisticated control interface and inheritance system of operator knowledge and knowhow for network operation and management by lower-skilled operators.

Below are candidates for FNs to achieve these goals.

a) Common interface for operation and management [b-TMF NGOSS] [b- Nishikawa]
This provides the high-efficient operation and management to adapt all of network systems that provide different services. The database technology to automatically migrate old system database, the database that contains user and infrastructure information to the new system is the key.

b) Sophisticated control interface and inheritance system of operator knowledge and knowhow [b-Kipler] [b-Kubo]

In order to make network control and management of various network systems and services easier for operators without special skills, FN operation systems should have autonomous control and self-stabilizing mechanisms. Sophisticated and friendly control interfaces will also help in some network operation and management tasks. One viable approach is "visualization" of various network statuses as follows:

- Visualization of system management (software-level technology)
  Network visualization technology supports the work of the system administrator and improves work efficiency by easily visualizing the state of the network. Visualization technology includes monitoring of networks, fault localization, and network system automation.
- Visualization of infrastructure management (hardware-level technology)
  Hardware-based visualization technology is also efficient for supporting field engineers. This includes monitoring of fiber and states of communications, fault localization, and fiber identification. It also makes it easy to identify the location of the failure, particularly if it is on the network side or in user devices, which reduces maintenance costs.

I.5 Network optimization (Optimization)

The appearance of new services will increase the bandwidth required by many users, while others will remain satisfied with the current bandwidth, which widens the variety of bandwidth requirements among users. Current networks have been designed to meet maximum user needs and the capacity of the equipment is over-specified for most services. Network equipment in the future will face various physical limitations such as capacity of optical fiber, operation frequency of

optical and electrical devices, and power consumption. Future Networks should therefore be designed to improve effectiveness of use in providing optimal (i.e., not abundant) capabilities for user needs.

Three promising areas can address the above issues: device level optimization, system level optimization, and network level optimization.

a) Device level optimization [b-Kimura]
This operation rate optimization technique composed of an optical layer, electrical layer, and optical/electrical layer hybrid technique provides the minimum needed bandwidth for services and applications.

b) System level optimization [b-Stok]
Though encrypting all data in networks is the ultimate solution against security threats, data are currently selectively encrypted via higher layer functions, and higher layers are too slow to encrypt everything. Optimizing security mechanisms, i.e., concentrating encryption functions in lower-layer processing (physical layer processing technique such as OCDM transmission technology) and stopping higher-layer encryption would enable high security to be achieved at the same time as low latency and power efficiency.

c) Network level optimization [b-Iiyama]
This form of optimization tackles problems such as the physical limitation of optical fiber capacity and operation frequency of electrical devices by changing the traffic flows themselves. The technique also offers potentially higher utilization of network resources such as network paths or equipment.

- Path optimization
  Current networks, which transmit current services such as text or voice, cannot evolve to high-speed, large-capacity, and low-latency End-to-End (E2E) for all optical networks due to economical, technical, and other such problems. The path optimization technique provides the optimized path considering service characteristics and traffic conditions of the transmission route. It also has the ability to synchronize data sent by a different path, thus enabling sending of information consisting of multiple data with different characteristics by using a different path. Combined with operation rate optimization, low- to very high-speed data transmission can be achieved in a single network that enables simultaneous easy operation and improved effectiveness.
- Network topology optimization
  This technology optimizes upper-layer (e.g., packet layer) network topology using not only upper-layer information, such as geographical distribution of users' traffic demands, but also topology information of underlying lower-layer (e.g., optical layer) networks.
- Accommodation point optimization
  In current networks, every service is transmitted on the same access line; therefore an access point accommodates all services for a user. This decreases accommodation efficiency because each service has different characteristics such as bandwidth, latency, and usability. The accommodation point optimization technique provides high accommodation efficiency and flexible accommodation that enables optimization of the accommodation point considering, for instance, the possible transmission distance for each service, which fully uses the advantage of optical technologies and long-distance transmission.
- Cache and storage optimization
  The distribution of different contents on an efficient manner improving QoS at lower cost is a challenge for future networks. The use of storage and caching capabilities allows distributing

and delivering contents as close as possible to the end-users, thus optimizing network performance and improving Quality of Experience(QoE) of the end-users.

- Computing optimization
  The computing capabilities provided by the network allow the end-users (principally enterprises) to deploy and run computing tasks (software applications, including optimization aspects). Distributed computing capabilities inside the network allow more flexible use of the network and improve both service and network performances.

I.6 Distributed mobile networking (Mobility)

In current networks, main functions such as physical mobility management, authentication, and application servers are installed in the centralized systems, or the mobile core network. This causes problems such as scalability, performance, single point of failure, and bottlenecks.

A small and portable wireless access node with distribution of network functions, including mobility functions, has been attracting broad attention as an alternative access method, especially for residential and enterprise deployment [b-Chiba]. In this distributed architecture, the mobility events and data paths can be managed and anchored as closely as possible to the terminals to prevent scalability and performance issues. Single point of failure and bottleneck issues can also be isolated since only a small number of terminals are managed at the edge of the access node level.

By flexibly locating functionalities, which have conventionally resided in the mobile core network, at any part of the network in a distributed fashion, a highly efficient and scalable mobile network can be realized. Thus, unlike the current mobile network, distributed mobile networking can:

- localize and optimize the signaling and data paths;
- enable the network administrator to control the signaling and data path
- locate the functional entities (e.g., mobility management) anywhere in the network (both in the mobile core and access networks)
- provide the discovery function (network resources and devices) of the connected devices in both centralized and distributed fashions
- connect devices not fully capable of mobility and/or security without degrading those features

By supporting the above functionalities, distributed mobile networking can provide always-on, always-best connected access with guaranteed end-to-end services.

Bibliography

[b-NICT Vision] National Institute of Information and Communications Technology, "Vision and Technology Requirements for a New-generation Network," February 2009.

[b-EC FI] European Commission, "Future Internet 2020: Visions of an Industry Expert Group," May 2009.

[b-Anderson] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the Internet impasse through virtualization," Computer, vol. 38, no. 4, 2005.

[b-ITU-T FG-FN NWvir] "Framework of Network Virtualization," ITU-T Focus Group on Future Networks , FGFN-OD73, December 2010.

[b-ITU-T FG-FN Energy] "Overview of Energy Saving of Networks," ITU-T Focus Group on Future Networks , FGFN-OD74, December 2010.

[b-Jacobson] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," CoNEXT 2009, Rome, December 2009.

[b-TMF NGOSS] "The NGOSS approach to Business Solutions," Tele Management (TM) Forum, Release 1.0, 2005.

[b-Nishikawa] K.Nishikawa, F.Yokose, H.Nozue, N.Nawa, T.Masuda and T.Yamamura, "Scenario Editing Method for Automatic Client Manipulation System," APNOMS, 2009.

[b-Kipler] D. C. Kilper et al., "Optical Performance Monitoring," J. Lightwave Technol., vol. 22, pp. 294-304, 2004.

[b-Kubo] T. Kubo et al., "In-line monitoring technique with visible light form 1.3μm-band SHG module for optical access systems," Optics Express, vol. 18, no. 3, 2010.

[b-Gupa] M. Gupta and S. Singh, "Greening of the Internet," Proc. ACM SIG-COMM '03, August 2003.

[b-Baliga2007] J. Baliga et al., "Photonic Switching and the Energy Bottleneck," Proc. IEEE Photonics in Switching, August 2007.

[b-Chabarek] J. Chabarek et. al., "Power Awareness in Network Design and Routing," in Proc. IEEE INFOCOM '08, April 2008.

[b-HIP] IETF Host Identity Protocol (hip), http://datatracker.ietf.org/wg/hip/.

[b-LISP] IETF Locator/ID Separation Protocol (lisp), http://datatracker.ietf.org/wg/lisp/.

[b-Kafle] V. P. Kafle and M. Inoue, "HIMALIS; Heterogeneous Inclusion and Mobility Adaption through Locator ID Separation in New Generation Network," IEICE Trans. Com., Vol. E93-B, March 2010.

[b-Bohl] O. Bohl, S. Manouchehri, U. Winand, "Mobile information systems for the private everyday life," Mobile Information Systems, December 2007.

[b-Chiba] T. Chiba and H. Yokota, "Efficient Route Optimization Methods for Femtocell-based All IP Networks," WiMob '09, October 2009.

[b-Kimura] H.Kimura et al., "A Dynamic Clock Operation Technique for Drastic Power Reduction in WDM-based Dynamic Optical Network Architecture," in Proc. S07-3, World Telecommunication Congress (WTC), 2010.

[b-Gunaratne] C. Gunaratne et al., "Reducing the energy consumption of Ethernet with adaptive link rate (ALR)," IEEE Trans. Computers, vol. 57, no. 4, pp. 448-461, Apr. 2008.

[b-Iiyama] N.Iiyama et al., "A Novel WDM-based Optical Access Network with High Energy Efficiency Using Elastic OLT," in Proc. ONDM'2010, 2.2, Feb. 2010.

[b-CCNX] Project CCNx (Content-Centric Networking), http://www.ccnx.org/.

[b-NAMED DATA] Named Data Networking, http://www.named-data.net/.

[b-Koponen] T. Koponen, M. Chawla, B. Chun, et al, "A data-oriented (and beyond) network architecture," ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, pp. 181-192, October 2007.

[b-NETINF] Network of Information (NetInf), http://www.netinf.org/.

[b-Dannewitz] C. Dannewitz, "NetInf: An Information-Centric Design for the Future Internet," In Proc. 3rd GI/ITG KuVS Workshop on The Future Internet, May 2009.

[b-Sarela] M. Särelä, T. Rinta-aho, and S. Tarkoma, "RTFM: Publish/Subscribe Internetworking Architecture," ICT-Mobile Summit, 2008.

[b-PSIRP] Publish-subscribe Internet Routing Paradigm(PSIRP), http://www.psirp.org/

[b-Clark] D. Clark, J. Wroclawski, K. Sollins, and R. Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," IEEE/ACM Transactions on Networking, vol. 13, no. 3, June 2005.

[b-MANA] A. Galis, H. Abramowicz, M. Brunner, D. Raz, P.R. Chemouil, J. Butler, C. Polychronopoulos, S. Clayman, H. de Meer, T. Coupaye, A. Pras, K. Sabnani, P. Massonet, S. Naqvi "Management and Service-aware Networking Architectures (MANA) for Future Internet - Position Paper: System Functions, Capabilities and Requirements", December 2008.

[b-UniverSELF] UniverSelf, realizing autonomics for Future Networks, http://www.univerself-project.eu/.